มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์: ศึกษากรณีการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

จิรัชยา จิ้นสุริวงษ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ปรีดี พนมยงค์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2564

LEGAL MEASURES ON MEDICAL COMMUNICATION TECHNOLOGY CONTROL: CASE STUDY OF THE PROTECTION OF PERSONAL DATA OF PATIENTS

JIRATCHVA JINSURIWONG

A Thsis Submitted in Partial Fulfillment of the Requirement

for the Drgree of Master of Law Department

Department of Law

Pridi Bhanomyong Faculty of Law, Dhurakij Pundit University

2021

ใบรับรองวิทยานิพนธ์

คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญานิติศาสตรมหาบัณฑิต

หัวข้อวิทยานิพนธ์ มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์: ศึกษากรณีการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

เสนอโดย นางสาวจิรัชยา จิ้นสุริวงษ์

สาขาวิชา นิติศาสตร์

หมวดวิชา กฎหมายทางการแพทย์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รองศาสตราจารย์ ดร.ภูมิ โชคเหมาะ

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบวิทยานิพนธ์แล้ว

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สุธี อยู่สถาพร)

.....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์

(รองศาสตราจารย์ ดร.ภูมิ โชคเหมาะ)

.....กรรมการ

(อาจารย์ ดร.จิรวุฒิ ลิปิพันธ์)

คณะนิติศาสตร์ปรีดี พนมยงค์ รับรองแล้ว

..... คณบดีคณะนิติศาสตร์ปรีดี พนมยงค์

(ผู้ช่วยศาสตราจารย์ ดร.สมชาย รัตนชื่อสกุล)

วันที่ ๓๑ เดือน กรกฎาคม พ.ศ. ๒๕๖๔

หัวข้อวิทยานิพนธ์	มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์: ศึกษากรณีการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย
ชื่อผู้เขียน	จิรัชยา จิ้นสุริวงษ์
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร.ภูมิ โชคเหมาะ
สาขาวิชา	นิติศาสตร์
ปีการศึกษา	2563

บทคัดย่อ

วิทยานิพนธ์เล่มนี้มีวัตถุประสงค์เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับเทคโนโลยีทางการแพทย์ และข้อมูลบุคคล ของผู้ป่วย เนื่องจากมาตรการทางกฎหมายเกี่ยวกับความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลของผู้ป่วยที่มีอยู่ในปัจจุบัน ไม่สามารถให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยเป็นการเฉพาะเมื่อมีเทคโนโลยีในการจัดเก็บข้อมูลของผู้ป่วยเข้ามาเกี่ยวข้องโดยศึกษาการวิเคราะห์และเปรียบเทียบระหว่างกฎหมายต่างประเทศ ได้แก่ สหภาพยุโรป สหพันธ์สาธารณรัฐเยอรมนี เครือรัฐออสเตรเลีย สหราชอาณาจักร และสหรัฐอเมริกา กับกฎหมายของประเทศไทย เพื่อหาแนวทางในการกำหนดมาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยได้อย่างเหมาะสมและมีประสิทธิภาพ

ปัจจุบันมีความก้าวหน้าทางด้านเทคโนโลยี ทำให้รูปแบบในการจัดเก็บข้อมูลส่วนบุคคลของผู้ป่วยมีความเปลี่ยนแปลงไปอย่างมาก ซึ่งข้อมูลส่วนบุคคลของผู้ป่วยที่เข้ารับบริการทางสาธารณสุขที่ให้ไว้แก่บุคลากรทางการแพทย์มีข้อมูลที่สำคัญ ซึ่งเป็นประโยชน์ต่อการวินิจฉัยและเพื่อการสร้างเสริมสุขภาพการป้องกันโรค การตรวจวินิจฉัยโรคการรักษาพยาบาลและการฟื้นฟูสมรรถภาพ โดยถูกบันทึกและจัดเก็บในรูปแบบเวชระเบียนอิเล็กทรอนิกส์ (Electronic Medical Record -EMR) ซึ่งมีความสะดวก และรวดเร็วในการสืบค้นข้อมูลของผู้ป่วย และส่งข้อมูลระหว่างโรงพยาบาลเพื่อความต่อเนื่องในการรักษาของผู้ป่วย การให้ความคุ้มครองในข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์จึงมีความสำคัญอย่างมาก เพราะมีความเสี่ยงที่ข้อมูลของผู้ป่วยจะถูกเปิดเผยซึ่งเกิดจากการกระทำของเจ้าหน้าที่ทางการแพทย์ หรือบุคคลภายนอกผู้ไม่ประสงค์ดี โดยการทำลายความปลอดภัยของระบบป้องกันข้อมูล หรือที่เรียกว่า “แฮคเกอร์ (Hackers)” การปล่อยไวรัสคอมพิวเตอร์ (Viruses Computer) เป็นต้น ทำให้ข้อมูลส่วนบุคคลของผู้ป่วยถูกเปิดเผยหรือเสียหาย อันส่งผลเสียต่อ

เจ้าของมูลไม่ว่าด้านชื่อเสียง ความปลอดภัย หรือทรัพย์สิน ซึ่งในปัจจุบันมีกฎหมายไทยที่เกี่ยวข้องกับความคุ้มครองข้อมูลส่วนบุคคล ปรากฏอยู่ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 หมวด 3 มาตรา 32 ซึ่งให้ความคุ้มครองข้อมูลส่วนบุคคลแต่ไม่ครอบคลุมถึงข้อมูลส่วนบุคคลของผู้ป่วยในรูปแบบอิเล็กทรอนิกส์ และพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล แต่กิจการด้านการแพทย์และสาธารณสุขไม่เป็นกิจการที่อยู่ในบังคับ ซึ่งทำให้ไม่มีความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในรูปแบบอิเล็กทรอนิกส์ และไม่มีบทบัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์ และไม่มีกำหนดความรับผิดกรณีข้อมูลส่วนบุคคลของผู้ป่วยถูกเปิดเผยโดยปราศจากความยินยอม อีกทั้งขาดเจ้าหน้าที่และหน่วยงานที่รับผิดชอบในการป้องกันข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์ จึงส่งผลให้ไม่มีมาตรการทางกฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์อย่างเหมาะสม

จากการศึกษาปัญหาข้างต้น ผู้ศึกษาจึงมีแนวความคิดให้กำหนดมาตรการทางกฎหมาย ดังนี้ 1. บัญญัติกฎหมายที่มีความเฉพาะเกี่ยวกับเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย 2. กำหนดการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยไว้โดยชัดแจ้ง 3. กำหนดหลักเกณฑ์ในการพิจารณาความรับผิด กรณีข้อมูลส่วนบุคคลของผู้ป่วยถูกแทรกแซงและได้รับความเสียหาย 4. กำหนดให้มีหน่วยงานที่รับผิดชอบในการป้องกันข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์ และ 5. แก้ไขปรับปรุงกฎหมายอื่น ๆ ที่เกี่ยวข้อง

Thesis title	Legal Measures on Medical Communication Technology Control : Case Study of the Protection of Personal Data of Patients
Author	Jiratchya Jinsuriwong
Thesis Advisor	Associate Professor Dr. Poom Chokmoh
Department	Law
Academic year	2020

ABSTRACT

Thesis of this research was to investigate the legal measures on medical technology and patient personal data, as current legal measures on the protection of patient personal data cannot provide protection of patient personal data specifically, especially when patient data collection technology was involved. This research studied, analyzed, and compared between foreign laws including the European Union, Federal Republic of Germany, Commonwealth of Australia, the United Kingdom and United States of America, and the laws of Thailand to determine legal measures for the protection of patient personal data appropriately and efficiently.

Today, advances in technology have dramatically changed the way the personal data of patients are collected. The personal data of patients attending public health services that are provided to healthcare professionals includes the following important data useful for diagnosis and for health promotion, disease prevention, diagnosis, medical treatment, and rehabilitation. Personal data is recorded and stored in an electronic medical record (EMR) format, which is convenient and fast in querying patient data and sending data between hospitals for continuity of treatment of patients. Protecting patient's personal data in electronic medical records is very important because there is a risk that patient data will be disclosed due to the actions of medical staff or third parties who have a bad intention by destroying the security of data protection systems known as “hackers”, releasing the virus computer, etc. This causes patient personal data to be disclosed or damaged that adversely affects the owner of the data, whether in reputation, safety, or property. At present, Thai laws relating to the protection of personal data appear in the Constitution of the Kingdom of Thailand, Buddhist

Era 2560 (2017), Chapter 3, Section 32, which provides protection for personal data, but does not cover patient personal data in electronic form and the Personal Data Protection Act, 2562 B.E. (2019). The controller of personal data must establish measures for the security of personal data. However, medical and public health businesses are not compulsory, so there is no electronic protection of patient personal data, no provision to protect patient personal data in electronic medical records, and there is no liability limit if patients' personal data is disclosed without their consent. There is also a lack of staff and departments responsible for the protection of patient personal information in electronic medical records. As a result, there are no legal measures to properly protect patient personal data in electronic medical records.

Based on the study of the above problems, the student has the idea to define legal measures as follows : 1. Enact laws specific to medical communication technology and personal data of Patients. 2. Specify the patient's personal data protection explicitly. 3. Establish criteria for determining liability in the case of patient personal data being interrupted and damaged. 4. Establish a body responsible for the protection of patient personal data in electronic medical records. 5. Amending other relevant laws.

กิตติกรรมประกาศ

วิทยานิพนธ์ เรื่อง มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ : ศึกษากรณีการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย สำเร็จลุล่วงได้นั้น เนื่องด้วยได้รับความเมตตากรุณาเป็นอย่างดียิ่งจาก รองศาสตราจารย์ ดร.ภูมิ โชคเหมาะ ซึ่งรับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์เล่มนี้ และคณะกรรมการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.สุธี อยู่สถาพร ซึ่งรับเป็นประธานสอบเล่มวิทยานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.จิราวุฒิ ลิปิพันธ์ ซึ่งรับเป็นกรรมการสอบวิทยานิพนธ์ ทุกท่านซึ่งสละเวลาอันมีค่าในการรับเป็นกรรมสอบวิทยานิพนธ์ และตรวจสอบรายละเอียดเนื้อหาสาระ ตลอดจนให้คำชี้แนะ และเจ้าหน้าที่ประจำคณะนิติศาสตร์ปรีดี พนมยงค์ที่ช่วยประสานงานและติดต่อด้านต่าง ๆ อำนวยความสะดวกระหว่างดำเนินการจัดทำวิทยานิพนธ์ตลอดมา จนกระทั่งสำเร็จลุล่วงละสมบูรณ์จนมาเป็นวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณ มหาวิทยาลัยธุรกิจบัณฑิตย์ คณาจารย์ เจ้าหน้าที่ คณะนิติศาสตร์ ปรีดี พนมยงค์ ทุกท่าน รวมถึงเพื่อนในสาขากฎหมายการแพทย์ มหาวิทยาลัยธุรกิจบัณฑิตย์ ที่คอบให้กำลังใจ คำปรึกษา ความช่วยเหลือที่เป็นประโยชน์ต่อผู้วิจัยมาโดยตลอด จนกลายเป็นแรงผลักดันให้ผู้วิจัยสามารถจัดทำวิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วง

ขอกราบขอบพระคุณบิดามารดาผู้ให้กำเนิด ซึ่งท่านได้อบรมสั่งสอน เลี้ยงดู และให้กำลังใจ รวมถึงคุณยาย และน้องสาว ซึ่งคอยให้กำลังใจ และคำแนะนำ แก่ผู้วิจัยเสมอมา ซึ่งผู้วิจัยหวังว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อผู้อ่านไม่มากก็น้อย หากเกิดความบกพร่องประการใดผู้วิจัยจึงขออภัยมา ณ ที่นี้ด้วย

จิรัชยา จิ้นสุริวงษ์

สารบัญ

สารบัญ(ต่อ)

สารบัญ(ต่อ)

สารบัญภาพ

สารบัญตาราง

ตารางที่ **หน้า**

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ข้อมูลส่วนบุคคลของผู้ป่วย ที่รับบริการทางสาธารณสุข[1]หรือการรับบริการด้านการแพทย์และสาธารณสุขที่ให้โดยตรงแก่บุคคลเพื่อการสร้างเสริมสุขภาพ การป้องกันโรค การตรวจวินิจฉัยโรค การรักษาพยาบาลและการฟื้นฟูสมรรถภาพ ที่จำเป็นต่อสุขภาพและการดำรงชีวิต ทั้งนี้ให้รวมถึงการบริการการแพทย์แผนไทยและการแพทย์ทางเลือกตามกฎหมายว่าด้วยการประกอบโรคศิลปะ[2] ซึ่งผู้เข้ารับบริการหรือผู้ป่วยจะให้ข้อมูลแก่เจ้าหน้าที่โรงพยาบาล เพื่อการขึ้นทะเบียนผู้ป่วย โดยเจ้าหน้าที่โรงพยาบาลจะทำการซักประวัติของผู้ป่วย เพื่อให้ได้เรื่องราวความเจ็บป่วยของผู้ป่วย โดยมีประวัติที่จำเป็นต้องซักถามกับผู้ป่วย ได้แก่ ข้อมูลส่วนตัว อาการสำคัญ ประวัติการเจ็บป่วย ในปัจจุบัน ประวัติการเจ็บป่วยในอดีต ประวัติครอบครัว ซึ่งเป็นประโยชน์ต่อการวินิจฉัยของ และการวางแผนการักษาของแพทย์ โดยข้อมูลดังกล่าวนั้น เป็นข้อมูลด้านสุขภาพของบุคคล[3] ซึ่งไม่สามารถนำไปเปิดเผยอันเป็นประการที่น่าจะทำให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับความเสียหายไม่ได้ เว้นแต่การเปิดเผยของข้อมูลนั้นเป็นไปตามความประสงค์ของบุคคลผู้เป็นเจ้าของข้อมูลโดยตรง

การพัฒนาทางด้านเทคโนโลยีและความเปลี่ยนแปลงของสังคมในปัจจุบัน ทำให้การจัดเก็บข้อมูลของผู้ป่วยอยู่ในรูปแบบอิเล็กทรอนิกส์ หรือที่เรียกว่า “เวชระเบียนอิเล็กทรอนิกส์ หรือ

---

[1] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550, มาตรา 3 ให้คำนิยาม “บริการสาธารณสุข” หมายความว่า บริการต่าง ๆ อันเกี่ยวกับการสร้างเสริม สุขภาพการป้องกันและควบคุมโรคและปัจจัยที่คุกคามสุขภาพ การตรวจวินิจฉัยและบำบัดสภาวะ ความเจ็บป่วย และการฟื้นฟูสมรรถภาพของบุคคล ครอบครัวและชุมชน”

[2] พระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. 2545, มาตรา 3

[3] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550, มาตรา 7

Electronic Medical Records (EMRs)" คือ บันทึกทางการแพทย์ของกระดาษแต่ละฉบับแบบดิจิทัล ที่สแกน เวชระเบียนอิเล็กทรอนิกส์หมายถึงบันทึกทางการแพทย์ของผู้ป่วยภายในสถานที่เดียว เช่น คลินิกของแพทย์หรือสำนักงาน EMR เป็นบันทึกดิจิตอล ที่แพทย์หรือองค์กรดูแลรักษา ผู้ป่วย เพื่อติดตามการรักษาและสภาพสุขภาพในปัจจุบัน ซึ่งในปัจจุบันประเทศไทยยังไม่มีมาตรการในการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ เพื่อการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย ซึ่งมีวัตถุประสงค์เพื่อให้ความคุ้มครองข้อมูลส่วนของผู้ป่วย ซึ่งเข้ารับบริการทางแพทย์และอยู่ในความดูแลของโรงพยาบาล

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐานที่นานาประเทศต่างให้ความสำคัญเป็นอันดับต้น ๆ การคุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นส่วนตัวนั้น หมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งเรื่องความคุ้มครองข้อมูลส่วนบุคคลนั้นมีการรับรองสิทธิดังกล่าวอย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 12[4] และรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 การให้ความคุ้มครองข้อมูลส่วนบุคคลในมาตรา 32[5] และในส่วนของความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย มีกำหนดไว้ในคำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย ในสิทธิของผู้ป่วย ข้อ 6[6]

---

[4] ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มาตรา 12 "บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น"

[5] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 "บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

[6] คำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย ข้อ 6. "ผู้ป่วยมีสิทธิได้รับการปกปิดข้อมูลของตนเอง เว้นแต่ผู้ป่วยจะให้ความยินยอมหรือเป็นการปฏิบัติตามหน้าที่ของผู้ประกอบวิชาชีพด้านสุขภาพ เพื่อประโยชน์โดยตรงของผู้ป่วยหรือตามกฎหมาย"

นอกจากนี้เทคโนโลยีที่ถูกนำใช้ในโรงพยาบาล คือ อุปกรณ์เครื่องมือทางการแพทย์ (Medical Device) เป็นสิ่งที่ถูกออกแบบมาเพื่อช่วยในด้านการแพทย์ และทางสาธารณสุขสำหรับการรักษาผู้ป่วยในสถานพยาบาล ซึ่งเป็นกรรมวิธีการรักษาสมัยใหม่ และมีประสิทธิภาพในการรักษา ซึ่งในปัจจุบันเครื่องมือทางการแพทย์มีบทบาทเพิ่มมากขึ้น เพราะทำให้การรักษามีความสะดวกรวดเร็วขึ้น ลดอาการบาดเจ็บ หรือความเสี่ยงจากการรักษาในรูปแบบเดิม ๆ ระยะเวลาในการพักฟื้นหลังจากทำการรักษาในโรงพยาบาลน้อยลงตามการพัฒนาของเทคโนโลยีด้านเครื่องมือทางการแพทย์ ซึ่งมีอยู่หลากหลายประเภท และขึ้นอยู่กับวัตถุประสงค์ที่นำมาใช้กับร่างกายของผู้ป่วยไม่ว่าจะเป็นเพื่อการวินิจฉัย รักษาโรค การป้องกันเฝ้าระวัง และดูแลผู้ป่วยตั้งแต่ระหว่างการรักษาจนถึงการฟักฟื้นตัวหลังรักษา การใช้อุปกรณ์ทดแทนแก่ร่างกายที่มีความบกพร่อง หรือเพื่อการทดลองด้านวิทยาการทางกายภาพ ซึ่งการใช้เครื่องมือทางการแพทย์จะต้องกระทำโดยแพทย์ผู้เชี่ยวชาญหรือผู้มีความรู้เฉพาะด้าน ทั้งนี้ไม่ว่าเครื่องมือทางการแพทย์นั้นจะใช้เพื่อการรักษาภายในหรือภายนอกของร่างกายของผู้ป่วย

เครื่องมือทางการแพทย์ได้จำแนกเครื่องมือทางการแพทย์ออกเป็น 4 ประเภทใหญ่ ๆ ด้วยกันดังนี้

1. อุปกรณ์การแพทย์ เช่น มีดผ่าตัด เครื่องวัดความดัน เครื่องวัดเบาหวาน
2. บริภัณฑ์การแพทย์[7] เช่น เครื่องเอกซเรย์ เครื่องอัลตราซาวด์ เครื่องสลายนิ่ว
3. วัสดุการแพทย์และวัสดุฝังในทางศัลยกรรม เช่น ถุงมือยางทางการแพทย์ ผ้าก๊อซ ซิลิโคน (Silicone)
4. เครื่องมือแพทย์เฉพาะทาง เช่น ชุดน้ำยาตรวจการติดเชื้อเอชไอวี (HIV) ชุดตรวจน้ำตาลในปัสสาวะ เครื่องมือทันตกรรม

ในปัจจุบันประเทศแม้ว่าจะมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวการให้ความคุ้มครองข้อมูลส่วนบุคคลที่หมายรวมถึงการเก็บ รวบรวม ใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล เนื่องจากความก้าวหน้าทาง

---

[7] บริภัณฑ์การแพทย์ เป็นเครื่องมือแพทย์ประเภทหนึ่ง ลักษณะการทำงานจะสลับซับซ้อน ให้ผลการทำงานที่แม่นยำ เครื่องมือแพทย์ประเภทนี้จะถูกพัฒนาขึ้นโดยเทคโนโลยีชั้นสูง และการรักษาจะต้องมีผู้เชียวชาญเฉพาะด้าน และมีความรู้ความสามารถเป็นอย่างมาก ผ่านการอบรม ประเมินผลอยู่ตลอด

เทคโนโลยีมีมากขึ้น ทำให้มีช่องทางสื่อสารต่าง ๆ หลากหลายช่องทาง ทั้งการนำเข้าหรือส่งออกข้อมูลมีความสะดวก รวดเร็วขึ้น

จากที่กล่าวมาข้างต้นพบว่า ประเทศไทยมีปัญหาทางกฎหมายเกี่ยวกับการการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย เนื่องจากการจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ หรือเวชระเบียนอิเล็กทรอนิกส์ จะมีความสะดวกรวดเร็ว ในการบันทึกเพื่อจัดเก็บข้อมูล และนำข้อมูลของผู้ป่วยออกมา แต่ก็มีความเสี่ยงในเรื่องความปลอดภัยจากการเข้าถึงข้อมูลของผู้ป่วยของผู้ป่วยโดยบุคคลภายนอก ระดับความปลอดภัยในการเข้าถึงข้อมูลในระดับความอ่อนไหวที่แตกต่างกันของข้อมูล จึงมีประเด็นปัญหาในการศึกษาดังนี้

ประเด็นปัญหาที่หนึ่ง ปัญหาทางกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

ปัจจุบันเทคโนโลยีทางการแพทย์ที่มีการพัฒนามากขึ้นเพื่อตอบสนองต่อการรักษา ตรวจวินิจฉัย ฟื้นฟู และการป้องกันโรคแก่ผู้ป่วย แต่มีปัญหาที่น่าสนใจเกี่ยว “ข้อมูลส่วนตัว” ของผู้ป่วยซึ่งถือเป็นเรื่องเฉพาะของผู้ป่วย ในการเข้ารีบบริการทางการแพทย์ ไม่ว่าจะเพื่อการตรวจรักษา ฟื้นฟู หรือประการอื่นใด ผู้ป่วยซึ่งเข้ารับบริการทางการแพทย์จะต้องแจ้งข้อมูลแก่ทางโรงพยาบาลโดยไม่ปิดบัง ทั้งเพื่อประสิทธิภาพ และการวินิจฉัยจะเป็นไปด้วยความแม่นยำ และเมื่อแพทย์ผู้ทำการรักษาได้ดำเนินการรักษาเป็นที่เรียบร้อยก็จะบันทึกข้อมูลการรักษาของผู้ป่วยลงในเวชระเบียนอิเล็กทรอนิกส์ แต่ข้อมูลส่วนบุคคลของผู้ป่วยบางประการเป็นข้อมูลที่มีความอ่อนไหวและไม่สามารถเปิดต่อบุคคลอื่นซึ่งไม่ใช่เจ้าของข้อมูล หรือเจ้าของไม่ได้ให้ความยินยอม เพราะการเปิดเผยบางอย่างอาจส่งผลกระทบต่อตัวผู้ป่วยได้ แต่เนื่องจากเทคโนโลยีที่มีการพัฒนาให้สามารถเชื่อมฐานข้อมูลกับระบบคอมพิวเตอร์และอยู่ในรูปแบบออนไลน์จึงอาจมีความเสี่ยงต่อการถูกโจรกรรมข้อมูลโดยบุคคลอื่นทำการเจาะฐานข้อมูล จึงเป็นกรณีที่น่าศึกษาว่ามาตรการการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยนั้นมีความปลอดภัย และมีหลักการป้องกันอย่างไร

ประเด็นปัญหาที่สอง ปัญหาความรับผิดเมื่อข้อมูลส่วนบุคคลของผู้ป่วยถูกละเมิด

ปัจจุบันการจัดเก็บข้อมูลของผู้ป่วยของโรงพยาบาลจะอยู่ในรูปแบบเวชระเบียนอิเล็กทรอนิกส์ ซึ่งมีความรวดเร็วในการบันทึก สืบค้น หรือใช้ข้อมูล เมื่อผู้ป่วยทำการแจ้งข้อมูลส่วนบุคคลแก่ทางเจ้าหน้าที่ของโรงพยาบาล เพื่อขึ้นทะเบียนผู้ป่วยและรับการรักษา เมื่อข้อมูลของ

ผู้ป่วยถูกจัดเก็บไว้ในระบบอิเล็กทรอนิกส์ หากมีบุคคลอื่นซึ่งไม่ใช้ผู้ป่วยเจ้าของข้อมูลเข้าถึงข้อมูลดังกล่าว ซึ่งมีชื่อ-นามสกุล ประวัติส่วนตัว ประวัติการรักษา อันเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถูกบุคคลภายนอกเข้าออกไปจากระบบความดูแลของของโรงพยาบาล ไม่ว่าจะเพื่อนำข้อมูลออกไปด้วยประการใด การกระทำนั้นถือว่าเป็นการทำละเมิดต่อเจ้าของ จึงเป็นที่ต้องพิเคราะห์ว่าเมื่อข้อมูลของผู้ป่วยถูกเข้าถึง หรือนำออกโดยบุคคลอื่น เป็นความรับผิดฐานละเมิดหรือไม่ และใครต้องรับผิดต่อการทำให้การละเมิดต่อผู้ป่วยซึ่งได้รับความเสียหาย

จากที่นำเสนอมาทั้งหมดนี้ จึงเห็นได้ว่า เมื่อข้อมูลส่วนบุคคลของผู้ป่วยถูกจัดเก็บไว้ในระบบเวชระเบียนอิเล็กทรอนิกส์ ซึ่งเป็นระบบอิเล็กทรอนิกส์ในการเก็บบันทึก รวบรวม ประวัติส่วนตัวของผู้ป่วย และประวัติการรักษาที่เป็นข้อมูลที่มีความละเอียดไม่อาจเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากจะสร้างความเสียต่อเจ้าของข้อมูลนั้น ไม่ว่าด้วยประการใด ๆ การกระทำอันเป็นการเข้าสู่ฐานข้อมูลซึ่งเก็บรักษาข้อมูลของผู้ป่วย และอยู่ในความควบคุมดูแลของโรงพยาบาลโดยผิดกฎหมาย

ดังนั้น เมื่อข้อมูลส่วนบุคคลของผู้ป่วย ถูกเข้าถึงโดยบุคคลภายนอกซึ่งไม่ได้ผู้ควบคุมดูแล และเข้าสู้ระบบโดยผิดกฎหมาย ถือว่าเป็นการกระทำละเมิดต่อเจ้าของข้อมูลซึ่งได้รับความเสียหายไม่ และความรับผิดเมื่อข้อมูลของผู้ป่วยถูกเข้าถึงใครเป็นผู้รับผิดชอบในกรณีดังกล่าวนี้ระหว่างแพทย์ และเจ้าหน้าที่ซึ่งเป็นผู้ควบคุมดูแลข้อมูล หรือโรงพยาบาล ซึ่งมีแพทย์ และเจ้าหน้าที่ปฏิบัติหน้าที่ตามคำสั่ง

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาวิวัฒนาการ แนวคิด และทฤษฎีเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์เพื่อความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

2. เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยในต่างประเทศและประเทศไทย

3. เพื่อศึกษาวิเคราะห์กฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ และความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยของต่างประเทศ

4. เพื่อเสนอแนะมาตรการทางกฎหมายที่เหมาะสมเพื่อนำไปใช้เป็นแนวทางในการ นำไปสู่ข้อเสนอแนะ หรือปรับปรุง/แก้ไขกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

1.3 สมมติฐาน

การใช้เทคโนโลยีทางการแพทย์ และการรักษาความลับของผู้ป่วย ซึ่งมีการจัดเก็บข้อมูลของผู้ป่วยโดยเวชระเบียนอิเล็กทรอนิกส์ และการส่งผ่านข้อมูลต่าง ๆ รวมถึงข้อมูลส่วนตัวของผู้ป่วยซึ่งต้องมีการแจ้งต่อเจ้าหน้าที่ของโรงพยาบาลหรือบุคลากรทางการแพทย์ โดยข้อมูลผู้ป่วยนั้นจะบันทึกข้อมูลส่วนตัว ข้อมูลการรับการรักษา ประเภทการรักษา โรค และอื่น ๆ อันเป็นข้อมูลสำคัญของผู้ป่วยที่ไม่ควรเปิดเผย เข้าสู่ระบบของโรงพยาบาลและมีการเก็บรักษา และส่งข้อมูลของผู้ป่วยให้แพทย์ที่ต้องทำการรักษา และเมื่อมีการใช้เทคโนโลยีทางการแพทย์ก็จะมีการเก็บข้อมูลของผู้ป่วยเข้าสู่ฐานระบบต่อไป ดังนั้น เมื่อมีการเข้าถึงข้อมูลของผู้ป่วยโดยไม่มีสิทธิและเผยแพร่ออกมาทั้งที่อยู่ในความดูแลของโรงพยาบาล และแพทย์ จึงเป็นกรณีที่ความรับผิดเกี่ยวกับข้อมูลของผู้ป่วยถูกเปิดเผยนั้น จำเป็นต้องอยู่ในความรับผิดของโรงพยาบาลหรือแพทย์ จึงจำเป็นอย่างยิ่งที่ต้องมีหลักเกณฑ์และวิธีการที่เหมาะสมกับสภาพปัญหาที่เกิดขึ้น เพื่อทำให้การคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยเป็นไปอย่างมีประสิทธิภาพ

1.4 ขอบเขตของการศึกษา

การศึกษาค้นคว้าทำวิทยานิพนธ์ เรื่อง มาตรการทางกฎหมายเกี่ยวกับควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ กรณีความคุ้มครองในข้อมูลส่วนบุคคลของผู้ป่วยที่เข้ารับบริการทางการแพทย์ โดยการรักษาของผู้ป่วยที่ใช้บริการทางการแพทย์จะมีการส่งข้อมูลที่มีการเชื่อมต่อในระบบอิเล็กทรอนิกส์ที่มีการส่งผ่านข้อมูลด้วยความรวดเร็ว และสามารถเข้าถึงได้สะดวกโดยทำการศึกษาเฉพาะกรณี จากกฎหมายของต่างประเทศ และกฎหมายที่มีอยู่ในประเทศไทยซึ่งเกี่ยวข้องหรือเทียบเคียงเกี่ยวกับมาตรการทางกฎหมายในคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย และศึกษาจากปัญหาที่จะเกิดจากการใช้เทคโนโลยีทางการแพทย์ และกฎหมายเทียบเคียงต่าง ๆ ที่เกี่ยวข้อง

1.5 วิธีดำเนินการศึกษา

ทำการศึกษาวิจัยเอกสาร (Documentary Research)โดยการรวบรวมและค้นคว้าหนังสือ ตำรากฎหมาย งานวิจัย บทความทางวิชาการที่เกี่ยวกับมาตรฐานการใช้กฎหมายควบคุมการใช้เทคโนโลยีทางการแพทย์ที่นำมาใช้ในการรักษาผู้ป่วย รวมถึงการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยที่ใช้บริการเทคโนโลยีทางการแพทย์นั้น แล้วนำมาวิเคราะห์ข้อมูลจากกฎหมายทั้งของต่างประเทศและประเทศไทย เพื่อนำมาวิเคราะห์ให้ได้มาซึ่งข้อสรุปและแนวทางในการใช้กฎหมาย

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงวิวัฒนาการ แนวคิด และทฤษฎีเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์เพื่อความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

2. ทำให้ทราบถึงกฎหมายต่างประเทศที่เกี่ยวกับมาตรการทางกฎหมายในการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ และคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

3. ทำให้ทราบถึงกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ และความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยของต่างประเทศ

4. ทำให้ทราบแนวทางมาตรการทางกฎหมายเพื่อปรับปรุง/แก้ไข กรณีคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย

1.7 นิยามศัพท์

1. ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6 ให้คำนิยามศัพท์

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทาให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดาเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคาสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดาเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้คำนิยาม “ข้อมูลส่วนบุคคล”

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับกำรเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2. พระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. 2545 ได้นิยามศัพท์ ดังนี้

“บริการสาธารณสุข” หมายความว่า บริการด้านการแพทย์และสาธารณสุขซึ่งให้โดยตรงแก่บุคคลเพื่อการสร้างเสริมสุขภาพ การป้องกันโรค การตรวจวินิจฉัยโรค การรักษาพยาบาลและการฟื้นฟูสมรรถภาพ ที่จำเป็นต่อสุขภาพและการดำรงชีวิต ทั้งนี้ให้รวมถึงการบริการการแพทย์แผนไทยและการแพทย์ทางเลือกตามกฎหมายว่าด้วยการประกอบโรคศิลปะ

3. พระราชบัญญัติสถานพยาบาล พ.ศ. 2541 ให้คำนิยาม “สถานพยาบาล” และ “ผู้ป่วย” ดังนี้

“สถานพยาบาล” หมายความว่า สถานที่รวมตลอดถึงยานพาหนะซึ่งจัดไว้เพื่อการประกอบโรคศิลปะตามกฎหมายว่าด้วยการประกอบโรคศิลปะ การประกอบวิชาชีพเวชกรรมตามกฎหมายว่าด้วยวิชาชีพเวชกรรม การประกอบวิชาชีพการพยาบาลและการผดุงครรภ์ตามกฎหมายว่าด้วยวิชาชีพการพยาบาลและการผดุงครรภ์การประกอบวิชาชีพทันตกรรมตามกฎหมายว่าด้วยวิชาชีพทันตกรรม การประกอบวิชาชีพกายภาพบำบัดตามกฎหมายว่าด้วยวิชาชีพกายภาพบำบัดการประกอบวิชาชีพเทคนิคการแพทย์ตามกฎหมายว่าด้วยวิชาชีพเทคนิคการแพทย์การประกอบวิชาชีพการแพทย์แผนไทยและการประกอบวิชาชีพการแพทย์แผนไทยประยุกต์ตามกฎหมายว่าด้วยวิชาชีพการแพทย์แผนไทย หรือการประกอบวิชาชีพทางการแพทย์และสาธารณสุขอื่นตามกฎหมายว่าด้วยการนั้น ทั้งนี้โดยกระทำเป็นปกติธุระไม่ว่าจะได้รับประโยชน์ตอบแทนหรือไม่

“ผู้ป่วย” หมายความว่า ผู้ขอรับบริการในสถานพยาบาล

4. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ได้นิยามศัพท์ ดังนี้

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกากาหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563

5. ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ได้ให้คำนิยาม ดังนี้

“ข้อมูลด้านสุขภาพของบุคคล” หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อมูลด้านสุขภาพของบุคคลที่เป็นเอกสารหรือข้อความในรูปแบบอิเล็กทรอนิกส์

“ระเบียนสุขภาพ” หมายความว่า ทะเบียนหรือรายการ ข้อมูลด้านสุขภาพของบุคคลที่กระทรวงสาธารณสุข หน่วยงานทั้งภาครัฐและเอกชน นำมาเก็บ จัดการ ใช้และเปิดเผยเพื่อประโยชน์ของเจ้าของข้อมูลตามระเบียบน

“เจ้าของข้อมูล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลด้านสุขภาพ

“ผู้ควบคุมข้อมูล” หมายความว่า ส่วนราชการ หน่วยงาน โรงพยาบาล โรงพยาบาลส่งเสริมสุขภาพตำบล สถานีอนามัยในสังกัดกระทรวงสาธารณสุขและหมายความรวมถึงสถานพยาบาลตามพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ และหน่วยงานของรัฐอื่นที่ประสงค์เข้าร่วมใช้ข้อมูลด้านสุขภาพร่วมกับกระทรวงสาธารณสุขซึ่งเป็นผู้จัดทำ เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลด้านสุขภาพของบุคคล

6. Section 3 แห่ง Federal Data Protection Act ได้บัญญัติคำนิยามศัพท์ของคำดังกล่าวกล่าวไว้ว่า

“ข้อมูลส่วนบุคคล (Personal Data)” หมายความว่า ข้อมูลอันใดอันหนึ่งที่เกี่ยวกับเรื่องส่วนบุคคลของบุคคลธรรมดาบุคคลใดบุคคลหนึ่ง หรือบุคคลธรรมดาที่สามารถระบุตัวได้

“การจัดเก็บข้อมูล (Collection)” หมายความว่า การได้มาซึ่งข้อมูลจากผู้เป็นเจ้าของข้อมูล

“การเก็บรักษา (Storage)” หมายความว่า การเข้าถึง การบันทึก หรือการป้องกัน ข้อมูลส่วนบุคคลในที่จัดเก็บ เพื่อที่จะสามารถนำข้อมูลดังกล่าวไปประมวลผลหรือใช้อีกครั้ง

“การเปิดเผย (Communication)” หมายความหมายว่า การเปิดเผยข้อมูลส่วนบุคคลที่จัดเก็บให้แก่บุคคลที่ 3 ไม่ว่าในรูปแบบใดก็ตาม โดยวิธีการ a) ส่งผ่านข้อมูลไปยังบุคคลที่ 3 หรือ b) ส่งผ่านข้อมูลให้แก่บุคคลที่ 3 เพื่อสามารถตรวจสอบหรือนำข้อมูลกลับใช้ได้

7. Federal Data Protection Act 2018 (BDSG) (พ.ศ. 2561) หรือรัฐบัญญัติคุ้มครองข้อมูลของรัฐบาลกลาง Section 46 ได้นินามคำจำกัดความไว้ ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึงข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุหรือระบุตัวตนได้ (เจ้าของข้อมูล) บุคคลธรรมดาที่สามารถระบุตัวตนได้คือบุคคลที่สามารถระบุได้โดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งโดยการอ้างอิงถึงตัวระบุ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลตำแหน่ง ตัวระบุออนไลน์ หรือปัจจัยหนึ่งหรือหลายปัจจัยเฉพาะทางกายภาพ สรีรวิทยา อัตลักษณ์ทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลนั้น

“การประมวลผล” หมายถึงการดำเนินการหรือชุดของการดำเนินการใด ๆ ที่ดำเนินการกับข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ เช่น การรวบรวม การบันทึก การจัดระเบียบ โครงสร้าง การจัดเก็บ การปรับ การเปลี่ยนแปลง การค้นคืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ หรือการทำให้พร้อมใช้งาน การจัดตำแหน่ง การรวมกัน การจำกัด การลบ หรือการทำลาย

“ระบบการจัดเก็บ” หมายถึงชุดข้อมูลส่วนบุคคลที่มีโครงสร้างซึ่งสามารถเข้าถึงได้ตามเกณฑ์เฉพาะ ไม่ว่าจะเป็นแบบรวมศูนย์ กระจายอำนาจ หรือกระจายตามการทำงานหรือตามภูมิศาสตร์

“ผู้ควบคุม” หมายถึงบุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะ หน่วยงานหรือหน่วยงานอื่นใดซึ่งโดยลำพังหรือร่วมกับผู้อื่นเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผล” หมายถึงบุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะ หน่วยงานหรือหน่วยงานอื่น ๆ ที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุม

“ข้อมูลเกี่ยวกับสุขภาพ” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพร่างกายหรือจิตใจของบุคคลธรรมดา รวมถึงการให้บริการด้านสุขภาพ ซึ่งเปิดเผยข้อมูลเกี่ยวกับสถานะสุขภาพของบุคคลนั้น

8. Data Protection Act 1998 หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบุคคล ค.ศ. 1998 (พ.ศ. 2541) ของสหราชอาณาจักร ได้นิยามคำศัพท์ ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่เกี่ยวข้องกับตัวบุคคลธรรมดาที่มีชีวิตอยู่ผู้ซึ่งอาจสามารถถูกบ่งชี้ตัวบุคคลโดยอาศัย (1) ข้อมูลนั้นเอง หรือ (2) ข้อมูลนั้นเองประกอบกับข้อมูลอื่นที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูล ทั้งนี้ รวมถึงข้อมูลเกี่ยวกับการแสดงความคิดเห็นเกี่ยวกับตัวบุคคลธรรมดาและการแสดงเจตนาของผู้ควบคุมข้อมูลหรือบุคคลอื่นที่เกี่ยวกับบุคคลธรรมดานั้นด้วย[8]

9. นิยามศัพท์อื่น ๆ

1. เทคโนโลยีทางการแพทย์ หมายถึง วิทยาการที่เกี่ยวกับศิลปะในการนำเอาวิทยาศาสตร์ มาประยุกต์ใช้เพื่อให้เกิดประโยชน์ต่อมนุษย์ในด้านการแพทย์ เช่น การตรวจ การรักษาพยาบาล และการป้องกันโรค ด้วยวิธีการต่าง ๆ ได้แก่

1.1 การพัฒนาเครื่องมือและอุปกรณ์ โดยอาศัยความรู้ด้านวิศวกรรมเป็นหลักในการผลิตเครื่องมือและอุปกรณ์ต่าง เช่น

1.1.1 เพื่อการตรวจและวินิจฉัยโรค

1.1.2 เพื่อการรักษาพยาบาล

1.1.3 เพื่อการป้องกันโรค

---

[8] Data Protection Act 1998, Section 1 Personal data mean data which relate to a individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indications of the data controller or any other person in respect of the individual.

1.2. การพัฒนาเทคโนโลยีเพื่อการผลิตยา สาร หรือวิธีการที่ใช้ในทางการแพทย์ ในการพัฒนาบางครั้งต้องอาศัยเทคโนโลยี เทคนิค และวิธีการต่าง ๆ เช่น เทคโนโลยีชีวภาพ และเทคนิคทางด้านวิศวกรรม ได้แก่

- การพัฒนาวิธีการเพาะเลี้ยงเชื้อซึ่งเก็บตัวอย่างมาจากผู้ป่วย
- การสร้างเด็กหลอดแก้ว
- การหาสาเหตุและการรักษาโรคที่เกิดจากความบกพร่องทางพันธุกรรม
- อุตสาหกรรมการผลิตยา
- การผลิตเซรุ่ม
- การผลิตวัคซีนป้องกันโรค

2. ผู้ป่วย หมายถึง ผู้ที่เข้ารับการรักษาหรือผู้รับบริการด้วยการพยาบาล ได้จำแนกไว้เป็น 2 ประเภท คือ

2.1 ผู้ป่วยใน หมายถึง ผู้ที่ต้องเข้ารับการรักษาในโรงพยาบาลหรือสถานพยาบาลอย่างน้อย 6 – 8 ชั่วโมง หรือผู้ที่ต้องเสียค่าห้องและอาหารประจำวันในการเข้ารักษาในโรงพยาบาลและสถานพยาบาล

2.2 ผู้ป่วยนอก หมายถึง ผู้ที่รับการบริการหรือเวชภัณฑ์อันเนื่องมาจากการรักษาพยาบาลในแผนกผู้ป่วยนอกหรือในห้องรักษาฉุกเฉินของโรงพยาบาลและสถานพยาบาล หรือผู้ที่รับการศัลยกรรมผ่าตัดเล็ก (minor surgery) โดยไม่เป็นผู้ป่วยในตามนิยามผู้ป่วยใน

3. การรักษาพยาบาล คือการรักษาคนที่รู้สึกไม่สบายเพราะความเจ็บไข้ ความเจ็บป่วย ความบกพร่อง หรือผิดปกติทางจิตใจและแพทย์เห็นว่าจำเป็นต้องรักษา ให้กลับสู่สภาพปกติ มิฉะนั้นจะเกิดอันตรายต่อสุขภาพของผู้ป่วย

4. สถานพยาบาล หมายถึง สถานที่รวมตลอดถึงยานพาหนะที่มีเตียงรับคนไข้ไว้ค้างคืน ซึ่งจัดไว้เพื่อการประกอบโรคศิลปะ ตามกฎหมายว่าด้วยการควบคุมการประกอบโรคศิลปะ หรือซึ่งจัดไว้เพื่อการประกอบการกิจการอื่นด้วยการผ่าตัด ฉีดยา หรือด้วยการใช้กรรมวิธีอื่นซึ่งเป็นกรรมวิธีการประกอบโรคศิลปะ ทั้งนี้โดยกระทำเป็นปกติธุระไม่ว่าจะได้รับผลประโยชน์ตอบแทนหรือไม่ และเป็นสถานพยาบาลซึ่งได้รับอนุญาตให้ตั้ง และดำเนินการตามพระราชบัญญัติสถานพยาบาล พ.ศ. 2541 และสถานพยาบาลโพลีคลินิก ทั้งนี้ไม่รวมสถานพยาบาลซึ่งมีประกาศ

กระทรวงสาธารณสุขให้ได้รับการยกเว้นตามพระราชบัญญัติสถานพยาบาล พ.ศ. 2541 (สถานพยาบาลซึ่งได้รับการยกเว้น ได้แก่ สถานพยาบาลของรัฐบาล เทศบาล สภากาชาดไทย และสถานพยาบาลอื่น ตามประกาศของกระทรวงสาธารณสุข ซึ่งประกาศในราชกิจจานุเบกษา)

5. โรงพยาบาล หมายถึง สถานพยาบาลใด ๆ ซึ่งได้รับอนุญาตให้ตั้งและดำเนินการสถานพยาบาลตามพระราชบัญญัติสถานพยาบาล พ.ศ. 2541 เพื่อประกอบการรักษาพยาบาลคนไข้หรือผู้ป่วย ซึ่งมีเตียงรับคนไข้ไว้ค้างคืน และจัดให้มีการวินิจฉัยโรค การศัลยกรรม ผ่าตัดใหญ่ (major surgery) และให้บริการด้านพยาบาลเต็มเวลา

6. “โรค” หมายความว่า ความเจ็บป่วย การบาดเจ็บ ความผิดปกติของร่างกายหรือจิตใจและหมายความรวมถึงอาการที่เกิดจากภาวะดังกล่าวด้วย[9]

7. “การรักษาพยาบาล” คือ การรักษาคนที่รู้สึกไม่สบายเพราะความเจ็บไข้ ความเจ็บป่วยความบกพร่อง หรือผิดปกติทางจิตใจและแพทย์เห็นว่าจำเป็นต้องรักษา ให้กลับสู่สภาพปกติมิฉะนั้นจะเกิดอันตรายต่อสุขภาพของผู้ป่วย

[9] ข้อบังคับแพทยสภา ว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพเวชกรรม พ.ศ. 2549

บทที่ 2

วิวัฒนาการ แนวคิด และความหมายเกี่ยวกับข้อมูลส่วนบุคคลของผู้ป่วย

ข้อมูลส่วนบุคคลของผู้ป่วย คือ ข้อมูลที่ผู้ป่วยหรือผู้รับบริการทางการแพทย์ให้ไว้แก่โรงพยาบาล โดยมีการจัดเก็บไว้ในรูปแบบเวชระเบียนอิเล็กทรอนิกส์ โดยในบทนี้ผู้วิจัยจะนำเสนอวิวัฒนาการ แนวคิด และความหมายเกี่ยวเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย และที่เกี่ยวข้องกับสาธารณสุข และเทคโนโลยีทางการแพทย์

2.1 วิวัฒนาการทางสาธารณสุข

การรักษาตัวเป็นสิ่งที่มนุษย์ต่างรู้จัก และสามารถทำได้ตั้งแต่ในอดีตแล้ว ซึ่งเป็นสัญชาตญาณที่มีเพื่อความอยู่รอดของตัวมนุษย์เองที่ติดตัวมนุษย์มาตั้งแต่เกิดมา สาธารณสุขในยุคดั้งเดิมนั้น ส่วนมากเชื่อว่าโรคทั้งหลายเกิดจากปรากฏการณ์ตามธรรมชาติ การที่มนุษย์จะหายจากโรคภัยได้นั้นก็โดยการกราบไหว้บูชาสิ่งศักดิ์สิทธิ์ เป็นต้น

ในช่วงหลายศตวรรษที่ผ่านมา หลังการปฏิวัติอุตสาหกรรมในประเทศตะวันตก สังคม และวิถีการดำเนินชีวิตของมนุษย์ได้เปลี่ยนแปลงไปอย่างมาก การค้นพบและพัฒนาเทคโนโลยีทางการแพทย์และสาธารณสุข ตัวอย่างเช่น การค้นพบยาเพนิซิลิน การคิดค้นวัคซีนเพื่อป้องกันไข้ทรพิษ เป็นต้น ซึ่งนอกจากยาและวัคซีนแล้วนั้น หนึ่งในผลิตภัณฑ์ทางการแพทย์ที่มีความจำเป็นในการตรวจวินิจฉัย รักษา และฟื้นฟูสุขภาพ ก็คือ เครื่องมือและอุปกรณ์การแพทย์ (Medical Devices) โดยปัจจุบันเครื่องมือและอุปกรณ์การแพทย์ได้รับการพัฒนาให้มีความหลากหลายและมีความซับซ้อนมากยิ่งขึ้น ซึ่งประมาณการได้คร่าว ๆ ว่าเครื่องมือและอุปกรณ์การแพทย์ที่ถูกคิดค้นตั้งแต่อดีตจนถึงปัจจุบันมีจำนวนมากถึง 1,500,000 ชนิด แม้เครื่องมือแพทย์จะมีความหลากหลายและความซับซ้อนที่ต่างกัน หรือเป็นเครื่องมือที่มีประสิทธิภาพมากเพียงใด จำต้องมีการดูแล จัดการที่ดีและเหมาะสมเพื่อให้

เครื่องมือแพทย์มีประสิทธิภาพในการใช้งานมากที่สุดและเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นได้ ซึ่งยังขาดมาตรการการเฝ้าระวังเกี่ยวกับผลข้างเคียงจากการใช้เครื่องมือแพทย์ตลอดจนการจัดการที่เหมาะสมในการกำจัดสารเคมีที่เป็นส่วนประกอบในเครื่องมือแพทย์ที่ต้องใช้รักษาต่อเนื้อตัวร่างกายของผู้เข้ารับการรักษา

Dr. Arshad Altaf (Vanderbilt Institute for Global Health & Bridge Consultants Foundation, Pakistan) ได้กล่าวเกี่ยวกับเครื่องมือแพทย์ ไว้ว่า “ถึงแม้ว่าเครื่องมือแพทย์จะมีประโยชน์อย่างมากในการดูแลรักษาและช่วยเหลือชีวิตคนไข้ แต่เครื่องมือแพทย์ก็อาจก่อให้เกิดอันตายอย่างมากได้เช่นกัน หากมีการนำไปใช้อย่างไม่ถูกวิธีหรือมีการจัดการเครื่องมือแพทย์ที่ชำรุดอย่างไม่ถูกต้อง” ซึ่งเป็นถ้อยคำที่แสดงให้เห็นว่าแม้เครื่องมือจะมีประโยชน์อย่างไร แต่หากใช้ไม่ถูกต้องหรือไม่ได้รับการรักษาแล้วก็ก่อให้เกิดโทษได้เช่นกัน ตัวอย่างที่เห็นได้อย่างชัดเจนในเครื่องมือแพทย์ที่ก่อให้เกิดผลเสียกันมาก คือ การใช้เข็มฉีดยาอย่างไม่ปลอดภัย และพิษจากสารปรอทที่เป็นส่วนประกอบในการผลิตเครื่องมือแพทย์

โดยมีตัวอย่างจากสาธารณรัฐอิสลามปากีสถานที่เป็นหนึ่งในประทศที่มีการใช้เข็มฉีดยาอย่างไปลอดภัยซึ่งก่อให้เกิดการแพร่ระบาดของโรคติดต่อทางโลหิตอย่างมาก เช่น ไวรัสตับอักเสบบีและซี (Hepatitis B, C) หรือไวรัส HIV สาธารณรัฐอิสลามปากีสถานเป็นประเทศกำลังพัฒนาที่มีประชากรมากเป็นดับ 6 ของโลก และโรคไวรัสตับอักเสบบีและซีเป็นปัญหาสาธารณสุขที่สำคัญเป็นอันดับต้น ๆ ของประเทศ เนื่องจากเป็นประเทศที่ประชากรและบุคลากรทางการแพทย์มีค่านิยมในการฉีดยาเพื่อบรรเทาอาการเจ็บป่วยจากโรคต่าง ๆ ทำให้อัตราการฉีดยาของสาธารณรัฐอิสลามปากีสถานสูงถึง 13.6 ครั้งต่อประชากรหนึ่งคนใน 1 ปี และจากผลการสำรวจพบว่า ร้อยละ 93 ของหารฉีดยาในสถานบริการเอกชนเป็นการฉีดยาที่ไม่จำเป็น นอกจากนี้ ร้อยละ 75 - 94 มีการนำอุปกรณ์การฉีดยากลับมาใช้ซ้ำอีก ส่วนในสถานบริการของรัฐบาลมีถึง ร้อยละ 12 ที่นำเข็มฉีดยาหลับมาใช้ซ้ำ จึงเห็นได้ว่าการฉีดยาที่ไม่จำเป็นและการนำเข็มฉีดยากลับมาใช้ซ้ำเป็นสาเหตุที่สำคัญของการแพร่ระบาดของเชื้อไวรัสตับอักเสบบีและซี

จากผลการวิจัยปัจจัยเสี่ยงของการติดเชื้อไวรัสตับอักเสบบี ในเมืองการาจี พบว่าผู้ที่ฉีดยามากกว่า 1 ครั้งมีอัตราส่วนของโอกาส (Odds Ratio) ในการติดเชื้อไวรัสตับอักเสบบีเป็น 6.3 เท่า เมื่อเทียบกับผู้ที่ไม่ได้ฉีดยา และจากผลการวิจัยเรื่องปัจจัยเสี่ยงของการติดเชื้อไวรัสตับอักเสบซี ในเมืองอิสลามาบัด พบว่าผู้ที่ฉีดยามากกว่า 10 ครั้งขึ้นไปมีความเสี่ยงในการติดเชื้อไวรัสตับอักเสบซีมากกว่าผู้ที่ไม่ได้ฉีดยา 3.1 เท่า

นอกจากนี้จากการสำรวจในเมือง Sindh ในสถานบริการที่ไม่ได้มาตรฐานมีการนำเข็มฉีดยากลับมาใช้ใหม่สูงถึง ร้อยละ 50 หรือแม้แต่สถานบริการของรัฐก็ยังมีการนำเข็มฉีดยากลับมาใช้ใหม่ถึง ร้อยละ 30

จากข้อมูลข้างต้นนี้จึงทำให้ทางรัฐบาลปากีสถานตระหนักถึงอันตรายจากการฉีดยาที่ไม่ปลอดภัยจึงได้ตั้งหน่วยงานที่ชื่อว่า “Center of Injection Safety” ในปี ค.ศ. 2006 (พ.ศ. 2549) ซึ่งจากผลการดำเนินงานของหน่วยงานนี้ทำให้การฉีดยาในปากีสถานมีความปลอดภัยมากขึ้นแต่ยังพบว่าอัตราการฉีดยาที่ไม่ปลอดภัยยังคงสูงในหมู่แพทย์ที่เปิดคลินิกเป็นของตัวเองและในสถานพยาบาลที่ไม่ได้มาตรฐานโดยเฉพาะในพื้นที่ชนบท จากปัญหาที่ได้กล่าวมาทำให้รัฐบาลปากีสถานต้องดำเนินนโยบายใหม่ ๆ โดยมีการตั้ง Injection Safety Clinic เพื่อใช้เป็นโมเดลการฉีดยาที่ปลอดภัยแก่ประชาชน นอกจากนี้ยังร่วมกับองค์การอนามัยโลกในฝึกอบรมบุคลากรจากทุกพื้นที่ของประเทศให้มีความรู้เรื่องการฉีดยาที่ถูกต้องและปลอดภัย และที่สำคัญยังได้ผลักดันให้รัฐบาลออกกฎหมายลงผู้ที่ให้บริการฉีดยาที่ไม่ปลอดภัยเพื่อลดอัตราการแพร่เชื้อของโรคไวรัสตับอักเสบบีและซี และไวรัส HIV ซึ่งเป็นปัญหาทางสาธารณสุขที่สำคัญ

2.2 วิวัฒนาการและความหมายของเทคโนโลยีทางการแพทย์

เทคโนโลยีทางการแพทย์ หมายถึง วิทยาการที่เกี่ยวกับศิลปะในการนำเอาวิทยาศาสตร์มาประยุกต์ใช้เพื่อให้เกิดประโยชน์ต่อมนุษย์ในด้านการแพทย์ เช่น การตรวจ การรักษาพยาบาล และการป้องกันโรค ด้วยวิธีการต่าง ๆ ได้แก่

1. การพัฒนาเครื่องมือและอุปกรณ์ โดยอาศัยความรู้ด้านวิศวกรรมเป็นหลักในการผลิตเครื่องมือและอุปกรณ์ต่าง เช่น

1.1 เพื่อการตรวจและวินิจฉัยโรค

1.2 เพื่อการรักษาพยาบาล

1.3 เพื่อการป้องกันโรค

2. การพัฒนาเทคโนโลยีเพื่อการผลิตยา สาร หรือวิธีการที่ใช้ในทางการแพทย์ ในการพัฒนาบางครั้งต้องอาศัยเทคโนโลยี เทคนิค และวิธีการต่าง ๆ เช่น เทคโนโลยีชีวภาพ และเทคนิคทางด้านวิศวกรรม ได้แก่

- การพัฒนาวิธีการเพาะเลี้ยงเชื้อซึ่งเก็บตัวอย่างมาจากผู้ป่วย
- การสร้างเด็กหลอดแก้ว
- การหาสาเหตุและการรักษาโรคที่เกิดจากความบกพร่องทางพันธุกรรม
- อุตสาหกรรมการผลิตยา
- การผลิตเซรุ่ม
- การผลิตวัคซีนป้องกันโรค

องค์การอนามัยโลก[10] 2011 (World Health Organization 2011 (พ.ศ. 2554)) กล่าวถึงอุปกรณ์ทางการแพทย์ หมายถึง เทคโนโลยีที่มีการพิจารณากันทั่วไปว่าเป็นสำคัญหรือที่จำเป็นสำหรับการเฉพาะขั้นตอนการป้องกันการวินิจฉัยการรักษาหรือการดำเนินการฟื้นฟูสมรรถภาพในที่สุดสิ่งอำนวยความสะดวกในการดูแลสุขภาพ โดยในปัจจุบันมีอุปกรณ์ทางการแพทย์มากกว่า 10,000 ชนิดของอุปกรณ์ทางการแพทย์ที่มีอยู่การเลือกใช้ทางการแพทย์ที่เหมาะสมย่อมขึ้นอยู่กับความต้องการของท้องถิ่นภูมิภาคหรือระดับชาติ ปัจจัยที่ควรพิจารณา ได้แก่ ประเภทของสถานบริการด้านสุขภาพที่

[10] องค์การอนามัยโลก (World Health Organization : WHO) เป็นทบวงการชำนัญพิเศษของสหประชาชาติ รับผิดชอบการประสานงานด้านสาธารณสุขระหว่างประเทศ ก่อตั้งเมื่อ 7 เมษายน ค.ศ. 1948 (พ.ศ. 2491) มีสำนักงานใหญ่ตั้งอยู่ที่กรุงเจนีวา ประเทศสวิตเซอร์แลนด์และมีสำนักงานส่วนภูมิภาคตั้งอยู่อีกใน 6 เมือง ได้แก่ บราซาวีล, วอชิงตัน ดี.ซี., ไคโร, โคเปนเฮเกน, นิวเดลี และ มะนิลา

อุปกรณ์นั้นจะใช้กำลังการทำงานด้านสุขภาพที่มีอยู่และภาวะของโรค ประสบการณ์ในพื้นที่เฉพาะ ดังนั้นจึงเป็นไปไม่ได้ที่จะทำให้รายการของอุปกรณ์ทางการแพทย์หลักซึ่งมีความละเอียดถี่ถ้วน หรือในระดับสากลที่ใช้บังคับของสถานบริการสุขภาพที่อุปกรณ์นั้นจะใช้กำลังการทำงานด้านสุขภาพที่มีอยู่และภาระของโรคประสบการณ์ในพื้นที่เฉพาะ ดังนั้น จึงเป็นไปไม่ได้ที่จะทำให้รายการของอุปกรณ์ทางการแพทย์

2.3 ความหมายและแนวคิดเกี่ยวกับเครื่องมือแพทย์

คำว่า "เครื่องมือแพทย์" ให้หมายถึง เครื่องใช้ผลิตภัณฑ์หรือวัตถุที่มุ่งหมายสำหรับใช้ในการประกอบวิชาชีพทางการแพทย์ เป็นต้น[11]

พระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2531 มาตรา 3 ในพระราชบัญญัตินี้

"เครื่องมือแพทย์" หมายความว่า

(1) เครื่องใช้ ผลิตภัณฑ์ หรือวัตถุสำหรับใช้ในการประกอบวิชาชีพ เวชกรรม การประกอบวิชาชีพการพยาบาลและการผดุงครรภ์ การประกอบ โรคศิลปะ หรือการบำบัดโรคสัตว์ตามกฎหมายว่าด้วยการนั้น ๆ

(2) เครื่องใช้ ผลิตภัณฑ์ หรือวัตถุสำหรับใช้ให้เกิดผลแก่สุขภาพ โครงสร้างหรือการกระทำหน้าที่ใด ๆ ของร่างกายมนุษย์หรือสัตว์

(3) ส่วนประกอบ ส่วนควบ อุปกรณ์ หรือชิ้นส่วนของเครื่องใช้ ผลิตภัณฑ์ หรือวัตถุตาม (1) หรือ (2)

(4) เครื่องใช้ ผลิตภัณฑ์ หรือวัตถุอื่นที่รัฐมนตรีประกาศกำหนดใน ราชกิจจานุเบกษาว่าเป็นเครื่องมือแพทย์

พระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2551 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2562 มาตรา 4 ในพระราชบัญญัตินี้

“เครื่องมือแพทย์” หมายความว่า

---

[11] พระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2531

(1) เครื่องมือ เครื่องใช้ เครื่องกล วัตถุที่ใช้ใส่เข้าไปในร่างกายมนุษย์หรือสัตว์ น้ำยาที่ใช้ตรวจในห้องปฏิบัติการ ผลิตภัณฑ์ ซอฟต์แวร์หรือวัตถุอื่นใดที่ผู้ผลิตมุ่งหมายเฉพาะสำหรับใช้อย่างหนึ่งอย่างใดดังต่อไปนี้ ไม่ว่าจะใช้โดยลำพัง ใช้ร่วมกันหรือใช้ประกอบกับสิ่งอื่นใด

(ก) ประกอบโรคศิลปะ ประกอบวิชาชีพเวชกรรม ประกอบวิชาชีพการพยาบาลและการผดุงครรภ์ ประกอบวิชาชีพทันตกรรม ประกอบวิชาชีพเทคนิคการแพทย์ ประกอบวิชาชีพกายภาพบำบัด และประกอบวิชาชีพการสัตวแพทย์ตามกฎหมายว่าด้วยการนั้นหรือประกอบวิชาชีพทางการแพทย์และสาธารณสุขอื่นตามที่รัฐมนตรีประกาศกำหนด

(ข) วินิจฉัย ป้องกัน ติดตาม บำบัด บรรเทาหรือรักษาโรคของมนุษย์หรือสัตว์

(ค) วินิจฉัย ติดตาม บำบัด บรรเทา หรือรักษาการบาดเจ็บของมนุษย์หรือสัตว์

(ง) ตรวจสอบ ทดแทน แก้ไข ดัดแปลง พยุง ค้ำ หรือจุนด้านกายวิภาคหรือกระบวนการทางสรีระของร่างกายมนุษย์หรือสัตว์

(จ) ประคับประคองหรือช่วยชีวิตมนุษย์หรือสัตว์

(ฉ) คุมกำเนิด หรือช่วยการเจริญพันธุ์ของมนุษย์หรือสัตว์

(ช) ช่วยเหลือหรือช่วยชดเชยความทุพพลภาพหรือพิการของมนุษย์หรือสัตว์

(ซ) ให้ข้อมูลจากการตรวจสิ่งส่งตรวจจากร่างกายมนุษย์หรือสัตว์ เพื่อวัตถุประสงค์ทางการแพทย์หรือการวินิจฉัย

(ฌ) ทำลายหรือฆ่าเชื้อสำหรับเครื่องมือแพทย์

(2) อุปกรณ์ หรือส่วนประกอบของเครื่องมือ เครื่องใช้ เครื่องกล ผลิตภัณฑ์ หรือวัตถุตาม (1)

(3) เครื่องมือ เครื่องใช้ เครื่องกล ผลิตภัณฑ์ หรือวัตถุอื่นที่รัฐมนตรีประกาศกำหนดว่าเป็นเครื่องมือแพทย์

เครื่องมือทางการแพทย์ตามพระราชบัญญัติเครื่องมือแพทย์ทั้งสองฉบับข้างแสดงให้เห็นถึงการวิวัฒนาการทางด้านเครื่องมือทางการแพทย์ที่มีความเปลี่ยนแปลงไปตามยุคสมัย และเพื่อให้เท่าทันต่อโรคชนิดใหม่ หรือเชื้อแบบใหม่ ให้ทันท่วงทีต่อการรักษา

เครื่องมือแพทย์ในปัจจุบันมีให้เห็นมีอยู่ด้วยกันมากมายหลายชนิด และมีใช้กันอย่างแพร่หลาย ทั้งชนิดที่ใช้ง่ายเป็นที่รู้จักกันโดยทั่วไป ซึ่งสามารถหาซื้อได้ด้วยตนเอง เช่น พลาสเตอร์ ผ้าก๊อซ สำลี ไปจนถึงเครื่องมือแพทย์ที่มีขั้นตอนการใช้ที่ยุ่งยากสลับซับซ้อน และต้องอาศัยผู้เชี่ยวชาญหรือบุคลากรทางการแพทย์เป็นผู้ใช้ หรืออยู่ในความดูแลของแพทย์ เช่น เครื่อง Computer Tomography (CT)[12] เครื่อง Magnetic Resonance Imaging (MRI)[13] เป็นต้น การใช้เครื่องมือแพทย์ ไม่ว่าจะเป็นการซื้อใช้ด้วยตนเอง หรือการใช้ในความดูแลของบุคลากรทางการแพทย์ หากใช้โดยขาดความรู้ ความเข้าใจ นอกจากจะเสียเงินโดยไม่จำเป็นแล้ว ยังอาจก่อให้เกิดอันตรายต่อร่างกายได้

ตามความหมายที่ได้ระบุไว้ในพระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2531 เครื่องมือแพทย์ คือ เครื่องใช้ผลิตภัณฑ์หรือวัตถุสำหรับใช้ในการประกอบวิชาชีพเวชกรรม การประกอบวิชาชีพพยาบาล และการผดุงครรภ์ การประกอบโรคศิลปะหรือการบำบัดโรคสัตว์ หรือเครื่องใช้ให้เกิดผลแก่สุขภาพ โครงสร้างของร่างกายมนุษย์หรือสัตว์ รวมทั้งส่วนประกอบ ส่วนควบ อุปกรณ์ หรือชิ้นส่วนของเครื่องใช้ผลิตภัณฑ์ หรือวัตถุดังกล่าว นอกจากนั้นยังรวมถึงเครื่องใช้ ผลิตภัณฑ์ หรือวัตถุอื่น ที่รัฐมนตรีประกาศกำหนดใน ราชกิจจานุเบกษาว่าเป็นเครื่องมือแพทย์

---

[12] เป็นเครื่องมือที่ใช้สำหรับการถ่ายภาพรังสีส่วนตัดอาศัยคอมพิวเตอร์ เป็นเทคโนโลยีที่ใช้ภาพรังสีเอกซ์ที่อาศัยคอมพิวเตอร์ประมวลผลเพื่อสร้างภาพตัดขวาง (เหมือนกับว่า 'ถูกหั่นออกเป็นชิ้นบาง ๆ') เฉพาะจุดของวัตถุที่ทำการสแกนซึ่งช่วยให้ผู้ใช้สามารถเห็นภายในโดยไม่ต้องผ่าตัด ในการสร้างภาพสามมิติภายในของวัตถุจะใช้การประมวลผลรูปทรงเรขาคณิตด้วยดิจิตอลจากชุดใหญ่ของภาพเอ็กซ์เรย์สองมิติที่ถูกบันทึกรอบแกนหมุนแกนเดียว X-ray CT ที่พบมากที่สุดถูกนำมาใช้ในการถ่ายภาพทางการแพทย์. ภาพตัดขวางของมันถูกนำมาใช้เพื่อการวินิจฉัยและการรักษาทางการแพทย์ในสาขาต่าง ๆ

[13] เป็นเครื่องมือที่ใช้สำหรับการสร้างภาพด้วยเรโซแนนซ์แม่เหล็ก หรือ การตรวจเอ็กซ์เรย์ด้วยคลื่นแม่เหล็กไฟฟ้า คือเทคนิคการสร้างภาพทางการแพทย์ที่ใช้ในรังสีวิทยาเพื่อการตรวจทางกายวิภาคและสรีรวิทยาของร่างกายทั้งในด้านสุขภาพและโรคต่าง ๆ โดยเครื่องตรวจที่ใช้สนามแม่เหล็กและคลื่นวิทยุความเข้มสูงในการสร้างภาพเหมือนจริงของอวัยวะภายในต่าง ๆ ของร่างกาย โดยเฉพาะ สมอง หัวใจ กระดูก-กล้ามเนื้อ และส่วนที่เป็นมะเร็ง ด้วยคอมพิวเตอร์รายละเอียดและความคมชัดสูง เป็นภาพตามระนาบได้ทั้งแนวขวาง แนวยาวและแนวเฉียง เป็น 3 มิติ ภาพที่ได้จึงจะชัดเจนกว่า การถ่ายภาพรังสีส่วนตัดอาศัยคอมพิวเตอร์ หรือ CT Scan ทำให้แพทย์สามารถตรวจวินิจฉัยความผิดปกติในร่างกายได้อย่างแม่นยำ การตรวจทางการแพทย์ด้วยเครื่องมือชนิดนี้ไม่ก่อให้เกิดความเจ็บปวดใด ๆ แก่ร่างกาย และไม่มีอันตรายจากรังสีตกค้าง

เครื่องมือแพทย์นั้นแบ่งได้เป็น 4 ประเภทใหญ่ ๆ ด้วยกัน คือ

1. อุปกรณ์ผ่าตัด และอุปกรณ์การแพทย์ เช่น มีดผ่าตัด กรรไกรผ่าตัด เครื่องวัดความดัน ปรอทวัดไข้ เป็นต้น

2. บริภัณฑ์การแพทย์ เช่น เครื่องเอกซเรย์ เครื่องอัลตราซาวด์ เครื่องสลายนิ่ว เป็นต้น

3. วัสดุการแพทย์และวัสดุฝังในทางศัลยกรรม เช่น ถุงมือยางทางการแพทย์ ผ้าก๊อซ ซิลิโคน (Silicone)

4. เครื่องมือแพทย์เฉพาะทาง เช่น ชุดน้ำยาตรวจการติดเชื้อเอชไอวี (HIV) ชุดตรวจน้ำตาลในปัสสาวะ เครื่องมือทันตกรรม เป็นต้น

ประโยชน์ของเครื่องมือแพทย์เครื่องมือแพทย์ในกลุ่มนี้ เช่น

- เครื่องนวดกระแสไฟฟ้า ที่ใช้นวดเพื่อคลายความปวดเมื่อย

- ผลิตภัณฑ์แม่เหล็กสุขภาพ เพื่อใช้ในการเพิ่มการไหลเวียนของโลหิตและคลายการปวดเมื่อย

- เครื่องวัดความดันโลหิต ชนิดดิจิตอลเพื่อใช้วัดความดันโลหิต

- ชุดผลิตภัณฑ์ตรวจสภาวะบางอย่างของร่างกาย เช่น ชุดตรวจสอบน้ำตาลในปัสสาวะ ชุดตรวจสอบการตั้งครรภ์

จะเห็นได้ว่าผลิตภัณฑ์เครื่องมือแพทย์นั้นมีประโยชน์มากมาย มีวิวัฒนาการในการพัฒนาการใช้เพื่อให้มีประสิทธิภาพมากขึ้น มีประโยชน์ต่อวงการแพทย์และสาธารณสุขเป็นอันมาก แต่ขณะเดียวกัน ถ้านำไปใช้ไม่ถูกกับโรค ไม่ถูกกับอาการ หรือใช้โดยผิดวัตถุประสงค์ก็อาจทำให้เกิดอันตรายได้เช่นกัน แม้เครื่องมือทางการแพทย์จะมีประโยชน์ในการรักษาพยาบาลผู้ป่วยแต่เมื่อมีการนำมาใช้ก็ย่อมอาจก่อให้เกิดอันตรายจากเครื่องมือแพทย์ได้ ดังนี้

- เครื่องมือแพทย์ไม่มีประสิทธิภาพหรือความแม่นยำเพียงพอ อาจทำให้การวินิจฉัยผิดพลาดได้ เช่น หากชุดผลิตภัณฑ์ในการตรวจวินิจฉัยโรคเอดส์ ไม่มีประสิทธิภาพเพียงพอที่จะตรวจวินิจฉัยเลือดที่ได้รับบริจาคว่ามีเชื้อเอชไอวี หรือไม่ โดยอาจตรวจไม่พบ แต่เลือดที่ได้รับบริจาคมีเชื้ออยู่ก็ทำให้ผู้รับ บริจาคเลือดติดเชื้อไปด้วย

- เครื่องมือแพทย์ไม่ปลอดภัยในการใช้ เช่น ถุงซิลิโคนเสริมทรวงอก อาจเกิดการแตกขณะที่ยังอยู่ในร่างกาย ซึ่งซิลิโคนจะทำให้เกิดพังพืดขึ้นทำให้เป็นอันตรายได้

- เครื่องมือแพทย์ที่อาจก่อให้เกิดผลข้างเคียงอันไม่พึงประสงค์ เช่น เครื่องเอ็กซเรย์ยังใช้ในการวินิจฉัยโรคนั้น หากผู้ป่วยได้รับการฉายรังสีเอ็กซ์บ่อยครั้ง ก็อาจทำให้มีโอกาสเสี่ยงเป็นมะเร็งได้

- เครื่องมือแพทย์บางชนิด มีสารห้ามใช้ หรือข้อควรระวังในการใช้กับผู้ป่วยที่มีภาวะบางอย่าง เช่น เครื่องมือทางทันตกรรม ประเภทเครื่องขูดหินปูนจะไม่ใช้กับผู้ป่วยที่มีการติดตั้งเครื่องช่วยการเต้น ของหัวใจ (Pacemaker) เนื่องจากการทำงานของเครื่องขูดหินปูนจะรบกวนการทำงานของเครื่องดังกล่าว

ในปัจจุบันมีการจำหน่ายเครื่องมือแพทย์กันมากมายหลายประเภท ผู้บริโภคสามารถหาซื้อได้ ทั่วไป และยังมีการส่งเสริมการขายโดยการโฆษณาผ่านสื่อต่าง ๆ ซึ่งการโฆษณาเครื่องมือแพทย์หลายชนิดมีการโฆษณาโอ้อวดเกินจริง เช่น เครื่องออกกำลังโดยการแกว่งขา เครื่องนวด เครื่องสั่นสะเทือน อุปกรณ์แม่เหล็กต่าง ๆ ซึ่งการโฆษณาที่เกินจริงนี้อาจทำให้ผู้บริโภคหลงเชื่อและซื้อหามาใช้ด้วยตนเอง ทำให้อาจเกิดอันตรายได้ หากมีโรคหรือความผิดปกติของร่างกายที่ไม่ควรใช้เครื่องมือแพทย์หรืออุปกรณ์นั้น

2.4 ความปลอดภัยของการใช้เครื่องมือแพทย์ [14]

ปัญหาเกี่ยวกับความไม่ปลอดภัยการใช้เครื่องมือแพทย์โดยหลักแล้วมีปัจจัยทางด้านมนุษย์ การพิจารณาทางด้านมนุษย์มีข้อพิจารณาอยู่ 3 ประการ

- สภาพแวดล้อม
- ลักษณะของผู้ใช้
- ลักษณะของ interface[15] หรือตัวประสานระหว่างเครื่องมือและผู้ใช้

---

[14] กันต์ธนัท รัถยาภานิธิชัยกุล, “Biomedical อุปกรณ์ทางการแพทย์”

[15] Interface (ตัวประสาน) หมายถึง การเชื่อมต่อระหว่าง คอมพิวเตอร์ ที่ถ่ายโอนข้อมูลจากกันและกันได้ แต่มักนำมาใช้ในความหมายของ user interface ที่แปลว่า การติดต่อประสานระหว่างเครื่องคอมพิวเตอร์กับผู้ใช้ เช่น

1. สภาพแวดล้อมของการใช้เครื่องมือ นั้นแปรผันได้มากและสามารถมีผลกระทบอย่างมากต่อการใช้เครื่องมือแพทย์ ซึ่งจะต้องใช้ปริมาณ ความคิด ความสนใจ และการจดจ่อของสิ่งนั้น ๆ เรียกว่าภาระงานทางด้านจิตใจ ซึ่งมีผลกระทบต่อผู้ใช้งานเครื่องมือ เช่น ในห้อง OR อาจมีสัญญาณเตือนหลายอย่างเกินไปของเครื่องมือ

2. ผู้ใช้เครื่องมือแพทย์ เครื่องมือที่ใช้ง่ายสำหรับคนหนึ่งในการใช้ให้มีความปลอดภัยและมีประสิทธิภาพอาจทำให้เกิดปัญหาได้สำหรับผู้อื่น ลักษณะต่าง ๆ ที่สำคัญของกลุ่มผู้ใช้เครื่องมือ คือ สุขภาพโดยทั่วไปและสภาพจิตใจ ความสามารถทางด้านสัมผัส และความรู้เกี่ยวกับการใช้งาน

3. Interface ของผู้ใช้เครื่องมือ การพิจารณาทางด้านวิศวกรรมของปัจจัยทางด้านมนุษย์เกี่ยวข้องโดยตรง Device User Interface ซึ่งหมายถึง ส่วนที่พบกันหรือส่วนที่ประกบกัน หรือส่วนที่ติดต่อกันระหว่างผู้ใช้กับเครื่องมือ และการตอบสนองของเครื่องมือต่อการกระทำของผู้ใช้ การออกแบบ User Interface ที่ดีนั้นจะช่วยเร่งให้มีการทำงานอย่างถูกต้องซึ่งจะต้องป้องกันการกระทำที่อาจทำให้เกิดอันตรายขึ้นได้[16]

2.5 การควบคุมเครื่องมือแพทย์ตามกฎหมาย

มีข้อกฎหมายแห่งพระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2551 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2562 ในส่วนสาระของการควบคุมเครื่องมือบัญญัติไว้ ดังนี้

มาตรา 48 เครื่องมือแพทย์ผิดมาตรฐาน หมายความว่า

(1) เครื่องมือแพทย์ที่มีคุณภาพหรือมาตรฐานไม่เป็นไปตามที่ได้รับอนุญาตหรือแจ้งรายการละเอียด

แป้นพิมพ์, “จอภาพ ต่างก็เป็นตัวประสานกับผู้ใช้ทั้งสิ้น,” https://www.online-english-thai-dictionary.com/?word=interface&d=1&m=0&p=1

[16] *เพิ่งอ้าง*.

(2) เครื่องมือแพทย์ที่มีมาตรฐานไม่เป็นไปตามมาตรา 6 (4) หรือที่มีมาตรฐานของภาชนะบรรจุไม่เป็นไปตามมาตรา 6 (6) เว้นแต่กรณี เป็นเครื่องมือแพทย์ที่ได้รับอนุญาตให้ผลิตเพื่อการส่งออกตามมาตรา 34

มาตรา 49 เครื่องมือแพทย์เสื่อมคุณภาพ หมายความว่า เครื่องมือแพทย์ที่แปรสภาพไปเป็นเครื่องมือแพทย์ผิดมาตรฐาน หรือเครื่องมือแพทย์ที่สิ้นอายุการใช้ตามที่แสดงไว้

มาตรา 50 เครื่องมือแพทย์ที่ไม่ปลอดภัยในการใช้ หมายความว่า เครื่องมือแพทย์ที่มีลักษณะดังต่อไปนี้

(1) เครื่องมือแพทย์ที่ใช้ได้ครั้งเดียว และผ่านการใช้ไปแล้ว

(2) เครื่องมือแพทย์ที่ผลิตหรือเก็บรักษาโดยไม่ถูกสุขลักษณะ

(3) เครื่องมือแพทย์ที่มีสิ่งอื่นแปลกปลอม หรือสิ่งที่น่าจะเป็นอันตรายแก่สุขภาพปนอยู่ด้วย

(4) เครื่องมือแพทย์ที่มีสารอันสลายได้รวมอยู่ด้วย และอาจทำให้เกิดพิษอันเป็นอันตรายแก่ผู้ใช้

(5) เครื่องมือแพทย์ที่มีคุณประโยชน์ไม่เป็นที่เชื่อถือ

(6) เครื่องมือแพทย์ที่ออกแบบหรือผลิตซึ่งหากนำไปใช้อาจเป็นผลให้เกิดอันตรายแก่ผู้ใช้

(7) เครื่องมือแพทย์ที่มีการแสดงฉลากหรือเอกสารกำกับไม่เป็นไปตามมาตรา 44 หรือมาตรา 45 ซึ่งอาจเป็นผลให้เกิดอันตรายแก่ผู้ใช้

เครื่องมือแพทย์สามารถแบ่งตามระดับการควบคุม ออกเป็น 3 ระดับ คือ

เครื่องมือแพทย์ที่ต้องมีใบอนุญาต จัดเป็นเครื่องมือแพทย์ที่อยู่ในระดับการควบคุมที่เข้มงวดที่สุด คือ เครื่องมือแพทย์ที่ต้องได้รับอนุญาตจากสำนักงานคณะกรรมการอาหารและยาก่อนจึงจะสามารถประกอบธุรกิจได้ ไม่ว่าจะเป็นการผลิต การนำเข้าจากต่างประเทศ หรือการขายเครื่องมือแพทย์ก็ตาม ทั้งนี้จะต้องมีการออกประกาศกระทรวงสาธารณสุข กำหนดประเภทชนิดคุณภาพมาตรฐานและข้อกำหนดต่าง ๆ ผลิตภัณฑ์ประเภทนี้ ได้แก่ ถุงยางอนามัย ถุงมือยาง สำหรับการตรวจโรค ถุงมือยางสำหรับการศัลยกรรม กระบอกฉีดยาผ่านผิวหนังปราศจากเชื้อ ชนิดใช้ได้ครั้งเดียว กระบอกฉีดยา

อินซูลินปราศจากเชื้อชนิดใช้ได้ครั้งเดียว ชุดตรวจการติดเชื้อเอชไอวี (HIV) เพื่อการตรวจวินิจฉัย เป็นต้น

เครื่องมือแพทย์ที่ต้องแจ้งรายละเอียด จัดเป็นเครื่องมือแพทย์ที่อยู่ในระดับการควบคุมที่เข้มงวดปานกลาง ซึ่งจะต้องมีการออกประกาศกระทรวงสาธารณสุขกำหนดผลิตภัณฑ์ และข้อกำหนดต่าง ๆ ของเครื่องมือแพทย์ที่จะควบคุม โดยมีลักษณะสำคัญในการดำเนินงาน คือ

1) มีการพิจารณารับแจ้งรายละเอียดต่าง ๆ เกี่ยวกับเครื่องมือแพทย์ ตามที่กฎหมายกำหนด

2) มีการตรวจสถานที่ประกอบธุรกิจ

3) มีการตรวจสอบฉลากและเอกสารกำกับเครื่องมือแพทย์

4) มีการพิจารณาตรวจสอบคำขอโฆษณา

5) มีการคืนสำเนาการรับแจ้งรายการละเอียดโดยไม่เสียค่าธรรมเนียมแต่อย่างใด ทั้งนี้ ไม่มีการกำหนดมาตรฐานผลิตภัณฑ์ ไม่มีการวิเคราะห์คุณภาพผลิตภัณฑ์ ผลิตภัณฑ์ประเภทนี้ เช่น ชุดตรวจการติดเชื้อเอชไอวี เพื่อวัตถุประสงค์อื่นที่มิใช่ เพื่อการตรวจวินิจฉัย (เพื่อการค้นคว้าและงานวิจัย) และอุปกรณ์หรือเครื่องใช้ เพื่อกายภาพบำบัด

เครื่องมือแพทย์ทั่วไป จัดเป็นเครื่องมือแพทย์ที่อยู่ในระดับการควบคุมที่เข้มงวดน้อยที่สุด เครื่องมือแพทย์กลุ่มนี้ไม่ต้องมีการออกประกาศกระทรวงสาธารณสุขเพื่อกำหนดผลิตภัณฑ์ที่จะต้องถูกควบคุมแต่อย่างใด แต่ก่อนที่จะนำเข้ามาจำหน่ายในประเทศไทยได้จะต้องนำหนังสือรับรองการขาย (Certificate of Free Sale) ของผลิตภัณฑ์ที่จะนำเข้าจากประเทศผู้ผลิตมาให้เจ้าหน้าที่กองควบคุมเครื่องมือแพทย์ สำนักงานคณะกรรมการอาหารและยาตรวจสอบความถูกต้อง และเมื่อมีการนำเข้าเครื่องมือแพทย์ดังกล่าวจะต้องแสดงหนังสือรับรองการขายที่ผ่านการตรวจสอบแล้วต่อเจ้าหน้าที่ ณ ด่านศุลกากร อย่างไรก็ดีก่อนที่จะทำการโฆษณาเครื่องมือแพทย์ทั่วไป ไม่ว่าจะเป็นกรณีนำเข้าจากต่างประเทศหรือผลิตในประเทศก็ตามจะต้องขออนุญาตโฆษณาก่อนดำเนินการได้ ผลิตภัณฑ์ประเภทนี้ได้แก่ เครื่องมือแพทย์ทั้งหมดที่อยู่นอกเหนือจากทั้ง 2 ประเภทข้างต้น เช่น เตียงผู้ป่วย เครื่องสลายนิ่ว เครื่องกรอฟัน ผ้าพันแผล เป็นต้น

การดำเนินการควบคุมดูแลผลิตภัณฑ์เครื่องมือแพทย์นั้นมีวิธีการที่ซับซ้อน และผ่านหลายขั้นตอน ทั้งก่อนออกสู่ท้องตลาด และหลังออกสู่ท้องตลาด มีการดำเนินการควบคุม กำกับดูแล โดยอาศัยกฎหมาย ระเบียบหลักเกณฑ์ข้อบังคับ ทั้งนี้ก็เพื่อให้ผู้บริโภคได้ใช้ผลิตภัณฑ์ที่สมประโยชน์ได้รับความปลอดภัย

2.6 ความปลอดภัยของผู้ป่วย

ความปลอดภัยของผู้ป่วยเป็นสิ่งที่มีความสำคัญทางการแพทย์เป็นอย่างมาก ไม่ว่าจะมีความเสี่ยงในการดูแลอนามัยของหญิงมีครรภ์ การใช้ยา รวมถึงคุณภาพทางการแพทย์อื่น ๆ

ความปลอดภัยของผู้ป่วยเป็นกฎระเบียบที่ค่อนข้างใหม่ข้อหนึ่งในสาขาการดูแลสุขภาพอันมุ่งเน้นไปยังการหาวิถีทางที่จะป้องกันความผิดพลาดในการรักษาพยาบาลซึ่งจะนำไปสู่เหตุการณ์ไม่พึงประสงค์ได้ หรือกล่าวในอีกนัยหนึ่ง คือ ความปลอดภัยของผู้ป่วยเป็นศาสตร์แห่งการกำจัดความเสี่ยงต่อสุขภาพของผู้ป่วยระหว่างที่ได้รับการรักษาพยาบาล

"สาเหตุที่ทำให้เกิดกฎระเบียบประการนี้ คือ ความปลอดภัยของผู้ป่วยนั้นเป็นศาสตร์แรกที่อยู่เบื้องหลังความพยายามที่จะสู้กับการติดเชื้อภายในโรงพยาบาล ก่อนที่ศาสตร์นี้จะเผยแพร่ไปในหลายทศวรรษที่ผ่านมา และยังเป็นศาสตร์แรกในแขนงเพื่อยับยั้งความผิดพลาดในการรักษาพยาบาล"

เมื่อกล่าวคำปฏิญาณฮิปโปคราเตสแล้ว แพทย์ได้สาบานว่าจะไม่ทำร้ายผู้ใดทั้งนั้น หากแต่ในปลายศตวรรษที่ 19 ดร.หลุยส์ ปาสเตอร์ ได้พิสูจน์ว่า เชื้อจุลินทรีย์เป็นต้นกำเนิดโรคติดต่อ และด้วยเหตุนั้นเอง บรรดานักวิทยาศาสตร์ต่างก็เข้าใจว่า แทนที่แพทย์จะช่วยรักษาผู้ป่วย กลับสามารถฆ่าผู้ป่วยได้ผ่านมือและเครื่องมือที่ล้างไม่ถูกวิธี ด่านแรกของกฎระเบียบความปลอดภัยของผู้ป่วยนั้นก็คือการรักษาสุขลักษณะและลดการแพร่กระจายเชื้อในโรงพยาบาล แนวความคิดนี้เป็นพื้นฐานโครงการ Cleaner Care is Safer Care (บริการปลอดภัยใส่ใจความสะอาด) โดยองค์การอนามัยโลก (WHO) แขนงใหม่ของกฎระเบียบนี้กระจ่างชัดต่อสาธารณชนเมื่อยุค 1980 - 1990 เมื่อมีรายงานหลายฉบับถูกเขียนขึ้นเกี่ยวกับความผิดพลาดทางระหว่างการรักษาพยาบาล เช่น การใช้ยาที่ผิดกับโรค การวินิจฉัยผิด หรือแม้กระทั่งการลืมเครื่องมือผ่าตัดไว้ในร่างกายผู้ป่วยระหว่างการผ่าตัด ความตระหนักถึงความผิดพลาด

จากการรักษาพยาบาลมีมากขึ้นในปี 1982 เมื่อมีรายการในช่อง ABC ชื่อ "The Deep Sleep" รายงานว่าในสหรัฐอเมริกา แต่ละปีมีผู้ป่วย 6,000 ราย ซึ่งเสียชีวิตลงหรือบาดเจ็บจากภาวะสมองตายเนื่องจากความผิดพลาดจากการให้ยาชา

ผลของการตระหนักที่เพิ่มขึ้นนี้ได้ช่วยส่งเสริมการพัฒนาแนวคิดความปลอดภัยของผู้ป่วยด้วยการกำจัดความผิดพลาดอันเกิดจากการรักษาพยาบาลโดยบุคลากรในโรงพยาบาลลง เพื่อลดความเสี่ยงในการติดเชื้อภายในโรงพยาบาลโดยยึดมาตรฐานสุขลักษณะที่ดีเอาไว้ ทั้งหมดทั้งมวลนี้ได้วางรากฐานให้กับโครงการ Safe Surgery Saves Lives การศึกษาวิจัยแสดงให้เห็นว่าจากยุค 1980 เป็นต้นมา ผู้ป่วย 1 ใน 10 ที่เข้ารับการรักษาในโรงพยาบาลมีอาการเจ็บป่วยจากความเสี่ยงที่สามารถป้องกันได้ และผู้ป่วยจำนวนระหว่าง 44,000 - 98,000 ราย ได้เสียชีวิตลงในสหรัฐอเมริกาทุก ๆ ปี เนื่องจากความผิดพลาดในการรักษาพยาบาลที่ป้องกันได้ ก่อนที่จะมีการตีพิมพ์งานวิจัยเหล่านี้ สาธารณชนเคยให้ความวางใจอย่างเต็มที่กับบุคลากรทางการแพทย์ ดังนั้น นี้ จึงเป็นเรื่องสำคัญที่เราต้องพึงระลึกว่า "เพราะเป็นมนุษย์จึงทำผิดพลาด" ซึ่งแพทย์ก็เช่นกันย่อมทำพลาดได้ นี่จึงเป็นสาเหตุที่ต้องมีมาตรการเพื่อที่จะช่วยบุคลากรทางการแพทย์ลดข้อผิดพลาดต่าง ๆ เหล่านั้น

2.7 มาตรฐานและข้อบังคับใช้สำหรับเทคโนโลยีทางการแพทย์

มาตรฐานที่ใช้ในการควบคุม ดูแล และเป็นข้อบังคับใช้สำหรับเครื่องมือและอุปกรณ์ทางการแพทย์มีมากมายในปัจจุบัน เพื่อความปลอดภัยของผู้ใช้ ผู้ได้รับบริการเครื่องมือทางการแพทย์ต่าง ๆ มีความเชื่อมั่น ไว้วางใจ ปลอดภัยในการใช้งานกับผลิตภัณฑ์เครื่องมือและอุปกรณ์การแพทย์ได้ในระดับสูงเพราะฉะนั้นองค์การที่ดูแลในส่วนของมาตรฐานต่าง ๆ ต่างก็ให้ความตระหนักในส่วนนี้เพื่อที่เครื่องมือแพทย์และอุปกรณ์ทางการแพทย์ที่ผลิตออกมาสู่ตลาด สู่โรงพยาบาล และผู้ใช้ ต้องเป็นเครื่องมือที่มีระบบมาตรฐานรับรองหรือแม้แต่โรงพยาบาลทั่วโลกก็ต้องมีมาตรฐานขององค์กรในการบริหารจัดการเครื่องมือแพทย์ให้เป็นมาตรฐานอยู่ตลอด เพื่อความปลอดภัยแก่ผู้ใช้ ยกตัวอย่างมาตรฐานของแต่ละองค์กรที่เกี่ยวข้องกับเครื่องมือแพทย์ เช่น

1. American National Standards Institute (ANSI) เป็นองค์กรสำคัญ ที่ให้การสนับสนุนการพัฒนามาตรฐานทางเทคโนโลยีของสหรัฐ ANSI ทำงานร่วมกับกลุ่มอุตสาหกรรม และเป็นสมาชิกของ International Organization for Standardization (ISO) มาตรฐานคอมพิวเตอร์ที่กำหนดมานานแล้วจาก ANSI ได้แก่ American Standard Code for Information Interchange (ASCII) และ Small Computer System Interface

2. Emergency Care Research Institute ; ECRI คือ องค์กรที่ไม่แสวงหากำไร โดยนำผลการวิจัยทางด้านวิทยาศาสตร์ประยุกต์มาใช้ในการค้นหาวิธีการดูแลผู้ป่วย อุปกรณ์ต่าง ๆ และยา ให้มีมาตรฐานดีที่สุด เพื่อช่วยให้ผู้ป่วยมีสุขภาพที่ดีขึ้น) การเรียกคืนผลิตภัณฑ์ของผู้ผลิต และการเตือนภัยและการปรับการบริการหรือสินค้าตามกฎหมาย

3. The Joint Commission International (JCI) อยู่ในการกำกับดูแลของ The Joint Commission ซึ่งเป็นสถาบันของสหรัฐอเมริกาที่ได้รับการยอมรับในระดับสากล เป็นองค์กรอิสระที่ไม่หวังผลกำไร ดำเนินงานมานานกว่า 75 ปี โดยมีวัตถุประสงค์เพื่อส่งเสริมการพัฒนาคุณภาพ และความปลอดภัยในการดูแลรักษาพยาบาลผู้ป่วยให้กับสถานพยาบาลต่าง ๆ ทั่วโลกอย่างต่อเนื่อง ด้วยการตรวจประเมินอย่างละเอียดถี่ถ้วน ตลอดจนให้การรับรองมาตรฐานคุณภาพแก่สถานพยาบาลที่มีคุณสมบัติเป็นไปตามข้อกำหนด

(1) รัฐบัญญัติระเบียบอุปกรณ์การแพทย์

รัฐบัญญัติระเบียบอุปกรณ์การแพทย์หรืออุปกรณ์ทางการแพทย์การแก้ไขปี 1976 (พ.ศ. 2519) ได้รับการแนะนำโดย 94 สภาคองเกรสของสหรัฐอเมริกา สมาชิกสภาคองเกรสของ พอลจีโรเจอร์ส และวุฒิสมาชิกเอ็ดเวิร์ดเคนเนดี้เมตร เป็นสปอนเซอร์ประธานของการแก้ไขอุปกรณ์ทางการ

แพทย์[17] ชื่อเรื่องการแก้ไข 21 ได้ลงนามในกฎหมาย 28 พฤษภาคม ค.ศ. 1976 (พ.ศ. 2519) โดย 38th ประธานาธิบดีสหรัฐอเมริกา Gerald R. Ford[18] (เจอรัลด์ อาร์ ฟอร์ด)

(2) บทบัญญัติของรัฐบัญญัติ

การจำแนกประเภทของอุปกรณ์การแพทย์ มีสามประเภทสำหรับอุปกรณ์การแพทย์ ได้แก่

- Class I – การควบคุมการทั่วไปสำหรับอุปกรณ์ที่ถือว่าเป็นความเสี่ยงต่ำสำหรับการใช้งานของมนุษย์

อุปกรณ์ทางการแพทย์ที่มีข้อมูลเพียงพอที่จะให้ความเชื่อมั่นที่เหมาะสมของความปลอดภัยและประสิทธิภาพของอุปกรณ์ อุปกรณ์ทางการแพทย์ไม่ได้ที่จะเป็นสำหรับการใช้งานในการสนับสนุนหรือค้ำจุนชีวิตมนุษย์สำหรับการใช้งานที่มีความสำคัญอย่างมากในการป้องกันการด้อยค่าของสุขภาพของมนุษย์และไม่ได้นำเสนอความเสี่ยงที่ไม่มีเหตุผลที่มีศักยภาพของการเจ็บป่วยหรือได้รับบาดเจ็บ

- Class II – มาตรฐานการปฏิบัติงานสำหรับอุปกรณ์ที่ถือว่าเป็นความเสี่ยงในระดับปานกลาง ที่ใช้สำหรับมนุษย์

อุปกรณ์ทางการแพทย์ที่มีข้อมูลไม่เพียงพอที่จะให้ความเชื่อมั่นที่เหมาะสมของความปลอดภัยและประสิทธิภาพของอุปกรณ์ อุปกรณ์ทางการแพทย์ที่ไม่สามารถจัดเป็นอุปกรณ์ชั้นผมเพราะการควบคุมที่ได้รับอนุญาตไม่เพียงพอที่จะให้ความเชื่อมั่นที่เหมาะสมของความปลอดภัยและประสิทธิภาพของอุปกรณ์ อุปกรณ์ทางการแพทย์ที่มีข้อมูลเพียงพอที่จะสร้างมาตรฐานการทำงานและมีความจำเป็นในการสร้างมาตรฐานการปฏิบัติงานสำหรับอุปกรณ์

- Class III - อนุมัติ Premarket สำหรับอุปกรณ์ที่ถือว่าเป็นความเสี่ยงสูงสำหรับการใช้งานของมนุษย์

---

[17] 94th U.S. Congress, “H.R.11124: Medical Device Amendments,” U.S. House of Representative Bill Summary & Status. Library of Congress THOMAS. Retrieved February 9, 2013(11 December 1975).

[18] Gerhard Peters, John T. Woolley. “Gerald R. Ford: “Statement on Signing the Medical Device Amendments of 1976,” The American Presidency Project. University of California - Santa Barbara, Retrieved 10 February 2013(28 May 1976).

อุปกรณ์ทางการแพทย์ที่ไม่สามารถจัดเป็นอุปกรณ์ชั้นฉันเนื่องจากข้อมูลไม่เพียงพอที่จะตรวจสอบว่าการควบคุมที่ได้รับอนุญาตมีเพียงพอที่จะให้ความเชื่อมั่นที่เหมาะสมของความปลอดภัยและประสิทธิภาพของอุปกรณ์ อุปกรณ์ทางการแพทย์ที่ไม่สามารถจัดเป็นอุปกรณ์ประเภท II เนื่องจากข้อมูลไม่เพียงพอสำหรับการจัดตั้งมาตรฐานในการปฏิบัติที่จะให้ความเชื่อมั่นที่เหมาะสมของความปลอดภัยและประสิทธิภาพของอุปกรณ์ของมัน อุปกรณ์ทางการแพทย์ที่จะเป็นสำหรับการใช้งานในการสนับสนุนหรือ ค้ำจุนชีวิตมนุษย์ที่มีความสำคัญอย่างมากในการป้องกันการด้อยค่าของสุขภาพของมนุษย์หรือนำเสนอ ความเสี่ยงที่ไม่มีเหตุผลที่มีศักยภาพของการเจ็บป่วยหรือได้รับบาดเจ็บคือการต้องอยู่ภายใต้การอนุมัติ Premarket เพื่อให้เชื่อมั่นอย่างสมเหตุสมผลของความปลอดภัยและ ประสิทธิผล

(3) การจัดประเภทสำหรับอุปกรณ์การแพทย์

- มีการจัดหมวดหมู่เพื่อตรวจสอบว่าอุปกรณ์ที่มีไว้สำหรับการใช้งานของมนุษย์ควรจะอยู่กับความต้องการของระดับ I - ควบคุมทั่วไป, ประเภท II – มาตรฐานการปฏิบัติงาน หรือระดับ III – อนุมัติ

- แผงการจัดหมวดหมู่เพื่อให้แจ้งให้ผู้ผลิตและผู้นำเข้าอุปกรณ์ทางการแพทย์ไว้สำหรับการใช้งานของมนุษย์

- ผู้ผลิตและผู้นำเข้าจะต้องเตรียมความพร้อมสำหรับการประยุกต์ใช้ข้อกำหนดดังกล่าวและรายงานอุปกรณ์ทางการแพทย์ที่มีไว้สำหรับการใช้งานของมนุษย์ที่ผลิตหรือนำเข้าโดยพวกเขา

- นัดหมายแผงต้องประกอบด้วยสมาชิกซึ่งมีความเชี่ยวชาญที่มีความหลากหลายอย่างเพียงพอในสาขาต่าง ๆ เช่นทางชีวภาพและกายภาพวิทยาศาสตร์การแพทย์คลินิกและการบริหารวิศวกรรมและวิชาชีพอื่น ๆ ที่เกี่ยวข้อง บุคคลซึ่งมีคุณสมบัติโดยการฝึกอบรมและประสบการณ์ในการประเมินความปลอดภัยและประสิทธิภาพของอุปกรณ์ทางการแพทย์หรือมีทักษะในการใช้ประสบการณ์ในการพัฒนา, การผลิตหรือการใช้อุปกรณ์ทางการแพทย์ เช่น

- บุคคลซึ่งอยู่ในการจ้างงานเต็มเวลาปกติของประเทศสหรัฐอเมริกาและมีส่วนร่วมในการบริหารงานตามพระราชบัญญัตินี้ไม่อาจจะเป็นสมาชิกคนหนึ่งของแผงจัดหมวดหมู่ใด ๆ อุปกรณ์ทางการแพทย์

ลักษณะทางเคมีของอุปกรณ์ทางการแพทย์ : จากทฤษฎีเพื่อการใช้งานจริง

ลักษณะทางเคมีจะกลายเป็นสำคัญมากขึ้นในโลกของอุปกรณ์ทางการแพทย์ในขั้นตอนต่าง ๆ ตลอดวงจรชีวิตของผลิตภัณฑ์ นามสกุลและความลึกของการตรวจสอบทางชีวภาพตามปกติจะมีการเชื่อมโยงโดยตรงกับระดับความเสี่ยงที่เกี่ยวข้องกับอุปกรณ์และนี้เป็นจริงสำหรับลักษณะทางเคมีได้เป็นอย่างดี อุปกรณ์ใหม่จะกลายเป็นความซับซ้อนมากขึ้นและดังนั้นจึงจำเป็นที่ผู้ผลิตมีความรู้กว้างขวางของอุปกรณ์

เมื่อการออกแบบอุปกรณ์ที่จะเสร็จสมบูรณ์และมันเป็นเวลาสำหรับขั้นตอนการประเมินความปลอดภัยที่สำคัญข้อมูลที่ได้รับจากการศึกษาลักษณะทางเคมีให้ข้อมูลที่สำคัญจะต้องมีการประเมินร่วมกับข้อมูลทางพิษวิทยาเพื่อตอบสนองกฎระเบียบระหว่างประเทศ ลักษณะนี้จะใช้รูปแบบของการศึกษาที่สกัดซึ่งเป็นข้อมูลที่มีความสำคัญต่อการกำหนดความปลอดภัยของอุปกรณ์สำหรับผู้ป่วย ข้อมูลการศึกษาที่สกัดได้รับการประเมินโดยทำตามวิธีการที่กำหนดใน ISO-10993-17 : 2002 Standard ("การประเมินผลทางชีวภาพของอุปกรณ์ทางการแพทย์ - ส่วนที่ 17 : การจัดตั้งของวงเงินที่อนุญาตสำหรับสารโลหะหนัก")

ลักษณะทางเคมีสามารถพิสูจน์ให้เป็นประโยชน์อย่างมากเมื่อมันมาถึงการจัดการการเปลี่ยนแปลง อุปกรณ์ที่ซับซ้อนมักจะได้รับผลกระทบจากการเปลี่ยนแปลงจากกระบวนการผลิตขั้นตอนการทำความสะอาดจากผู้ผลิต (Supplier) วัสดุในการขั้นตอนการฆ่าเชื้อ ในหลายกรณีลักษณะทางเคมีอย่างละเอียดอาจช่วยในการลดปริมาณของการทดสอบกันได้ทางชีวภาพที่จะดำเนินการตัวอย่างเช่นถ้าเปรียบเทียบของโปรไฟล์สกัดระหว่าง "เก่า" และ "ใหม่" อุปกรณ์ที่แสดงให้เห็นว่าไม่มีความแตกต่างที่เกี่ยวข้องหรือเทียบเท่าพิษ (เชื่อมโยงแนวคิด) แล้วคุณอาจจะไม่สามารถที่จะจำกัดความต้องการที่จะดำเนินการของชุดที่ลดลงของ Biocompatibility การทดสอบ

2.8 หลักความปลอดภัยทางการแพทย์

อุปกรณ์ทางการแพทย์ช่วยชีวิตปรับปรุงสุขภาพและคุณภาพชีวิตและมีความขาดไม่ได้สำหรับการป้องกันการวินิจฉัยการรักษาและการจัดการของทุกเงื่อนไขทางการแพทย์ โรค และคนพิการ อุปกรณ์ทางการแพทย์และโดยเฉพาะอย่างยิ่งอุปกรณ์อำนวยความสะดวกนอกจากนี้ยังมีที่สำคัญเพื่อการฟื้นฟูและเปิดใช้งานคนที่มีความพิการที่จะดำเนินการต่อไปฟังก์ชัน โดยไม่ต้องใช้อุปกรณ์ทางการแพทย์ประจำวิธีการทางการแพทย์จากแผลข้อเท้าแพลงเพื่อการวินิจฉัยเอชไอวี / เอดส์ หรือการปลูกฝังสะโพกจะเป็นไปไม่ได้

แม้ว่าจะเป็นส่วนประกอบที่สำคัญของสุขภาพการดูแลอุปกรณ์ทางการแพทย์ที่มีประสิทธิภาพมากที่สุดเมื่อพิจารณาในบริบทที่กว้างขึ้นของแพคเกจการดูแลสุขภาพที่สมบูรณ์จำเป็นที่จะต้องตอบสนองความต้องการด้านสุขภาพของประชาชน:การป้องกันการดูแลทางคลินิก (การตรวจสอบการวินิจฉัยการรักษาและการจัดการติดตามและการฟื้นฟูสมรรถภาพ) และการเข้าถึงและการส่งมอบสุขภาพที่เหมาะสมการดูแล ยกตัวอย่าง เช่น วางเข็มฉีดยาที่ใช้แล้วทิ้ง และเข็มสนับสนุนหลักประกันสุขภาพถ้วนหน้าความปลอดภัยและความสะดวกในการใช้งานของพวกเขาทำให้คนแรกทฤษฎีของประชาชนเป็นศูนย์กลางการดูแลสุขภาพเบื้องต้น ประชาชนยังแข็งแกร่งนโยบายด้านสุขภาพที่มีความจำเป็นเพื่อให้แน่ใจว่าใช้และการกำจัดความปลอดภัยของอุปกรณ์เหล่านี้และเพื่อให้แน่ใจว่าการกำกับดูแลสุขภาพส่วนร่วมของชุมชน

อุปกรณ์ทางการแพทย์ที่จะต้องมีความเหมาะสมสำหรับบริบทหรือการตั้งค่าในสิ่งที่มันเป็นตั้งใจว่า บริบทในความหมายนี้หมายถึงการเชื่อมโยงอุปกรณ์ทางการแพทย์ที่ถูกต้องด้วยจำเป็นต้องมีสุขภาพที่สอดคล้องกับการเพิ่มประสิทธิผล ดังนั้นเมื่อความพยายามเพื่อให้การดูแลสุขภาพที่เป็นธรรมและความพร้อมการเข้าถึงความเหมาะสมและราคาไม่แพงควรได้รับการพิจารณาและแก้ไขในส่วนที่เกี่ยวข้องของสุขภาพแห่งชาตินโยบายเทคโนโลยี

ความปลอดภัยในการใช้เครื่องมือและอุปกรณ์ ทางการแพทย์ประเภทต่าง ๆ ในโรงพยาบาล (Safety for Using Type of Medical Equipment and Device in Hospital)

การป้องกันอันตรายจากการปฏิบัติงานในโรงพยาบาลสิ่งสำคัญผู้ใช้เครื่องมือแพทย์ในแต่ละโรงพยาบาล ต้องตระหนกและให้ความใส่ใจตั้งแต่การดูแล บำรุงรักษาเครื่องมือให้อยู่ในสภาพการใช้งานที่ปลอดภัย เข้าใจถึงจุดอันตรายของการใช้เครื่องและข้อควรระวังต่าง ๆ โดยเฉพาะอันตรายจากเครื่องมือและอุปกรณ์ทางการแพทย์ที่มีความเสี่ยงสูงต่อการใช้งานและสิ่งแวดล้อม

ความปลอดภัย[19] จากการใช้เครื่องมือและอุปกรณ์ทางการแพทย์ในและสถานบริการสุขภาพ นับวันจะมีความสำคัญต่อการให้บริการในโรงพยาบาลและสถานบริการสุขภาพมากขึ้น เพราะตั้งแต่กระบวนการจัดหา การติดตั้ง การใช้ และการบำรุงรักษา ซึ่งหากทุกคนที่มีส่วนเกี่ยวข้องตระหนักถึงความปลอดภัยที่อาจเกิดขึ้นในทุกขั้นตอน ย่อมเป็นหลักประกันได้ว่า โอกาสที่จะเกิดอันตรายทั้งต่อผู้ให้บริการและผู้รับบริการ ตลอดจนผู้คนทั่วไปมีน้อยมาก สิ่งสำคัญอีกอย่างหนึ่งคือการสริมสร้างความปลอดภัยความรู้ ที่เกี่ยวกับความปลอดภัยจากการใช้เครื่องมือแพทย์ อย่างถูกต้องและเข้าใจ สามารถประหยัดค่าใช้จ่ายที่อาจเกิดขึ้นจากการเกิดอุบัติเหตุได้อย่างแน่นอน และสามารถทำให้การตรวจรักษาสำเร็จเร็วขึ้นด้วย โดยทั่วไปหากปล่อยให้เกิดอันตรายในโรงพยาบาลแล้ว จะนำมาซึ่ง

1. การเจ็บพิการ หรือตาย
2. ทรัพย์สินเสียหาย
3. เสียเวลา
4. การให้บริการหยุดชะงัก
5. เจ้าหน้าที่เสียขวัญ
6. การเสียชื่อเสียง

---

[19] ความปลอดภัย (Safety) หมายถึง การปราศจากภัยซึ่งในทางปฏิบัติเป็นไปไม่ได้ที่จะขจัดภัย หรืออันตรายทุกชนิดให้หมดไป โดยสิ้นเชิงความปลอดภัยจึงให้รวมถึง การปราศจากอันตรายที่มีโอกาสจะเกิดขึ้นในทุก ๆ ด้าน และในทุกที่ภายในโรงพยาบาล

ส่วนสำคัญสามประการในการเสริมสร้างความปลอดภัยที่เป็นสากล คือ การรู้และเข้าใจถึงเทคโนโลยีของเครื่องมือแพทย์ ประการที่สองคือการรู้และเข้าใจถึงการใช้ การดูแลและบำรุงรักษา และประการสุดท้ายคือการกำหนดกฎระเบียบ ข้อบังคับ วิธีการใช้งานอย่างปลอดภัย ถึงแม้หลักการทั้งสามประการจะต้องดำเนินการไปพร้อม ๆ กัน จึงจะทำให้การเกิดอันตรายจากการใช้เครื่องมือแพทย์จึงจะมีประสิทธิภาพสูงสุด ในที่นี่จะเป็นการนำเสนอข้อกำหนดด้านความปลอดภัยเฉพาะด้านการใช้เครื่องมือแพทย์เท่านั้น เพื่อเสริมสร้างในสองประการแรกเป็นสำคัญ อันตราย[20] ที่เกิดในโรงพยาบาล โดยทั่วไปจะแบ่งได้ 9 กลุ่มหลัก คือ

1. อันตรายที่เกิดจากไฟฟ้า (Electrical Hazard)

ซึ่งโดยทั่วไปสามารถแบ่งสาเหตุของการเกิดอันตรายจากไฟฟ้าได้ 2 สาเหตุหลัก ๆ คือ ไฟฟ้าลัดวงจร (Short Circuit) และไฟฟ้าดูด (Electric Shock)

1.1 ไฟฟ้าลัดวงจร (Short Circuit) หมายถึงกระแสไฟฟ้าไหลครบวงจรโดยไม่ผ่านโหลดหรือไม่ผ่านเครื่องใช้ไฟฟ้า กระแสที่ลัดวงจรนี้มีกระแสไหลในปริมาณสูงมาก ประกายไฟและความร้อนจะทำให้เกิดการหลอมละลายของฉนวนไฟฟ้าและส่งผลให้สายตัวนำไฟฟ้าสัมผัสกัน เกิดเป็นประกายไฟฟ้า และทำให้ฉนวน ที่หลอมละลายลุกไหม้ขึ้นมา ส่วนสายตัวนำที่สัมผัสหรือลัดวงจรกันนั้นก็จะเกิดการสะบัดตัว กระจายเปลวไฟที่กำลังลุก ไหม้ขยายวงออกไป หากมีวัสดุติดไฟอยู่ในบริเวณนั้นก็เสริมให้การลุกไหม้รุนแรงในกรณีหากเกิดขึ้นในบริเวณ ของโรงพยาบาล ที่เป็นโซนก๊าซติดไฟอาจจะทำให้เกิดการระเบิดขึ้นได้ทำความเสียหายแก่ทรัพย์สินและบุคคลได้ ซึ่งสาเหตุของการเกิดไฟฟ้าลัดวงจรพอสรุปได้ดังนี้

- การติดตั้งอุปกรณ์ที่ไม่ถูกต้องตามมาตรฐานและขาดความรับผิดชอบ
- เกิดจากการผลิตไม่ได้มาตรฐาน
- ฉนวนไฟฟ้าชำรุดและเสื่อมสภาพ อาจเนื่องมาจากอายุการใช้งานนาน และสภาพแวดล้อมมีความร้อนสูง

---

[20] อันตราย (Danger) หมายถึง ระดับความรุนแรงที่ต่อเนื่องมาจากคำว่า ภัยอันตรายจากภัย อาจมีระดับสูง หรือมากน้อยก็ได้ขึ้นอยู่กับมาตรการในการป้องกันของสถานที่นั้น ๆ

- การใช้งานที่ไม่ถูกต้อง เช่นการใช้งานเครื่องใช้ไฟฟ้าที่มีกระแสมากเกินกว่าที่สายไฟฟ้าจะรับได้ ซึ่งทำให้เกิดความร้อนและหลอมละลายจนเกิดลัดวงจรได้

1.2 ไฟฟ้าดูด (Electric Shock) หมายถึง กระแสไฟฟ้าไหลครบวงจรโดยผ่านร่างกายของบุคคลทำให้เกิดอันตรายแก่บุคคลนั้นได้ ซึ่งลักษณะการเกิดกระแสไฟฟ้าไหลผ่านร่างกายเกิดได้ 2 ลักษณะคือกระแสไฟฟ้าไหลผ่านร่างกาย

ซึ่งลักษณะร่างกายสัมผัสส่วนที่มีไฟฟ้า แบ่งได้ 2 แบบ

- สัมผัสโดยตรง (Direct Contact) คือการที่ส่วนหนึ่งส่วนใดของร่างกายสัมผัสไฟฟ้าโดยตรง เช่น สัมผัสสายไฟฟ้าที่รั่วจากการที่ฉนวนชำรุด

- สัมผัสโดยอ้อม (Indirect Contact) คือการที่ส่วนหนึ่งส่วนใดของร่างกายไปสัมผัสกับเครื่องใช้ไฟฟ้าหรือเครื่องมือที่มีกระแสไฟฟ้ารั่ว

2. อันตรายที่เกิดจากเครื่องจักรกล (Mechanical Hazard)

3. อันตรายที่เกิดจากเชื้อ/ชีวภาพ (Biological Hazard)

4. อันตรายที่เกิดจากสารเคมี (Chemicals Hazard)

5. อันตรายที่เกิดจากรังสี (Radiation Hazard)

รังสีที่มีต่อร่างกายของมนุษย์ นอกจากก่อให้เกิดอันตรายต่อเซลล์ที่ได้รับรังสีโดยตรงแล้วยังมีผลถ่ายทอดไปยังลูกหลานได้ หากเซลล์เหล่านั้นเป็นเซลล์ในระบบอวัยวะสืบพันธุ์ เมื่อเซลล์ได้รับรังสีจะทำให้เกิด Mitotic Delay หรือ Division Delay การแบ่งตัวของเซลล์จะช้าลง ขึ้นอยู่กับปริมาณรังสีที่ได้รับและระยะในวงจรชีวิตของเซลล์ เซลล์บางเซลล์อาจจะตายเพราะเกิด Chromosome Aberration

กลุ่มอาการจากรังสีสามารถแบ่งออกได้หลายลักษณะดังนี้คือ

2.1 ผลเฉียบพลันจากรังสี (Acute Radiation Effect) เป็นกลุ่มอาการซึ่งเกิดขึ้นเฉียบพลันอาจจะปรากฏขึ้นทันทีหลังได้รับรังสี หรือเกิดขึ้นภายใน 1-2 เดือนหลังได้รับรังสี

2.2 ผลเรื้อรังจากรังสี (Late Radiation Effect) เป็นกลุ่มอาการที่เกิดขึ้นหลังได้รับรังสีไปนานแล้ว อาจจะใช้เวลาเป็นปีหรือหลาย ๆ ปีขึ้นไป

2.3 รังสีขนาดที่ทำให้ตายได้ (Early Lethal Effect) เป็นผลเฉียบพลันจากรังสีขนาดที่ทำให้ตายได้ การตายอย่างเฉียบพลันเนื่องจากได้รับรังสีอาบทั้งตัวจะเกิดขึ้นช้าหรือเร็วขึ้นอยู่กับปริมาณรังสีที่ได้รับ อัตรารังสี อายุ เพศ สปีชีส์ ฯลฯ

6. อันตรายที่เกิดจากก๊าซทางการแพทย์ (Medical Gases Hazard)

ก๊าซเป็นสภาวะของสสารที่โมเลกุล อะตอม หรือ อิออน เคลื่อนที่ได้อย่างอิสระและเป็นสสารที่มีความหนาแน่นน้อยมาก จึงไม่มีรูปร่างที่แน่นอนเหมือนของแข็ง ไม่มีปริมาตรที่แน่นอนเหมือนของเหลวและของแข็ง แต่ก๊าซสามารถเข้าไปอยู่เต็มภาชนะที่บรรจุ คือ โมเลกุลของก๊าซเมื่อเข้าไปอยู่ในภาชนะใด ๆ แม้จะมีหนึ่งอะตอม สองอะตอม หนึ่งโมเลกุล สองโมเลกุล หรือหลายโมเลกุล ก็จะเคลื่อนที่ไปมาตลอดเวลา ทำให้เกิดการชนกันระหว่างโมเลกุลและการชนกับผนังภาชนะ การชนกันเหล่านี้ทำให้ก๊าซเกิดมีความดัน ซึ่งเป็นคุณสมบัติที่ทำให้มีความหนาแน่นเพิ่มมากขึ้นได้หลายเท่า โดยการเพิ่มความดันหรือลดอุณหภูมิ ก๊าซที่ถูกบีบอัดแล้วอาจอยู่ได้ทั้งในรูปของแข็ง ของเหลวและก๊าซ[21]

ประเภทของก๊าซทางการแพทย์สามารถแบ่งได้ตามความเป็นอันตราย (Categories of Medical Gases and their Associated Hazard)[22]

– ก๊าซถาวร (Permanent Gas) เป็นก๊าซที่เมื่อทำการบรรจุลงท่อจะมีสถานะเป็นก๊าซที่ทุก ๆ ระดับความดัน เช่น ออกซิเจน ฮีเลียม อากาศทางการแพทย์ (Medical Air) เป็นต้น

– ก๊าซเหลว (Liquefied Gas) เป็นก๊าซที่เมื่อทำการบรรจุภายใต้ความดันที่อุณหภูมิปกติมีสภาพเป็นของเหลวบางส่วน เช่น คาร์บอนไดออกไซด์ ไนทรัสออกไซด์ เป็นต้น

– ก๊าซเหลวเย็นยิ่งยวด (Cryogenic Liquid) เป็นก๊าซเหลวในภาชนะบรรจุภายใต้ความดันซึ่งเก็บไว้ที่อุณหภูมิต่ำกว่า –150 °C (เซลเซียส) จึงมีความเย็นอย่างมาก ก่อให้เกิดอันตรายต่อเนื้อเยื่อที่มี

---

[21] “ณัฐินี โมพันธุ์ และคณะสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ และสถาบันนวัตกรรมและพัฒนากระบวนการเรียนรู้มหาวิทยาลัยมหิดล.” สืบค้นเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ. 2557, จาก http://www.li.mahidol.ac.th/e–media/ap–chemistry2/gases/web/link/gases.htm.

[22] Learning and Development Department “BasicMedical GasSafety,” Salford Royal NHS Foundation Trust, January 2012.

ชีวิต ทำให้เกิดการไหม้อย่างรุนแรงได้ เช่น ออกซิเจนเหลว (Liquid Oxygen) ไนโตรเจนเหลว (Liquid Nitrogen) เป็นต้น

7. อันตรายที่เกิดจากของแหลมทิ่มตำ (Sharps Handling hazard)

8. อันตรายที่เกิดจากสิ่งแวดล้อม (Environmental hazard)

9. อันตรายที่เกิดจากไฟไหม้ (Fire hazard)

2.9 หลักสิทธิผู้ป่วย

คำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย เป็นคำประกาศที่เกิดจากความร่วมขององค์กรวิชาชีพ ทั้ง 6 คือ

1. แพทยสภา

2. สภาการพยาบาล

3. สภาเภสัชกรรม

4. ทันตแพทยสภา

5. สภาเทคนิคการแพทย์

6.สภากายภาพบำบัด

7. กระทรวงสาธารณสุข

ซึ่งมีวัตถุประสงค์เพื่อให้ผู้ป่วยได้รับประโยชน์สูงสุดและตระหนักถึงความสำคัญของการให้ความร่วมมือกับผู้ประกอบวิชาชีพด้านสุขภาพ

ภาพที่ 2.1 คำประกาศและข้อพึงปฏิบัติของผู้ป่วย

คำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย

เพื่อให้ผู้ป่วยได้รับประโยชน์สูงสุดจากกระบวนการ และตระหนักถึงความสำคัญของการให้ความร่วมมือกับผู้ประกอบวิชาชีพด้านสุขภาพ แพทยสภา สภาการพยาบาล สภาเภสัชกรรม ทันตแพทยสภา สภากายภาพบำบัด สภาเทคนิคการแพทย์ และคณะกรรมการการประกอบโรคศิลปะ จึงได้ร่วมกันออกประกาศรับรองสิทธิและข้อพึงปฏิบัติของผู้ป่วย ไว้ดังต่อไปนี้

ที่มา: กระทรวงสาธารณสุข ประกาศ ณ วันที่ 12 สิงหาคม พ.ศ. 2558

(1) คำประกาศและข้อพึงปฏิบัติของผู้ป่วย

เพื่อให้ผู้ป่วยได้รับประโยชน์สูงสุดจากกระบวนการ และตระหนักถึงความสำคัญของการให้ความร่วมมือกับผู้ประกอบวิชาชีพด้านสุขภาพ แพทยสภา สภาการพยาบาล สภาเภสัชกรรม ทันตแพทยสภา สภากายภาพบำบัด สภาเทคนิคการแพทย์และคณะกรรมการการประกอบโรคศิลปะ จึงได้ร่วมกันออกประกาศรับรองสิทธิและข้อพึงปฏิบัติของผู้ป่วย ไว้ดังต่อไปนี้

(2) สิทธิของผู้ป่วย

ข้อ 1. ผู้ป่วยทุกคนมีสิทธิขั้นพื้นฐานที่จะได้รับการรักษาพยาบาลและการดูแลด้านสุขภาพตามมาตรฐานวิชาชีพจากผู้ประกอบวิชาชีพด้านสุขภาพโดยไม่มีการเลือกปฏิบัติตามที่บัญญัติในรัฐธรรมนูญ

ข้อ 2. ผู้ป่วยที่ขอรับการรักษาพยาบาลมีสิทธิได้รับทราบข้อมูลที่เป็นจริงและเพียงพอเกี่ยวกับการเจ็บป่วย การตรวจ การรักษา ผลดีและผลเสียจากการตรวจการรักษาจากผู้ประกอบวิชาชีพด้านสุขภาพ ด้วยภาษาที่ผู้ป่วยสามารถเข้าใจได้ง่าย เพื่อให้ผู้ป่วยสามารถเลือกตัดสินใจในการยินยอมหรือไม่ยินยอมให้ผู้ประกอบวิชาชีพด้านสุขภาพปฏิบัติต่อตน เว้นแต่ในกรณีฉุกเฉินอันจำเป็นเร่งด่วนและเป็นอันตรายต่อชีวิต

ข้อ 3. ผู้ป่วยที่อยู่ในภาวะเสี่ยงอันตรายถึงชีวิตมีสิทธิได้รับการ ช่วยเหลือรีบด่วนจากผู้ประกอบวิชาชีพด้านสุขภาพโดยทันทีตามความจำเป็นแก่กรณี โดยไม่ต้องคำนึงว่าผู้ป่วยจะร้องขอความช่วยเหลือหรือไม่

ข้อ 4. ผู้ป่วยมีสิทธิได้รับทราบชื่อ สกุล และวิชาชีพของผู้ให้การ รักษาพยาบาลแก่ตนเพื่อคุ้มครองความปลอดภัยของตนเอง โดยเฉพาะอย่างยิ่งจากผู้ให้บริการซึ่งไม่มีคุณภาพเพียงพอ

ข้อ 5. ผู้ป่วยมีสิทธิขอความเห็นจากผู้ประกอบวิชาชีพด้านสุขภาพอื่นที่มิได้ เป็นผู้ให้การรักษาพยาบาลแก่ตน และมีสิทธิในการขอเปลี่ยนผู้ประกอบ วิชาชีพด้านสุขภาพหรือเปลี่ยนสถานพยาบาลได้ ทั้งนี้เป็นไปตาม หลักเกณฑ์ของสิทธิการรักษาของผู้ป่วยที่มีอยู่

ข้อ 6. ผู้ป่วยมีสิทธิได้รับการปกปิดข้อมูลของตนเอง เว้นแต่ผู้ป่วยจะให้ความยินยอมหรือเป็นการปฏิบัติตามหน้าที่ของผู้ประกอบวิชาชีพด้านสุขภาพ เพื่อประโยชน์โดยตรงของผู้ป่วยหรือตามกฎหมาย

ข้อ 7. ผู้ป่วยมีสิทธิได้รับทราบข้อมูลอย่างครบถ้วนในการตัดสินใจเข้าร่วมหรือถอนตัวจากการ เป็นผู้เข้าร่วมหรือผู้ถูกทดลองในการทำวิจัยของผู้ประกอบวิชาชีพด้านสุขภาพ เพื่อเป็นแนวทางปฏิบัติว่าความยินยอมจะต้องเป็นความยินยอมภายหลังจากที่ได้รับทราบข้อมูลต่าง ๆ อย่างครบถ้วน

แล้ว (Informed Consent) เช่นเดียวกับความยินยอมในการรับการ รักษาพยาบาล และแม้ว่าจะตัดสินใจยินยอมแล้วก็มีสิทธิที่จะเลิกได้ เพื่อคุ้มครองผู้ถูกทดลองให้ได้รับความปลอดภัย

ข้อ 8. ผู้ป่วยมีสิทธิได้รับทราบข้อมูลเกี่ยวกับการรักษาพยาบาลเฉพาะของตนที่ปรากฏในเวชระเบียนเมื่อร้องขอตามขั้นตอนของสถานพยาบาลนั้น ทั้งนี้ข้อมูลดังกล่าวต้องไม่เป็นการละเมิดสิทธิหรือข้อมูลข่าวสารส่วนบุคคลของผู้อื่น

ข้อ 9. บิดา มารดา หรือผู้แทนโดยชอบธรรม อาจใช้สิทธิแทนผู้ป่วยที่เป็นเด็กอายุยังไม่เกินสิบแปดปีบริบูรณ์ ผู้บกพร่องทางกายหรือจิตซึ่งไม่สามารถใช้สิทธิ ด้วยตนเองได้

(3) ข้อพึงปฏิบัติของผู้ป่วย

ข้อ1. สอบถามเพื่อทำความเข้าใจข้อมูลและความเสี่ยงที่อาจเกิดขึ้นก่อนลงนามให้ความยินยอม หรือไม่ยินยอมรับการตรวจวินิจฉัยหรือการรักษาพยาบาล

ข้อ 2. ให้ข้อมูลด้านสุขภาพและข้อเท็จจริงต่าง ๆ ทางการแพทย์ที่เป็นจริงและครบถ้วนแก่ผู้ประกอบวิชาชีพด้านสุขภาพในกระบวนการรักษาพยาบาล

ข้อ 3. ให้ความร่วมมือและปฏิบัติตัวตามคำแนะนำของผู้ประกอบวิชาชีพด้านสุขภาพเกี่ยวกับการรักษาพยาบาล ในกรณีที่ไม่สามารถปฏิบัติตามได้ให้แจ้งผู้ประกอบวิชาชีพด้านสุขภาพทราบ

ข้อ 4. ให้ความร่วมมือและปฏิบัติตามระเบียบข้อบังคับของสถานพยาบาล

ข้อ 5. ปฏิบัติต่อผู้ประกอบวิชาชีพ ผู้ป่วยรายอื่น รวมทั้งผู้ที่มาเยี่ยมเยียน ด้วยความสุภาพให้เกียรติและไม่กระทำสิ่งที่รบกวนผู้อื่น

ข้อ 6. แจ้งสิทธิการรักษาพยาบาลพร้อมหลักฐานที่ตนมีให้เจ้าหน้าที่ของสถานพยาบาลที่เกี่ยวข้องทราบ

ข้อ 7. ผู้ป่วยพึงรับทราบข้อเท็จจริงทางการแพทย์ ดังต่อไปนี้

7.1 ผู้ประกอบวิชาชีพด้านสุขภาพที่ได้ปฏิบัติหน้าที่ตามมาตรฐานและจริยธรรม ย่อมได้รับความคุ้มครองตามที่กฎหมายกำหนดและมีสิทธิได้รับความคุ้มครองจากการถูกกล่าวหาโดยไม่เป็นธรรม

7.2 การแพทย์ในที่นี้ หมายถึง การแพทย์แผนปัจจุบันซึ่งได้รับการพิสูจน์ทางวิทยาศาสตร์โดยองค์ความรู้ในขณะนั้นว่ามีประโยชน์มากกว่าโทษสำหรับผู้ป่วย

7.3 การแพทย์ไม่สามารถให้การวินิจฉัย ป้องกัน หรือรักษาให้หายได้ทุกโรคหรือทุกสภาวะ

7.4 การรักษาพยาบาลทุกชนิดมีความเสี่ยงที่จะเกิดผลอันไม่พึงประสงค์ได้นอกจากนี้ เหตุสุดวิสัยอาจเกิดขึ้นได้ แม้ผู้ประกอบวิชาชีพด้านสุขภาพจะใช้ความระมัดระวังอย่างเพียงพอ ตามภาวะวิสัยและพฤติการณ์ในการรักษาพยาบาลนั้น ๆ แล้ว

7.5 การตรวจเพื่อการคัดกรอง วินิจฉัย และติดตามการรักษาโรค อาจให้ผลที่คลาดเคลื่อนได้ด้วยข้อจำกัดของเทคโนโลยีที่ใช้ และปัจจัยแวดล้อมอื่น ๆ ที่ไม่สามารถควบคุมได้ตามมาตรฐานการปฏิบัติงาน

7.6 ผู้ประกอบวิชาชีพด้านสุขภาพมีสิทธิใช้ดุลพินิจในการเลือกกระบวนการรักษาพยาบาลตามหลักวิชาการทางการแพทย์ ตามความสามารถและข้อจำกัดตามภาวะวิสัยและพฤติการณ์ที่มีอยู่ รวมทั้งการปรึกษาหรือส่งต่อโดยคำนึงถึงสิทธิและประโยชน์โดยรวมของผู้ป่วย

7.7 เพื่อประโยชน์ต่อตัวผู้ป่วย ผู้ประกอบวิชาชีพด้านสุขภาพอาจให้คำแนะนำหรือส่งต่อผู้ป่วยให้ได้รับการรักษาตามความเหมาะสม ทั้งนี้ผู้ป่วยต้องไม่อยู่ในสภาวะฉุกเฉินอันจำเป็นเร่งด่วนและเป็นอันตรายต่อชีวิต

7.8 การปกปิดข้อมูลด้านสุขภาพ และข้อเท็จจริงต่าง ๆ ทางการแพทย์ของผู้ป่วยต่อผู้ประกอบวิชาชีพด้านสุขภาพ อาจส่งผลเสียต่อกระบวนการรักษาพยาบาล

7.9 ห้องฉุกเฉินของสถานพยาบาล ใช้สำหรับผู้ป่วยฉุกเฉินอันจำเป็นเร่งด่วนและเป็นอันตรายต่อชีวิต

2.10 หลักการควบคุมคุณภาพเครื่องมือทางการแพทย์

[23]เครื่องมือแพทย์เป็นผลิตภัณฑ์สุขภาพที่สำคัญชนิดหนึ่งภายใต้อุตสาหกรรมสาขาสุขภาพที่เป็นหนึ่งในอุตสาหกรรมสำคัญลำดับแรก (Priority Integration Sector) ที่อยู่ในเป้าหมายของการเข้าสู่ประชาคมเศรษฐกิจอาเซียน (ASEAN Economic Community หรือ AEC) ภายในปี พ.ศ. 2558 (ค.ศ. 2015) โดยมีคณะทำงานด้านผลิตภัณฑ์เครื่องมือแพทย์ (Medical Device Product Working Group หรือ MDPWG) เป็นองค์กรขับเคลื่อนที่ดำเนินการทำความตกลงด้านกฎระเบียบในการกำกับดูแลเครื่องมือแพทย์ระหว่างกลุ่มประเทศสมาชิกอาเซียนให้มีความสอดคล้องกัน โดยมีวัตถุประสงค์เพื่อลดอุปสรรคทางการค้าอันเนื่องมาจากมาตรการทางเทคนิคของกฎระเบียบที่แตกต่างกัน และเพื่อคุ้มครองหรือให้ความมั่นใจแก่ผู้บริโภคในคุณภาพ ประสิทธิภาพ และความปลอดภัยของเครื่องมือแพทย์ที่จำหน่ายในตลาดอาเซียน คณะทำงาน MDPWG ได้ตกลงร่วมกันให้มีข้อบังคับอาเซียนว่าด้วยเครื่องมือแพทย์ (ASEAN Medical Device Directive หรือ AMDD) ซึ่งจะมีผลผูกพันให้สมาชิกอาเซียนทุกประเทศต้องปฏิบัติตาม AMDD โดยการบังคับใช้ผ่านกฎหมายภายในของแต่ละประเทศสมาชิก

MDPWG ได้ถูกจัดตั้งขึ้นโดยคณะกรรมการที่ปรึกษาของอาเซียนด้านมาตรฐานและคุณภาพ (ASEAN Consultative Committee for Standards and Quality หรือ ACCSQ) ในการประชุม ACCSQ ครั้งที่ 24 ระหว่างวันที่ 3 - 4 สิงหาคม พ.ศ. 2547 และผ่านความเห็นชอบจากคณะเจ้าหน้าที่เศรษฐกิจ อาวุโส (Senior Economic Officials Meeting หรือ SEOM) ในการประชุมครั้งที่ 1/36 ระหว่างวันที่ 17-19 มกราคม พ.ศ. 2548 MDPWG ประกอบด้วยผู้แทนภาครัฐซึ่งเป็น Head Delegate ของประเทศสมาชิกอาเซียน และ Head Delegate ของประเทศสมาชิกจะแต่งตั้ง Delegates อีกไม่เกิน 3 คน จากภาครัฐหรือภาคเอกชนของประเทศสมาชิกก็ได้ ประเทศ สมาชิก 10 ประเทศ ได้แก่ บรูไนดารุสซาลาม กัมพูชา อินโดนีเซีย สาธารณรัฐประชาธิปไตยประชาชนลาว มาเลเซีย สหภาพพม่า ฟิลิปปินส์ สิงคโปร์ ไทย และเวียดนาม มีมาเลเซียภาครัฐ เป็นประธาน สิงคโปร์ภาครัฐเป็นประธานร่วมมีการ

---

[23] ยุวดี พัฒนวงศ์, “ความตกลงร่วมกันของกลุ่มประเทศสมาชิกอาเซียนด้านกฎระเบียบในการกำกับดูแลเครื่องมือแพทย์และข้อบังคับอาเซียนว่าด้วยเครื่องมือแพทย์ (ASEAN Harmonization on Medical Device and ASEAN Medical Device Directive),” FDA Journal : May-August 2012, น. 12 -13.

ประชุม MDPWG ครั้งแรกระหว่างวันที่ 3-4 มีนาคม พ.ศ. 2548 ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย และมีการประชุมอย่างต่อเนื่องปีละ 2 ครั้ง การประชุมครั้งล่าสุดคือ ครั้งที่ 15 ระหว่างวันที่ 26 - 27 เมษายน พ.ศ. 2555 ณ จังหวัดภูเก็ต ประเทศไทย MDPWG ได้จัดทำร่าง AMDD เสร็จแล้ว ซึ่งจะต้องผ่านกระบวนการรับฟังความคิดเห็นจากภาคส่วนที่เกี่ยวข้องในแต่ละประเทศสมาชิกต่อไป

หลักวิธีการปฏิบัติเพื่อความเป็นเลิศ (The Best Practice)

[24]หลักหรือวิธีการปฏิบัติเพื่อความเป็นเลิศ หรือที่เรียกว่า “The Best Practice” หมายถึง กระบวนการทางการค้า หรือการประกอบวิชาชีพที่เป็นที่ยอมรับโดยกำหนดเป็นเกณฑ์ให้ต้องยึดถือปฏิบัติเพื่อบรรลุความปรารถนาในที่สุด (“Communication or professional procedures that are accepted or prescribed as being correct or most effective”) กล่าวอีกนัยหนึ่งคือเทคนิค หรือวิธีการทำงานในเรื่องใด ๆ อย่างดีที่สุด หรือเป็นเทคนิควิธีการบริหารเพื่อบรรลุเป้าหมายสูงสุดที่ตั้งไว้หรือแนวการปฏิบัติหน้าที่ที่ได้รับมอบหมายอย่างดีที่สุด ยกตัวอย่างเช่น หลัก Best Practice ต้นแบบการพัฒนาคุณภาพให้บริการประชาชนจัดทำโดยสำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร.)

หลัก Best Practice นำมาใช้กับการปฏิบัติหน้าที่แพทย์หมายความว่าแพทย์จะต้องให้การรักษาผู้ป่วยอย่างดีที่สุดในทุกสถานการณ์อันนำไปสู่ความสำเร็จของการรักษา จนทำให้หลัก Best Practice กลายเป็น “มาตรฐานในทางการแพทย์” เช่นการให้การดูแลผู้ป่วยต่อมลูกหมากแพทย์จะต้องตัดสินใจอย่างดีที่สุดในการรักษาโรคต่อมลูกหมากโดยอาศัยความยินยอมของผู้ป่วยในขณะที่แพทย์ใช้มาตรฐานทางการแพทย์รักษาโรคอย่างดีที่สุดอาจมีการเปรียบเทียบการรักษาโรคเดียวกันกับแพทย์รายอื่นในสาขาเดียวกัน

---

[24] ดรสุธี อยู่สถาพร, “ความรับผิดตามกฎหมายของแพทย์ในการรักษาผู้ป่วยกับหลักวิธีปฏิบัติเพื่อเป็นเลิศทางการแพทย์,” Public Health & Health Laws Journal Vol. 1 January - April 2016, น. 144 - 145

2.11 การควบคุมดูแลเครื่องมือแพทย์[25]

เครื่องมือทางการแพทย์เป็นเทคโนโลยีที่มีความซับซ้อนและหลากหลายซึ่งเครื่องมือแพทย์บางชนิดอาจก่อให้เกิดอันตรายกับผู้ป่วย จึงมีการพัฒนากฎเพื่อควบคุมเครื่องมือแพทย์โดยแยกออกจากยา ในปี ค.ศ. 1992 (พ.ศ. 2535) ได้มีการก่อตั้ง Global Harmonization Task Force (GHTF) ซึ่งเป็นความร่วมมือในระดับนานาชาติ ได้แก่ ประเทศในทวีปยุโรป อเมริกา แคนาดา ออสเตรเลีย และญี่ปุ่น เพื่อควบคุม กำกับ ดูแล เครื่องมือแพทย์และในปี ค.ศ. 2003 องค์กรอนามัยโลกได้ออกกฎเพื่อควบคุมการใช้เครื่องมือแพทย์ (Medical Devices Regulation) โดยกล่าวถึงภาพรวมทั่วโลก และหลักการซึ่งเป็นแนวทางการควบคุมเครื่องมือแพทย์

กรณีศึกษากรอบการควบคุมเครื่องมือแพทย์ในประเทศออสเตรเลีย ประกอบด้วย 6 ส่วน ดังนี้

1) หลักการทั่วไป เช่น ประสิทธิผลและความปลอดภัย

2) กฎการจำแนกประเภทของเครื่องมือแพทย์ เช่น ระดับความเสี่ยงที่จะเกิดอันตรายต่อผู้ป่วย ตำแหน่งและระยะเวลาที่ใช้

3) การประเมินกระบวนการผลิตเครื่องมือแพทย์

4) มาตรฐานการใช้เครื่องมือแพทย์

5) ระบบการเฝ้าระวังและติดตามหลังวางจำหน่าย เช่น ระบบบริการหลังการขาย

6) สิทธิประโยชน์สำหรับผู้ป่วยในอนาคต

ระบบการควบคุมเครื่องมือแพทย์ที่มีประสิทธิภาพที่สามารถเพิ่มเข้าถึงการบริการ ซึ่งช่วยเพิ่มคุณภาพบริการความเหมาะสมในการใช้นั้น จะต้องมีความต่อเนื่องและความโปร่งใสมีการวัดผลและเป็นไปตามความต้องการของผู้ใช้โดยองค์กรที่มีหน้าที่ควบคุมและองค์กรที่มีหน้าที่ในการประเมินเทคโนโลยีด้านสุขภาพ ควรมีการแลกเปลี่ยนเรียนรู้ประสบการณ์ระหว่างประเทศร่วมกัน

---

[25] Dr.Ruth Lopert (Therapeutic Goods Administration, Australia), รายงานฉบับสมบูรณ์สรุปเนื้อหาการประชุมนานาชาติเรื่องเครื่องมือแพทย์ ครั้งที่ 1, น. 97.

2.12 ความหมายของเทคโนโลยีทางการแพทย์

ฟอร์บส์ เผย 6 เทรนด์การแพทย์ยุคใหม่[26] ท่ามกลางยุคแห่งเทคโนโลยีพลิกโลก (Technology Disruption) ที่หลายอุตสาหกรรมต้องเร่งปรับตัวเพื่อความอยู่รอดและเติบโต แต่สำหรับอุตสาหกรรมการดูแลสุขภาพ (Healthcare) แนวโน้มการเปลี่ยนแปลงสู่ดิจิทัล ได้ขยับบทบาทของเทคโนโลยีทางการแพทย์ให้สูงขึ้น จากจุดเด่นที่ว่า เทคโนโลยีช่วยคนให้มีชีวิตยืนยาวขึ้น ปลอดภัยขึ้น สุขภาพแข็งแรงขึ้น ใช้ชีวิตอย่างมีคุณภาพได้ดีขึ้น

นิตยสารฟอร์บส์ ได้คาดการณ์ 6 แนวโน้มสำคัญของเทคโนโลยีทางการแพทย์ในปี 2019 ซึ่งสามารถช่วยอำนวยความสะดวกให้กับทั้งผู้ป่วย และแพทย์ ทั้งในด้านค่าใช้จ่าย เพิ่มความเที่ยงตรงใน การวินิจฉัยอาการ ลดกระบวนการทำงาน และเพิ่มความรวดเร็วในการรักษาหรือช่วยชีวิตคนไข้ เทคโนโลยีมาแรงด้านการแพทย์เหล่านี้ ได้แก่

1. การแพทย์ทางไกล (Telemedicine)

ตัวเลขผู้รับบริการการรักษาพยาบาลทางไกล (Telehealth) เพิ่มอย่างโดดเด่นจากจำนวนกว่า 1 ล้านคน เมื่อปี 2558 เป็น 7 ล้านคนในปีที่ผ่านมา ปัจจัยหนุนส่วนหนึ่งมาจากความก้าวหน้าด้านเทคโนโลยีที่ช่วยให้การรักษาพยาบาลไฮเทคนี้ ‘เข้าถึง’ ผู้ป่วยในพื้นที่ห่างไกลได้ครอบคลุมทั่วถึงมากขึ้น ยื้อชีวิตและสนับสนุนการมีคุณภาพชีวิตที่ดีให้กับกลุ่มคนในพื้นที่ห่างไกล และด้อยความสามารถในการใช้จ่ายเพื่อเดินทางเข้ามารับการรักษาที่โรงพยาบาล

นอกเหนือจากผู้รับประโยชน์จากเทคโนโลยีนี้ในฟากของผู้รับบริการหรือผู้ป่วยในส่วนของแพทย์ก็สามารถประหยัดเวลา และค่าใช้จ่ายในการเดินทางออกไปเยี่ยมเยียนคนไข้อีกด้วย เรียกได้ว่า win - win กันทั้งสองฟาก

2. ปัญญาประดิษฐ์ (Artificial Intelligence)

การสแกนตรวจร่างกาย และบริการทางการแพทย์ต่าง ๆ จะถูกยกระดับไปอีกหลาย ๆ ขั้น ด้วยการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และการเรียนรู้เชิงลึก (Deep Learning) ซึ่งจะช่วยเพิ่มความ

---

[26] “คอลัมน์ อินโนสเปซ โดย บัซซี่บล็อก หนังสือพิมพ์ คมชัดลึก ฉบับวันที่ 11 - 12 พฤษภาคม พ.ศ. 2562,” https://www.komchadluek.net/news/lifestyle/371309

รวดเร็วในการวิเคราะห์ภาพถ่ายจากซีทีสแกนได้มากกว่าเดิมถึง 150 เท่า สามารถตรวจพบสิ่งผิดปกติจากผลการสแกนได้ภายในหลักวินาที เมื่อเทียบกับการรอผลจากนักรังสีวิทยา

คนไข้ไม่ต้องเครียดกับการรอลุ้นผลตรวจ ได้ความเที่ยงตรงของผลลัพธ์ ทั้งนี้ AI ยังสามารถช่วยประเมินแนวทางการรักษาที่มีประสิทธิภาพมากที่สุดสำหรับแต่ละอาการ

3. บล็อกเชน (Blockchain)

บล็อกเชน จะเข้ามีบทบาทในกระบวนการส่งต่อแฟ้มข้อมูลการรักษาพยาบาลของคนไข้ระหว่างแพทย์ผู้รักษา เพราะต้องตระหนักถึงข้อเท็จจริงที่ว่า คนไข้ 1 คน จะมีแพทย์ผู้รับผิดชอบมากกว่า 1 คน ในทางกลับกันแพทย์แต่ละคนก็ต้องดูแลคนไข้มากกว่า 1 ราย เทคโนโลยีนี้จะเข้ามา 'ปิดช่องว่าง' เรื่องความไม่มั่นใจต่อความปลอดภัยหรือการรั่วไหลของข้อมูลคนไข้ในระหว่างทางของกระบวนการส่งต่อ เนื่องจากจะอนุญาตให้แพทย์ผู้มีสิทธิ์เข้าถึงข้อมูลการรักษานั้น ๆ จึงจะสามารถอ่านประวัติคนไข้/การรักษาที่ผ่านมาได้ ป้องกันข้อผิดพลาดหรือความคลาดเคลื่อนในขั้นตอนการรักษา ทำให้ได้รับการวินิจฉัยและการรักษาตรงตามอาการ

4. AR และเทคโนโลยีเสมือน (AR and VR)

เทคโนโลยีการผสานโลกจริงและโลกเสมือน หรือ AR (Augmented Reality) ช่วยให้แพทย์เรียนรู้วิธีการทำงานในกระบวนการรักษาที่อาจเป็นอันตราย อย่างเช่น การผ่าตัดหัวใจ แต่แนวโน้มที่เหนือล้ำไปอีกก็คือ มีการคาดการณ์ว่า AR และ VR จะเป็นเทคโนโลยีที่เข้ามาช่วยเหลือในขั้นตอนการรักษาผู้ป่วยไม่เฉพาะแต่อาการทางร่างกาย แต่รวมไปถึงอาการของโรคอัลไซเมอร์ และภาวะสมองเสื่อมในผู้สูงอายุ

การใช้เทคโนโลยีที่สามารถจำลองสถานการณ์หรือโรคจริง จะเข้ามาช่วยฟื้นฟูความทรงจำให้กับผู้ป่วยในกลุ่มนี้ ความสุขในการย้อนกลับสู่ภาพแห่งวันเวลาและประสบการณ์ต่าง ๆ จะเป็นหนึ่งในเครื่องมือบำบัดและเยียวยาที่มีประสิทธิภาพ

5. การเก็บสำเนาในรูปดิจิทัล (Digital Twin)

เทคโนโลยี Digital Twins เป็นเสมือนสะพานเชื่อมระหว่างโลกทางกายภาพและโลกดิจิทัลเพื่อจำลองสภาพแวดล้อมตามแบบของจริง ในแง่ของอุตสาหกรรมด้านการแพทย์ เทคโนโลยีนี้ จะช่วย

สร้างสภาพแวดล้อมที่มีความปลอดภัย สำหรับผู้ให้บริการทางการแพทย์ หรือผู้ผลิตเครื่องมือแพทย์ สามารถทดสอบผลกระทบต่าง ๆ ที่อาจเกิดขึ้นเมื่อมีการเปลี่ยนแปลงใด ๆ ในกระบวนการปฏิบัติงาน หรือทำการรักษาคนไข้ การทดสอบเหล่านี้เกิดขึ้นได้อย่างมีประสิทธิภาพด้วยการเรียนรู้จากปริมาณข้อมูลมหาศาล (Big Data) ที่รวบรวมไว้จากระบบจริงนั่นเอง ซึ่งหมายความว่ายิ่งมีการรวบรวมข้อมูลจากการรักษาจริงมาให้ระบบเรียนรู้ได้มากเท่าไหร่ (ด้วยการใช้ประโยชน์จาก AI และการเรียนรู้ของเครื่องจักร (Machine Learning) ความรู้และความเชี่ยวชาญในการด้านการักษาพยาบาลก็จะยิ่งก้าวไกลเพิ่มขึ้นเท่านั้น

6. อุปกรณ์สวมใส่ได้ และ IoT

อุปกรณ์ไฮเทคใหม่ ๆ ชิ้นเล็ก ๆ อย่างนาฬิกา หรือสายรัดข้อมือที่ตรวจวัดชีพจร อัตราการเต้นของหัวใจ ปริมาณแคลอรี่ต่าง ๆ เหล่านี้ หรือที่เรียกกันติดปากว่า Wearable กำลังพัฒนาจากการเป็นแฟชั่นด้านสุขภาพ มาสู่การเป็นเครือข่ายเครื่องมือจัดเก็บข้อมูลสุขภาพแบบเรียลไทม์ ด้วยการรวบรวมข้อมูลผ่านอินเทอร์เน็ตในทุกสิ่ง (IoT) ในยุคที่ IoT พุ่งแรงอย่างไม่หยุด ทำให้เทคโนโลยีนี้จะยิ่งทรงพลังมากขึ้นต่ออุตสาหกรรมการแพทย์ ตามปริมาณข้อมูลที่จะทวีปริมาณมหาศาลขึ้นเรื่อย ๆ ตามจำนวนอุปกรณ์ IoT ด้านสุขภาพที่กระจายอยู่ในโลกจริง ข้อมูลเหล่านี้สามารถพัฒนามาใช้ในการวิจัยและพัฒนาตัวยา ตลอดจนวิธีการรักษาทางการแพทย์ที่ก้าวหน้าขึ้นกว่าเดิมอีกด้วย

โดยปัจจุบันประเทศไทยมีระบบฐานข้อมูลของสาธารณสุข มีข้อมูลคนไข้อยู่ 40-50 ล้านราย แต่ยังขาดการเชื่อมโยงกับฐานข้อมูลของโรงพยาบาลเอกชน ซึ่งหากปลดล็อคในส่วนนี้ได้ จะเอื้อต่อการให้บริการทางการแพทย์ด้วยเทคโนโลยีการรักษาทางไกล (Telemedicine)

2.13 ความหมายของข้อมูลส่วนบุคคลของผู้ป่วย

[27]สหภาพยุโรปได้ออกกฎหมายฉบับใหม่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือที่เรียกกันว่า GDPR หรือ General Data Protection Regulation ซึ่งมีบังคับใช้เมื่อเดือนพฤษภาคม พ.ศ. 2561 โดยมีข้อกำหนดให้องค์กรต่าง ๆ ที่มีธุรกรรมหรือการดำเนินการบนอินเทอร์เน็ตที่มีข้อมูลส่วนบุคคลของผู้บริโภคต้องปฏิบัติตามมาตรการต่าง ๆ ที่เข้มงวดขึ้นเพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวของบุคคล ซึ่งเป็นการปรับปรุงกฎหมายเดิม (EU Data Protection Directive 95/46/EC) ซึ่งใช้บังคับมานานกว่า 20 ปี ทำให้เกิดการเปลี่ยนแปลงหลักการที่สำคัญ เช่น

- กำหนดการใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) กล่าวคือ ข้อมูลส่วนบุคคลของสหภาพยุโรปอยู่ภายใต้ความคุ้มครองไม่ว่าจะอยู่ในที่ใดในโลก

- กำหนดบทลงโทษสูงขึ้น โดยองค์กรที่กระทำผิดอาจต้องจ่ายค่าปรับสูงถึงอัตราร้อยละ 4 ของผลประกอบการรายได้ทั่วโลก

- กำหนดให้การขอความยินยอมจากเจ้าของข้อมูลต้องชัดเจนและชัดแจ้ง (Clear and Affirmative Consent)

- กำหนดการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล หน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และประชาชนทราบภายใน 72 ชั่วโมง

- กำหนดขอบเขตสิทธิของเจ้าของข้อมูล ให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลจะถูกใช้อย่างไร เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

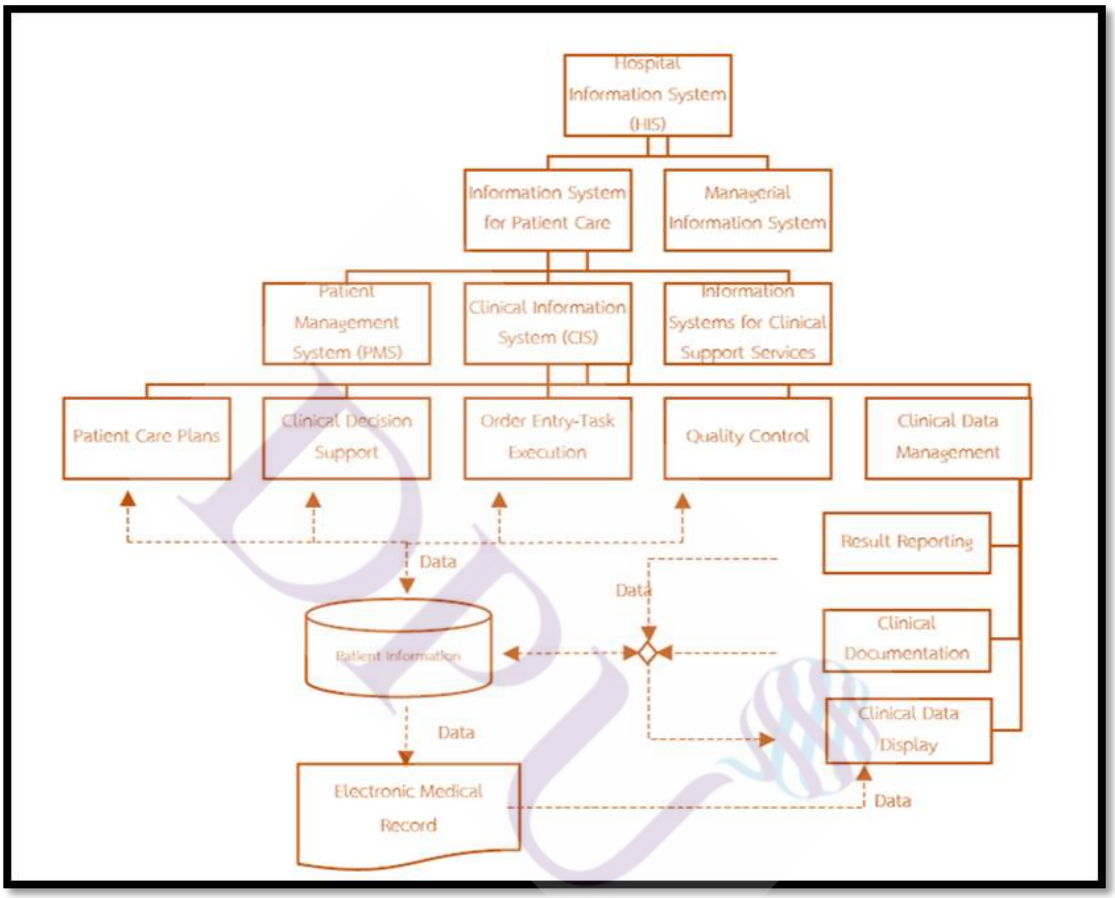
- กำหนดรับรองสิทธิในการโอนข้อมูลไปยังผู้ประกอบการอื่น (Right to Data Portability)

- กำหนดรับรองสิทธิที่จะถูกลืม (Right to be Forgotten) เจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้

---

[27] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, “Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล,” โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, พิมพ์ครั้งที่1 (ธันวาคม 2563), น. 17 – 18.

ภาพที่ 2.2 การจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลแบบกว้าง



ที่มา : Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2.14 ความเป็นส่วนตัวทางการแพทย์

ความเป็นส่วนตัวทางการแพทย์หรือความเป็นส่วนตัวด้านสุขภาพคือการปฏิบัติในการรักษาความปลอดภัยและความลับของบันทึกผู้ป่วย มันเกี่ยวข้องกับทั้งการสนทนากับดุลยพินิจของผู้ให้บริการด้านการดูแลสุขภาพและความปลอดภัยของเวชระเบียน ข้อตกลงนี้ยังสามารถดูได้ทางกายภาพความเป็นส่วนตัวของผู้ป่วยจากผู้ป่วยอื่น ๆ และผู้ให้บริการในขณะที่สิ่งอำนวยความสะดวกทางการแพทย์ ความกังวลที่ทันสมัยรวมถึงระดับของการเปิดเผยข้อมูลต่อบริษัท ประกันภัยนายจ้างและ

บุคคลที่สามอื่น ๆ การมาถึงของเวชระเบียนอิเล็กทรอนิกส์ (EMR) และระบบการจัดการการดูแลผู้ป่วย (PCMS) มีความกังวลเกี่ยวกับความเป็นส่วนตัวใหม่, สมดุลกับความพยายามที่จะลดความซ้ำซ้อนของการบริการและผิดพลาดทางการแพทย์[28,29] หลายประเทศ - รวมถึงออสเตรเลีย[30] แคนาดา ตุรกี สหราชอาณาจักร สหรัฐอเมริกา นิวซีแลนด์ และเนเธอร์แลนด์ ได้ออกกฎหมายที่พยายามปกป้องความเป็นส่วนตัวของผู้คน อย่างไรก็ตามกฎหมายเหล่านี้จำนวนมากได้พิสูจน์แล้วว่ามีประสิทธิภาพน้อยกว่าในทางทฤษฎี[31] สหรัฐอเมริกาได้ผ่านพระราชบัญญัติประกันสุขภาพพกพาและพระราชบัญญัติความรับผิดชอบ (HIPAA) เป็นความพยายามที่จะเพิ่มข้อควรระวังความเป็นส่วนตัวภายในสถาบันการแพทย์[32]

---

[28] Hiller, Mare, "Patient Care Management Systems, Medical Records, and Privacy: A Balancing Act.b 1982," https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1424350). "Public Health Reports. 97: 332–45. PMC 1424350," https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1424350) – via JSTOR.

[29] Miller, Amalia, "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. "Management Science. 55: 1077–1093. doi:10.1287/mnsc.1090.1014, (2009)," https://doi.org/10.1287%2Fmnsc.1090.101 4) – via JSTOR.

[30] . Manager, Web, "Australian Privacy Law & Practice - Key Recommendations for Health Information Privacy Reform," (2011-09-28) (https://www.alrc.gov.au/news-media/2011/australian-privacy-law-practice-key-recommendation s-health-information-privacy-refor). www.alrc.gov.au. Retrieved 2018-12-03.

[31] Andriole, Katherine P. "Security of Electronic Medical Information and Patient Privacy: What You Need to Know, Journal of the American College of Radiology. 11: 1212–1216. doi:10.1016/j.jacr.2014.09.011 (2014)," (https://doi. org/10.1016%2Fj.jacr.2014.09.011).

[32] Edemekong, Peter F.; Haydel, Micelle J. "Health Insurance Portability and Accountability Act (HIPAA), (2018)," (htt ps: / / www. ncbi. nlm. nih. gov/ books/ NBK500019/) , StatPearls, StatPearls Publishing, PMID 29763195 (https://www. ncbi.nlm.nih.gov/pubmed/29763195), retrieved 2018-12-03

ก่อนที่จะมีความก้าวหน้าทางเทคโนโลยีสถาบันทางการแพทย์ต้องอาศัยสื่อกลางในการจัดเก็บข้อมูลทางการแพทย์ของแต่ละบุคคล ปัจจุบันมากขึ้นและข้อมูลเพิ่มเติมจะถูกเก็บไว้ภายในฐานข้อมูลอิเล็กทรอนิกส์[33]

2.15 เทคโนโลยีการสื่อสาร

การสื่อสาร หรือ การสื่อความหมาย (Communication) เป็นคำที่รากศัพท์มาจากภาษาลาติน ว่า "Communius" หมายถึง "พร้อมกัน" หรือ "ร่วมกัน (Common)" หมายความว่า เมื่อมีการสื่อสารระหว่างกันเกิดขึ้น คนเราพยายามที่จะสร้าง "ความพร้อมกันหรือความร่วมกัน" ทางด้านความคิดเรื่องราวเหตุการณ์ ทัศนคติ ฯลฯ กับบุคคลที่เรากำลังสื่อสารด้วยนั้น ดังนั้น การสื่อสารจึงหมายถึง การถ่ายทอดเรื่องราว การแลกเปลี่ยนความคิดเห็น การแสดงออกของความคิดและความรู้สึก ตลอดรวมไปถึง "ระบบ" (เช่น ระบบโทรศัพท์) เพื่อการติดต่อสื่อสารข้อมูลซึ่งกันและกัน (Webster's Dictionary 1978 : 98) นอกจากนี้ การสื่อสารยังเป็นการที่บุคคลในสังคมมีปฏิสัมพันธ์โต้ตอบกันโดยผ่านทางข้อมูลข่าวสาร สัญลักษณ์ตลอดจนเครื่องหมายต่าง ๆ ด้วย

เทคโนโลยี มีความหมายค่อนข้างกว้าง โดยทั่วไปหมายถึง สิ่งที่มนุษย์พัฒนาขึ้น เพื่อช่วยในการทำงานหรือแก้ปัญหาต่าง ๆ เช่น อุปกรณ์ เครื่องมือ เครื่องจักร วัสดุ หรือ แม้กระทั่งที่ไม่ได้เป็นสิ่งของที่จับต้องได้ เช่น กระบวนการต่าง ๆ เทคโนโลยี เป็นการประยุกต์ใช้วิทยาศาสตร์ให้เกิดประโยชน์ ในทางเศรษฐศาสตร์ มองเทคโนโลยีว่า เป็นความรู้ของมนุษย์ ณ ปัจจุบัน ในการนำเอาทรัพยากรมาผลิตเป็นผลิตภัณฑ์ที่ต้องการ (รวมถึงความรู้ว่าเราสามารถผลิตอะไรได้บ้าง) ดังนั้น การเปลี่ยนแปลงทางเทคโนโลยี จะเกิดขึ้นเมื่อความรู้ทางเทคนิคของเราเพิ่มขึ้น

---

[33] Alpert, Sheri, “Smart Cards, Smarter Policy Medical Records, Privacy, and Health Care Reform,” The Hastings Center Report. 23: 13–23. doi:10.2307/3562918, (1993), (https://doi.org/10.2307%2F3562918) – via JSTOR.

2.16 เวชระเบียน

เวชระเบียน (Medical Record) คือ เอกสารทางการแพทย์ทุกประเภท ที่ใช้บันทึกและเก็บรวบรวมประวัติของผู้ป่วยที่มารับบริการทางการแพทย์ที่โรงพยาบาล ไม่ว่าจะเป็นการรับบริการตรวจและรักษาโรค ทั้งประวัติส่วนตัว ประวัติครอบครัว ประวัติการแพ้ยา เอกสารการยินยอมให้ทำการรักษาพยาบาล ประวัติการเจ็บป่วยในอดีตและปัจจุบัน ข้อมูลบ่งชี้เฉพาะของบุคคล การรักษาพยาบาล ค่ารักษาพยาบาล ผลจากห้องปฏิบัติการ ผลการชันสูตรบาดแผลหรือพลิกศพ ผลการบันทึกค่าทั้งที่เป็นตัวเลข ตัวอักษร รูปภาพหรือเครื่องหมายอื่นใด จากอุปกรณ์ เครื่องมือในสถานบริการสาธารณสุข หรือเครื่องมือทางการแพทย์ทุกประเภท หรือเอกสารการบันทึกการกระทำใด ๆ ที่เป็นการสั่งการรักษา การปรึกษาเพื่อการรักษาพยาบาล การส่งต่อผู้ป่วยไปทำการรักษาที่อื่น การรับผู้ป่วยรักษาต่อ การกระทำตามคำสั่งของผู้มีอำนาจในการรักษาพยาบาลตามที่สถานบริการสาธารณสุขกำหนดไว้ เอกสารอื่น ๆ ที่ใช้ประกอบเพื่อการตัดสินใจทางการแพทย์ เพื่อการประสานงานในการรักษาพยาบาลผู้ป่วย และเอกสารอื่นใดที่ทางองค์การอนามัยโลก หรือสถานบริการสาธารณสุขกำหนดไว้ว่าเป็นเอกสารทางเวชระเบียน หมายรวมถึงชื่อของหน่วยงานที่ทำหน้าที่ในการจัดทำเอกสารดังกล่าว การเก็บรวบรวม การค้นหา การบันทึก การแก้ไข การให้รหัสโรค การจัดทำรายงานทางการแพทย์ การนำมาจัดทำสถิติผู้ป่วย การนำมาเพื่อการศึกษาวิจัย หรือเพื่อการอื่นใดตามที่สถานบริการสาธารณสุขกำหนด นอกจากนี้ยังรวมถึงเอกสารทางการแพทย์ที่อยู่ในรูปแบบสื่อดิจิตอล หรือระบบอิเล็กทรอนิกส์ (Electronic Medical Record -EMR) ซึ่งเป็นรูปแบบของเวชระเบียนที่มีการพัฒนาขึ้นในปัจจุบัน[34,35]

เวชระเบียนมีการแบ่งงานออกตามภารกิจ[36] ซึ่งงานเวชระเบียนแบ่งออกเป็น

---

[34] แสงเทียน อยู่เถา, เวชระเบียน, (กรุงเทพมหานคร: มิสเตอร์ก๊อปปี้ (ประเทศไทย), 2556).

[35] คู่มือคำแนะนำการบันทึกเวชระเบียนสำหรับแพทย์, สำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข, สำนักงานกิจการโรงพิมพ์องค์การสงเคราะห์ทหารผ่านศึก, พิมพ์ครั้งที่ 1 : สิงหาคม 2555.

[36] แสงเทียน อยู่เถา, การบริหารงานเวชระเบียน, (กรุงเทพมหานคร: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2560).

1. งานเวชระเบียนผู้ป่วยนอก

2. งานเวชระเบียนผู้ป่วยใน

เวชระเบียนเป็นเอกสารที่มีประวัติการเจ็บป่วย ผลการตรวจ และรายละเอียดการรักษาของผู้ป่วยแต่ละราย ผู้ที่มีหน้าที่หลักในการบันทึกเวชระเบียนคือแพทย์ โดยแพทย์จะบันทึกเวชระเบียนทุกครั้งที่ซักประวัติตรวจร่างกายและให้การรักษาผู้ป่วย โดยแพทย์ พยาบาล และเจ้าหน้าที่อื่น ๆ ที่เกี่ยวข้องกับการดูแลรักษาผู้ป่วยจะอ่านข้อมูลที่บันทึกอยู่ในเวชระเบียนเพื่อใช้ข้อมูลนั้นประกอบการดูแลรักษาผู้ป่วยอย่างมีคุณภาพ อย่างไรก็ตาม หากแพทย์ผู้บันทึกเวชระเบียนเขียนข้อมูลไม่ครบ ใช้อักษรย่อลายมือหวัดเกินไป หรือบันทึกขาดตกบกพร่องตั้งแต่ต้น จะทำให้แพทย์คนอื่น พยาบาล และเจ้าหน้าที่อื่น ๆ ที่มาอ่านข้อมูล ไม่สามารถใช้ข้อมูลนั้นประกอบการดูแลรักษาผู้ป่วยได้อย่างดีการบันทึกเวชระเบียนอย่างมีคุณภาพจึงมีความสำคัญอย่างยิ่งต่อคุณภาพการรักษาผู้ป่วย และส่งผลให้การทำสถิติการเจ็บป่วยสามารถระบุสาเหตุของโรคต่าง ๆ ได้อย่างถูกต้อง[37]

[38]เวชระเบียนที่มีคุณภาพ ต้องมีองค์ประกอบ 4 ด้าน คือ

1. ความครบถ้วน หมายถึง มีข้อมูลที่สำคัญครบทุกด้าน ไม่ขาดตกบกพร่อง

เป็นเวชระเบียนที่มีการบันทึกหัวข้อสำคัญครบทุกหัวข้อ ไม่เว้นว่างไม่โดยไม่เขียน เช่น การบันทึกแบบฟอร์มสรุปเวชระเบียน (Discharge Summary) จะต้องบันทึกการวินิจฉัยหลัก โรคร่วม โรคแทรก โรคอื่น ๆ และสาเหตุการบาดเจ็บ ให้ครบทุกหัวข้อ หรือ การบันทึกรายละเอียดการผ่าตัด ก็จะต้องบันทึก Position Incision Finding Prodedures ให้ครบทุกหัวข้อ เป็นต้น

2. ความถูกต้อง หมายถึง มีเนื้อหาที่ตรงตามความเป็นจริง ไม่ผิดเพี้ยน

เป็นเวชระเบียนที่มีการบันทึกเนื้อหาต่าง ๆ อย่างถูกต้องแม่นยำ ไม่ผิดเพี้ยน เช่น ประวัติการเจ็บป่วย ผลการตรวจร่างกาย ผลการตรวจทางห้องปฏิบัติการ การให้ยารักษา ต้องไม่ผิดไปจาก

---

[37] World Health Organization, Inte0rnational Statistical Classification of Diseases and Related Health Problems, Tenth Revision, volume 2. 2nd ed. (Geneva: The Organization; 2004).

[38] คู่มือคำแนะนำการบันทึกเวชระเบียนสำหรับแพทย์, สำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข, สำนักงานกิจการโรงพิมพ์องค์การสงเคราะห์ทหารผ่านศึก, พิมพ์ครั้งที่ 1 : สิงหาคม 2555, น. 1 - 2

ความเป็นจริง อย่างไรก็ตาม บางครั้ง แพทย์อาจบันทึกผิดในเบื้องต้น แต่เมื่อรู้ว่าผิดก็สามารถขีดฆ่าข้อความที่ผิดพลาดแล้วลงนามกำกับก่อนบันทึกเพิ่มเติมให้ถูกต้อง

3. ความมีรายละเอียดที่ดี หมายถึง มีการขยายความให้เห็นลักษณะย่อย ไม่กำกวม หรือคลุมเครือ

เป็นเวชระเบียนที่มีการบันทึกรายละเอียดที่สำคัญได้อย่างชัดเจน ไม่มีคำกำกวมไม่มีคำย่อไม่มีสัญลักษณ์ที่บางคนอ่านไม่เข้าใจ แพทย์ควรระวังการเขียนคำย่อ เพราะหากคำย่อนั้นไม่เป็นที่เข้าใจของแพทย์ พยาบาลหรือเจ้าหน้าที่อื่น ๆ ที่มาอ่านจะทำให้เกิดความสับสน เข้าใจผิดได้ง่าย

4. ความทันสมัย หมายถึง มีข้อมูลสดใหม่ พบรายละเอียดครั้งล่าสุดที่ผู้ป่วย มารับบริการ

เป็นเวชระเบียนที่มีข้อมูลสดใหม่ เช่น มีข้อมูลครั้งสุดท้ายที่ผู้ป่วยมาตรวจรักษา มีผลการตรวจทางห้องปฏิบัติการครั้งล่าสุด เมื่ออ่านเวชระเบียนแล้ว สามารถเข้าใจรายละเอียดครั้งล่าสุดที่ผู้ป่วยมารักษาได้ครบทุกด้าน

2.17 เวชระเบียนอิเล็กทรอนิกส์ (Electronic Medical Record)[39]

คือ การจัดเก็บข้อมูลประวัติของผู้ป่วยของสถานพยาบาล หรือสถานบริการสาธารณสุขในรูปของข้อมูลอิเล็กทรอนิกส์ รวมถึงการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างสถานพยาบาล เพื่อประโยชน์ต่อการให้บริการรักษาอย่างต่อเนื่อง เช่น การค้นประวัติย้อนหลังของผู้ป่วยเกี่ยวกับรักษาที่ผ่านมา การจัดเก็บในรูปฐานข้อมูลอกจากง่ายต่อการสืบค้นแล้วการจัดเก็บยังเป็นไปโดยง่ายกว่าการจัดเก็บเวชระเบียนในแบบเดิมที่เป็นรูปแบบเอกสารกระดาษซึ่งอาจเสียหายจากการจัดเก็บได้ และยังค้นข้อมูลได้ยากกว่าการค้นในฐานข้อมูลอิเล็กทรอนิกส์ ทำให้ในปัจจุบันโรงพยาบาลใช้รูปแบบการจัดข้อมูลอิเล็กทรอนิกส์

ข้อมูลการจัดเก็บเวชระเบียนอิเล็กทรอนิกส์ สิ่งที่จัดเก็บมีดังต่อไปนี้

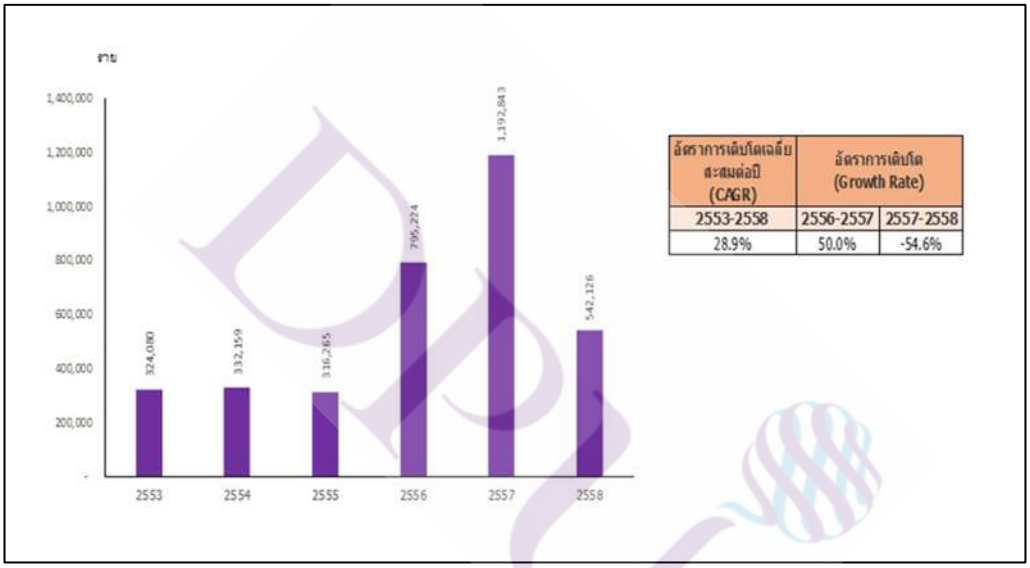
(1) ข้อมูลพื้นฐานเวชระเบียนอิเล็กทรอนิกส์

---

[39] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), “e-Medical Record,” https://www.etda.or.th/content/e-medical-record.html

เวชระเบียนอิเล็กทรอนิกส์ เป็นการพัฒนาจากความก้าวหน้าของเทคโนโลยีสารสนเทศ ที่อำนวยความสะดวกเพื่อการแพทย์ ที่ดำเนินการโดยจัดเก็บเอกสารผู้ป่วยทั้งแฟ้มโดยการสแกนภาพลงบนสื่ออิเล็กทรอนิกส์หรือคอมพิวเตอร์ เช่น ซีดี หรือฮาร์ดดิสก์ เป็นต้น และการบันทึกข้อมูลประวัติผู้ป่วยเข้าสู่ระบบคอมพิวเตอร์โดยตรง เพื่อลดพื้นที่การจัดเก็บเอกสารและประโยชน์ในการสืบค้น

ภาพที่ 2.3 ปริมาณเวชระเบียนอิเล็กทรอนิกส์



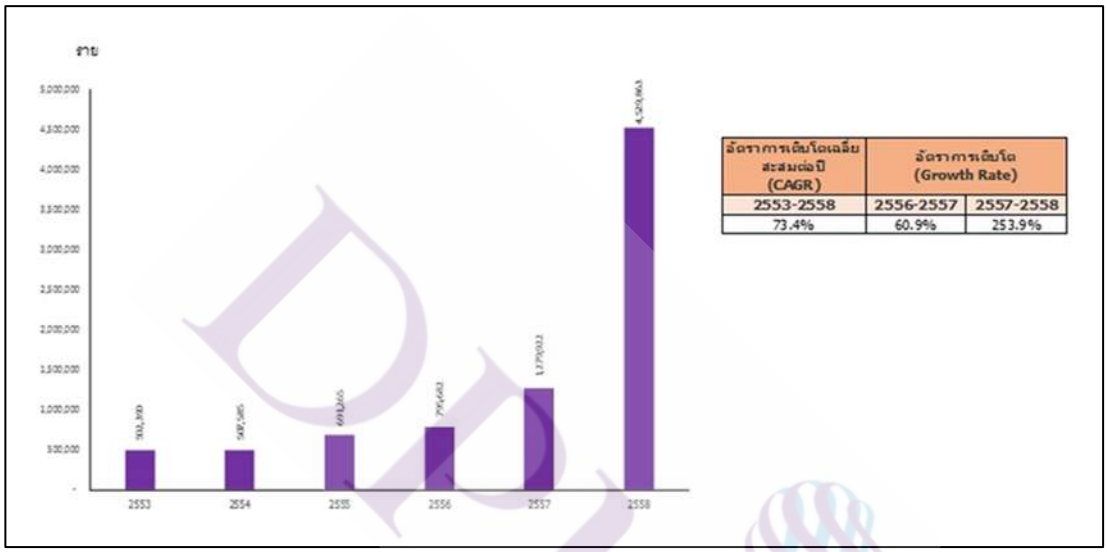
ที่มา: โรงพยาบาลที่มีการผลิตบุคลากรทางการแพทย์ ซึ่งเป็นหน่วยงานที่ได้ให้ข้อมูลเพื่อการเผยแพร่ในปี 2553 - 2557 ได้แก่ โรงพยาบาลศิริราช โรงพยาบาลจุฬาลงกรณ์ และโรงพยาบาลมหาราชนครเชียงใหม่

เวชระเบียนในโรงพยาบาลที่มีการผลิตบุคลากรทางการแพทย์ซึ่งจัดเก็บในรูปสื่ออิเล็กทรอนิกส์ ในปี พ.ศ. 2558 มีปริมาณทั้งสิ้น 542,126 ราย มีอัตราการเติบโต ร้อยละ 54.6 จากปีก่อนหน้า เมื่อดูภาพรวมการเติบโตของในช่วงตั้งแต่ปี พ.ศ. 2553 ถึง 2558 พบว่าปริมาณเวชระเบียนอิเล็กทรอนิกส์มีอัตราการเติบโตเฉลี่ยสะสมต่อปีร้อยละ 28.9 ทั้งนี้ ขึ้นอยู่กับปริมาณผู้ป่วยที่เข้ารับการ

รักษาของโรงพยาบาลในปีนั้น ๆ ด้วย แสดงตามภาพที่ 2.1 ทั้งนี้ โรงพยาบาลจุฬาลงกรณ์ ได้มีจัดเก็บเวชระเบียนในรูปแบบอิเล็กทรอนิกส์เฉพาะผู้ป่วยในอย่างเดียวในปี พ.ศ. 2557 - 2558

(2) สถานภาพการใช้บริการเวชระเบียนอิเล็กทรอนิกส์

ภาพที่ 2.4 ปริมาณการใช้บริการเวชระเบียนอิเล็กทรอนิกส์



ที่มา: โรงพยาบาลที่มีการผลิตบุคลากรทางการแพทย์ ซึ่งเป็นหน่วยงานที่ได้ให้ข้อมูลเพื่อการเผยแพร่ในปี พ.ศ. 2553 - 2557 ได้แก่ โรงพยาบาลศิริราช โรงพยาบาลจุฬาลงกรณ์ และโรงพยาบาลมหาราชนครเชียงใหม่

ปริมาณการใช้บริการเวชระเบียนอิเล็กทรอนิกส์ ในปี พ.ศ. 2558 มีจำนวนทั้งสิ้น 4,529,863 ราย ปรับตัวเพิ่มขึ้นในอัตราการเติบโต ร้อยละ 259.3 จากปีก่อนหน้า และการเติบโตตั้งแต่ปี พ.ศ. 2553 ถึง 2558 พบว่าปริมาณการเรียกใช้บริการเวชระเบียนอิเล็กทรอนิกส์ มีอัตราการเติบโตเฉลี่ยสะสมต่อปี ร้อยละ 73.4 ซึ่งเป็นบริการที่ช่วยอำนวยความสะดวกในการใช้บริการจากเวชระเบียนในรูปแบบต่าง ๆ ผ่านเครือข่ายของโรงพยาบาลนั้น ๆ แสดงตามภาพที่ 2.2

การรับ - ส่งข้อมูลผู้ป่วยทางระบบอิเล็กทรอนิกส์

1) ข้อมูลพื้นฐานด้านการรับ - ส่งข้อมูลผู้ป่วยทางอิเล็กทรอนิกส์

การโอนเงินค่าบริการสาธารณสุขให้กับหน่วยบริการผ่านระบบอิเล็กทรอนิกส์ เป็นการขอรับการจ่ายชดเชยค่าใช้จ่ายเพื่อบริการสาธารณสุขทั้งประเภทผู้ป่วยนอกและผู้ป่วยในปัจจุบัน สำนักงานหลักประกันสุขภาพแห่งชาติ หรือ สปสช. ได้ดำเนินการจ่ายชดเชยการจัดและส่งเสริมให้ประชาชนเข้าถึงการบริการสาธารณสุขที่เน้นการให้บริการได้อย่างทั่วถึง รวดเร็วและมีประสิทธิภาพ โดยมีการขอเบิกชดเชยผ่านทางระบบ E-Claim และจ่ายชดเชยค่าบริการทางการแพทย์ผ่านระบบ E-Payment เพื่ออำนวยความสะดวกให้กับหน่วยบริการ

2) การขอรับค่าใช้จ่ายเพื่อบริการสาธารณสุข (E-Claim)

E-Claim คือ โปรแกรมที่ใช้สำหรับบันทึกข้อมูลการให้บริการสาธารณสุขของหน่วยบริการทั้งประเภทผู้ป่วยนอกและผู้ป่วยใน เพื่อขอเบิกชดเชยค่าบริการทางการแพทย์จาก สปสช. ตามเกณฑ์และเงื่อนไขที่กำหนด โดยมีขั้นตอนของการขอเบิกชดเชยค่าบริการทางการแพทย์

3) การขอเบิกจ่ายยาจากหน่วยบริการ ภายใต้ระบบ Vendor Managed Inventory หรือ VMI

ระบบ Vendor Managed Inventory หรือ VMI เป็นระบบซึ่ง สปสช.ได้ร่วมกับองค์การเภสัชกรรม (อภ.) ไม่เพียงแต่ทำให้เกิดการกระจายยาส่งไปยังหน่วยบริการทั่วประเทศเท่านั้น แต่ยังช่วยลดปัญหาการจัดเก็บยาของโรงพยาบาลได้ เนื่องจากเป็นระบบที่มีการรายงานรายการยาในระบบต่อเนื่อง และดูความต้องการยาของพื้นที่ ทำให้มีการตรวจสอบ และการเติมยาเข้าสู่คลังยาของโรงพยาบาลและพื้นที่ต่อเนื่อง จึงทำให้ไม่มีปัญหาเรื่องยาขาด ยาหมดอายุ และการจัดส่งไม่ทัน เป็นระบบที่รับประกันได้ว่าทั้งยา และวัคซีนจะมีใช้ในโรงพยาบาลโดยไม่ขาดแคลน ช่วยลดปัญหาการจัดเก็บยาของโรงพยาบาล

4) การตรวจสอบสิทธิ์การรักษา

เพื่อให้ประชาชนได้รับทราบข้อมูลส่วนตัวของผู้รับบริการ โดยประชาชนสามารถตรวจสอบสิทธิ์ของการรับการรักษาสุขภาพว่า สามารถเข้ารับบริการจากหน่วยบริการในระบบประกัน

สุขภาพแห่งชาติได้ จากคำนิยามของ การตรวจสอบสิทธิ์ คือ การตรวจสอบสิทธิ์ที่หน่วยบริการหรือหน่วยงานที่เกี่ยวข้องขอรับการบริการจาก สปสช.

เวชระเบียนอิเล็กทรอนิกส์ (EMR)[40]

ความแตกต่างระหว่างเวชระเบียนอิเล็กทรอนิกส์และประวัติสุขภาพอิเล็กทรอนิกส์

EMR มีข้อมูลทางการแพทย์และการแพทย์ที่ได้มาตรฐานในสำนักงานของผู้ให้บริการรายหนึ่ง บันทึกสุขภาพทางอิเล็กทรอนิกส์ หรือ Electronic Health Records (EHRs) มีมากกว่าข้อมูลที่เก็บรวบรวมในสำนักงานของผู้ให้บริการและรวมประวัติผู้ป่วยที่ครอบคลุมมากขึ้น

บันทึกสุขภาพอิเล็กทรอนิกส์ (EHR) หรือเวชระเบียนอิเล็กทรอนิกส์ (EMR) เป็นการจัดเก็บข้อมูลเป็นระบบของผู้ป่วยและจำนวนประชากรอิเล็กทรอนิกส์ที่จัดเก็บข้อมูลด้านสุขภาพในรูปแบบดิจิตอล[41,42] บันทึกเหล่านี้สามารถใช้ร่วมกันในการดูแลสุขภาพที่มีความแตกต่างกัน บันทึกข้อมูลผ่านเครือข่ายที่เชื่อมต่อระบบข้อมูลทั้งองค์กรหรือเครือข่ายข้อมูลและการแลกเปลี่ยนข้อมูลอื่น ๆ EHRs อาจรวมถึงช่วงของข้อมูลรวมทั้งประชากร, ประวัติทางการแพทย์ยาและโรคภูมิแพ้, สร้างภูมิคุ้มกันสถานะผลการทดสอบในห้องปฏิบัติการภาพรังสีวิทยาสัญญาณชีพสถิติส่วนบุคคล เช่น อายุ น้ำหนัก และข้อมูลการชำระเงิน[43],[44]

---

[40] the National Coordinator for Health Information Technology U.S. Department of Health and Human Services, HeathIT.gov, https://www.healthit.gov/providers-professionals/electronic-medical-records-emr

[41] An electronic health record (EHR), or electronic medical record (EMR), is the systematized collection of patient and population electronically-stored health information in a digital format

[42] Gunter, Tracy D; Terry, Nicolas P (2005). "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions," Journal of Medical Internet Research. 7 (1): e3.

[43] These records can be shared across different health care settings. Records are shared through network-connected, enterprise-wide information systems or other information networks and exchanges. EHRs may include a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information.

[44] "Mobile Tech Contributions to Healthcare and Patient Experience"

เวชระเบียนอิเล็กทรอนิกส์ (EMR) เป็นรูปแบบดิจิทัลของแผนภูมิกระดาษที่มีประวัติทางการแพทย์ของผู้ป่วยทั้งหมดจากการปฏิบัติอย่างหนึ่ง EMR ส่วนใหญ่ใช้โดยผู้ให้บริการสำหรับการวินิจฉัยและการรักษา[45]

ประโยชน์ของเวชระเบียนอิเล็กทรอนิกส์

EMR เป็นประโยชน์มากกว่าการบันทึกด้วยกระดาษเพราะช่วยให้ผู้ให้บริการ :

1. การติดตามข้อมูลตลอดเวลา (Track Data Over Time)

2. การคัดแยกผู้ป่วยซึ่งต้องเข้ารับการรักษา และการป้องกัน (Identify Patients Who Are Due for Preventive Visits and Screenings)

3. สังเกตการณ์ค่าพารามิเตอร์ของผู้ป่วยวัดว่าเป็นอย่างไร เช่น การฉีดวัคซีน และการอ่านค่าความดันโลหิต (Monitor How Patients Measure up to Certain Parameters, such as Vaccinations and Blood Pressure Readings)

4. ปรับปรุงคุณภาพโดยรวมของการดูแลในการปฏิบัติ (Improve Overall Quality of Care in a Practice)

ข้อมูลที่จัดเก็บใน EMR ไม่สามารถส่งต่อให้กับผู้ให้บริการได้ นอกจากการ บันทึกของผู้ป่วยอาจต้องพิมพ์ออกและส่งทางไปรษณีย์ไปยังผู้เชี่ยวชาญและสมาชิกคนอื่น ๆ ของทีมดูแล

---

[45] An electronic medical record (EMR) is a digital version of a paper chart that contains all of a patient's medical history from one practice. An EMR is mostly used by providers for diagnosis and treatment.

บทที่ 3
มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยในต่างประเทศและประเทศไทย

ในบทนี้จะทำการศึกษาถึงมาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีทางการแพทย์และข้อมูลส่วนบุคคล ซึ่งหลักการในการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยของต่างประเทศ และประเทศไทย รวมทั้งกฎหมายที่เกี่ยวข้องทั้งต่างประเทศและประเทศไทย ตามลำดับ

3.1 มาตรฐานระหว่างประเทศเกี่ยวกับเทคโนโลยีทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยในต่างประเทศ

การคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนขั้นพื้นฐานที่นานประเทศให้ความสำคัญเป็นอย่างมาก การคุ้มครองข้อมูลส่วนบุคคลจึงถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว ประเทศต่าง ๆ จึงมีมาตรการทางกฎหมายในการความคุ้มครองข้อมูลส่วนบุคคล และการความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยซึ่งรับบริการทางการแพทย์และจัดเก็บในรูปแบบอิเล็กทรอนิกส์

3.1.1 มาตรการทางกฎหมายที่เกี่ยวกับเครื่องมือแพทย์

ระบบการบริหาร (Total Quality Management หรือ TQM[46]) คือ การรวบรวมเอาความพยายามของทุกคนในองค์กร ทุกแผนก ทุกหน่วยงานที่เกี่ยวข้องกับการผลิตสินค้า หรือบริการเพื่อมุ่งสู่การพัฒนาคุณภาพในทุกขั้นตอนของกระบวนการให้บริการ และเพื่อสร้างความพึงพอใจที่ตรงตามความต้องการของลูกค้าอย่างแท้จริงวิธีการสำคัญที่ทำให้วิธีการบริหารงานโดยการมีส่วนร่วมของทุก

[46] ที คิว เอ็ม (TQM) ของ โรงพยาบาลราชวิถี

คนในองค์กรประสบความสำเร็จได้ คือ ผู้บริหารระดับสูงต้องมีความมุ่งมั่น และเข้าร่วมผลักดันอย่างอดทน และต่อเนื่องยาวนาน ขั้นตอนการเริ่มต้นในการนำ TQM เข้ามาใช้ในองค์กรอาจแตกต่างกันไปตามสภาพความเป็นจริงของแต่ละองค์กรอาจเริ่มต้น ณ จุดใดก็ได้ เช่น กิจกรรมกลุ่มพัฒนาคุณภาพ (QC) หรือ กลุ่มกิจกรรม 5 ส. เป็นต้น แต่มีข้อแม้ว่าต้องทำการบริหารคุณภาพในส่วนอื่น ๆ ให้ครบทุกหน่วยงานด้วย โดยมีต้นทุนที่ประหยัดที่สุด

มาตรฐานสถานพยาบาลระดับสากล[47] (Joint Commission International หรือ JCI)

มาตรฐาน JCI (Joint Commission International) อยู่ในการกำกับดูแลของ the Joint Commission ซึ่งเป็นสถาบันของสหรัฐอเมริกาที่ได้รับการยอมรับในระดับสากล เป็นองค์กรอิสระที่ไม่หวังผลกำไร และมีการดำเนินงานมานานกว่า 75 ปี โดยมีวัตถุประสงค์เพื่อส่งเสริมการพัฒนาคุณภาพและความปลอดภัยในการดูแลรักษาพยาบาลผู้ป่วยให้กับสถานพยาบาลต่าง ๆ ทั่วโลกอย่างต่อเนื่องด้วยการตรวจประเมินอย่างละเอียดถี่ถ้วน ตลอดจนให้การรับรองมาตรฐานคุณภาพแก่สถานพยาบาลที่มีคุณสมบัติเป็นไปตามข้อกำหนด ในปัจจุบันทั่วโลกมีสถานพยาบาลที่ผ่านการรับรองมาตรฐาน JCI แล้ว กว่า 300 แห่ง จาก 39 ประเทศ และสำหรับในประเทศไทยมีสถานพยาบาลที่ผ่านการรับรองมาตรฐาน JCI รวม 53 แห่ง ได้แก่ โรงพยาบาล 43 แห่ง และคลินิกอีก 10 แห่ง โดยกรมสนับสนุนบริการสุขภาพ[48] (สบส.) ก็ได้มีนโยบายพัฒนาและส่งเสริม ให้ความรู้สถานพยาบาลของประเทศไทยให้ได้รับการรับรองจากมาตรฐานสากล JCI มาอย่างต่อเนื่อง

การตรวจประเมินของ the Joint Commission เพื่อพิจารณารับรองสถานพยาบาลตามมาตรฐาน JCI นั้น ครอบคลุมทั้งการบริหารจัดการองค์กร ทิศทางและภาวะผู้นำ ระบบโครงสร้างความปลอดภัยทางกายภาพ ระบบการรองรับภาวะฉุกเฉิน ระบบการป้องกันและควบคุมการติดเชื้อ ระบบ

---

[47] "DHSS News," Website : http:// www.medicalhub.org

[48] กรมสนับสนุนบริการสุขภาพ เป็นกรมที่จัดตั้งใหม่ภายหลังจากการปรับบทบาทภารกิจและโครงสร้างกระทรวงสาธารณสุข ตาม พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 ซึ่งประกาศ ณ วันที่ 2 ตุลาคม พ.ศ. 2545 โครงสร้างใหม่ในส่วนของกระทรวงสาธารณสุข กำหนดให้มีการจัดกลุ่มภารกิจ (Cluster) ในการสนับสนุนหน่วยบริการสุขภาพในทุกระดับให้มีประสิทธิภาพในการดูแลสุขภาพของประชาชน โดยส่งเสริมสนับสนุน และพัฒนาระบบบริหารจัดการ ระบบบริการสุขภาพ และ ระบบคุ้มครองประชาชนด้านบริการสุขภาพ ทำให้ประชาชนมีสุขภาพที่ดีสามารถพิทักษ์สิทธิ และเข้าถึงบริการสุขภาพที่มีคุณภาพได้มาตรฐาน กระทรวงสาธารณสุข , https://hss.moph.go.th/index2.php?form=1

การสื่อสารและสารสนเทศ ระบบการบริหารจัดการทรัพยากรบุคคล ระบบคุณภาพและความปลอดภัยผู้ป่วย รวมไปถึงการพัฒนาและปรับปรุงคุณภาพการดูแลรักษาตั้งแต่ผู้ป่วยเข้ามาในโรงพยาบาลจนกระทั่งผู้ป่วยออกจากโรงพยาบาล โดยคำนึงถึงสิทธิผู้ป่วย การให้ข้อมูลเกี่ยวกับโรคและอาการที่เป็นตลอดจนการปฏิบัติที่ถูกต้องเพื่อให้กระบวนการดูแลรักษาเกิดผลลัพธ์ที่ให้ประโยชน์สูงสุดต่อผู้ป่วย โดยมาตรฐาน JCI ที่ต้องรับการตรวจประเมินประกอบไปด้วย 2 หมวดหลัก ๆ ได้แก่

1) มาตรฐานที่เน้นผู้ป่วยเป็นศูนย์กลาง ประกอบไปด้วย เป้าหมายความปลอดภัยผู้ป่วยสากล (IPSG) การเข้าถึงการดูแลและความต่อเนื่องของการดูแล (ACC) สิทธิผู้ป่วยและครอบครัว (PFR) การประเมินผู้ป่วย (AOP) การดูแลผู้ป่วย (COP) การดูแลด้านวิสัญญีและศัลยกรรม (ASC) การจัดการด้านยาและการใช้ยา (MMU) การให้ความรู้แก่ผู้ป่วยและครอบครัว (PFE)

2) มาตรฐานการจัดการสถานพยาบาล ประกอบไปด้วย การพัฒนาคุณภาพและความปลอดภัยผู้ป่วย (QPS) การป้องกันแลควบคุมการติดเชื้อ (PCI) การกำกับดูแลกิจการ การนำ และทิศทางองค์กร (GLD) การจัดการและความปลอดภัยในอาคารสถานที่ (FMS) คุณสมบัติและการฝึกอบรมของบุคลากร (SQE) และการจัดการสารสนเทศ (MOI)

มาตรฐาน JCI นี้ สถานพยาบาลที่ได้รับการรับรองแล้วจะแตกต่างจากสถานพยาบาลที่ยังไม่ได้รับการรับรองอย่างไร ต้องบอกเลยว่าสถานพยาบาลที่ผ่านมาตรฐาน JCI แล้วนั้น จะทำให้ให้ผู้ป่วยหรือผู้รับบริการได้รับการรักษาพยาบาลที่มีคุณภาพทัดเทียมกับสถานพยาบาลในประเทศยุโรปและสหรัฐอเมริกาและมีมาตรฐานด้านความปลอดภัยสูงสุด เนื่องจากสถานพยาบาลที่ผ่านมาตรฐาน JCI จะต้องมีแนวทางการปฏิบัติ อย่างเคร่งครัด ดังต่อไปนี้

1. ระบุตัวผู้ป่วยถูกต้อง (ถูกคน) เพื่อให้ผู้รับบริการสามารถมั่นใจได้ว่าจะได้รับการรักษาที่ถูกต้องและถูกคน

2. บุคลากร ในทีมดูแลผู้ป่วยจะต้องมีการสื่อสารระหว่างกันที่ชัดเจนและมี ประสิทธิภาพเพื่อป้องกันความผิดพลาดจากการสื่อสารข้อมูลการรักษาพยาบาล

3. ผู้ป่วยจะได้รับการดูแลและเฝ้าระวังหากมีการใช้ยาที่ต้องระมัดระวังสูง

4. ผู้ป่วยได้รับการผ่าตัดที่ถูกตำแหน่ง ถูกหัตถการ ถูกคน

5. ผู้ป่วยจะปลอดภัยจากการติดเชื้อในโรงพยาบาล โดยมุ่งเน้นให้บุคลากรในทีมดูแลผู้ป่วย ญาติ และผู้ที่มาเยี่ยมผู้ป่วยล้างมืออย่างถูกต้องเพื่อป้องกันการนำเชื้อโรคไปสู่ผู้ป่วย

6. ผู้ป่วยจะได้รับการประเมินความเสี่ยงต่อการพลัดตกหกล้มและได้รับการเฝ้า ระวังในทุกจุดบริการ เพื่อลดความเสี่ยงต่อการเกิดภยันตรายของผู้ป่วยจากภาวะพลัดตกหกล้มในโรงพยาบาล

การเข้ารับการรักษาพยาบาล หากต้องการทราบว่าโรงพยาบาลใดได้รับการรับรองมาตรฐาน JCI สามารถสังเกตได้จากตราสัญลักษณ์ และในประเทศไทยมีโรงพยาบาลที่มีคุณภาพมาตรฐาน ซึ่งได้รับการยอมรับและรับรองคุณภาพในระดับสากลแล้วถึง 53 แห่ง

3.1.2 กฎเกณฑ์กฎหมายระหว่างประเทศเกี่ยวกับข้อมูลส่วนบุคคลทางการแพทย์

สิทธิมนุษยชน (Human Right)

สิทธิมนุษยชน (Human Right) หมายถึง สิทธิที่มนุษย์ทุกคนมีความเท่าเทียมกัน มีศักดิ์ศรีของความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลที่ได้รับการรับรอง ทั้งความคิดและการกระทำที่ไม่มี การล่วงละเมิดได้ โดยได้รับการ คุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย และสนธิสัญญาระหว่างประเทศ

(1) ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนแห่งสหประชาชาติ (Universal Declaration of Human Rights)

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนแห่งสหประชาชาติ เป็นข้อตกลงที่องค์การสหประชาชาติได้กำหนดขึ้น ในการวางกรอบเบื้องต้นเกี่ยวกับสิทธิมนุษยชนและเป็นเอกสารหลักด้านสิทธิมนุษยชนฉบับแรก ซึ่งที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ .ให้การรับรอง เพื่อให้ประเทศสมาชิกทั้งหลายใช้เป็นแนวทางในการคุ้มครองดูแลสิทธิและเสรีภาพของพลเมืองในประเทศของตน

วันที่ 10 ธันวาคม ค.ศ.1948 (พ.ศ. 2491) ประเทศสมาชิกสหประชาชาติได้รับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Right: UDHR) โดยสมัชชาแห่งสหประชาชาติ ถือเป็นการกำหนดมาตรฐานสากลด้านสิทธิมนุษยชนซึ่งไทยเป็นประเทศหนึ่งที่ร่วมกับประเทศต่าง ๆ ให้การรับรอง ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนแห่งสหประชาชาติ สิทธิเด่น ๆ ที่ระบุไว้ในปฏิญญาสากล ว่าด้วยสิทธิมนุษยชน สิทธิต่อชีวิต เสรีภาพและความปลอดภัยของบุคคล การศึกษา เสรีภาพทางความคิด มโนธรรมและศาสนา เสรีภาพแห่งความคิดเห็น การแสดงออก การมีงานทำ การแสวงหาและได้รับการลี้ภัย ในประเทศอื่น เป็นต้น วันแห่งสิทธิมนุษยชนโลก ตรงกับวันที่ 10 ธันวาคม

หน่วยงานในสหประชาชาติ (UN) ที่รับผิดชอบปัญหาสิทธิ มนุษยชน (HR) คือสำนักงานข้าหลวงใหญ่สิทธิมนุษยชน ที่นครเจนีวา[49] (ชื่อเดิมคือ Centre for Human Rights) ประเทศสวิตเซอร์แลนด์

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน พ.ศ. 2491 ที่บรรดาประเทศสมาชิกองค์การสหประชาชาติ ได้ร่วมรับรองเมื่อ ค.ศ. 1948 (พ.ศ. 2491) ถือเป็นมาตรฐานในการปฏิบัติต่อกันของมวลมนุษย์และของนานาชาติโดยถือเป็นหลักเกณฑ์สำคัญในการปฏิบัติเกี่ยวกับสิทธิมนุษยชนที่บรรดาประเทศต่าง ๆ ทั่วโลกยอมรับเป็นพื้นฐานในการดำเนินงานขององค์การสหประชาชาติ และมีอิทธิพลสำคัญต่อการร่างรัฐธรรมนูญของประเทศที่มีการร่างรัฐธรรมนูญในเวลาต่อมา

ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนได้มีการรับรองสิทธิดังกล่าว ไว้ใน ข้อ 12 บุคคลใดจะถูกแทรกแซงตามอำเภอใจ ในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น[50]

(2.) ความเป็นส่วนตัวทางการแพทย์

ความเป็นส่วนตัวทางการแพทย์หรือความเป็นส่วนตัวด้านสุขภาพคือการปฏิบัติในการรักษาความปลอดภัยและความลับของบันทึกผู้ป่วย มันเกี่ยวข้องกับดุลยพินิจการสนทนาของผู้ให้บริการด้านการดูแลสุขภาพและความปลอดภัยของเวชระเบียน เงื่อนไขยังสามารถอ้างถึงความเป็นส่วนตัวทางกายภาพของผู้ป่วยจากผู้ป่วยรายอื่นและผู้ให้บริการในขณะที่อยู่ในสถานพยาบาล ความกังวลที่ทันสมัยรวมถึงระดับของการเปิดเผยข้อมูลต่อ บริษัท ประกันภัยนายจ้างและบุคคลที่สามอื่น ๆ การถือกำเนิดของเวชระเบียนอิเล็กทรอนิกส์ (EMR) และระบบการจัดการดูแลผู้ป่วย (PCMS) ทำให้เกิด

---

[49] เจนีวา (Geneva) เป็นเมืองใหญ่อันดับสองของประเทศสวิตเซอร์แลนด์ ถือเป็นเมืองที่มีประชากรมากที่สุดในภาครอมองดีอันเป็นภูมิภาคที่ใช้ภาษาฝรั่งเศสเป็นหลักในสวิตเซอร์แลนด์ นครเจนีวาตั้งอยู่บริเวณต้นแม่น้ำโรนซึ่งไหลออกจากทะเลสาบเจนีวา เจนีวามีสถานะเป็นเมืองหลวงของสาธารณรัฐแห่งรัฐเจนีวา

[50] Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ความกังวลใหม่เกี่ยวกับความเป็นส่วนตัวสมดุลกับความพยายามในการลดความซ้ำซ้อนของบริการและข้อผิดพลาดทางการแพทย์[51,52]

หลายประเทศรวมถึงออสเตรเลีย[53] แคนาดา ตุรกี สหราชอาณาจักร สหรัฐอเมริกา นิวซีแลนด์ และเนเธอร์แลนด์ได้ออกกฎหมายที่พยายามปกป้องความเป็นส่วนตัวของผู้คน อย่างไรก็ตามกฎหมายเหล่านี้จำนวนมากได้พิสูจน์แล้วว่ามีประสิทธิภาพน้อยกว่าในทางทฤษฎี[54] สหรัฐอเมริกาได้ผ่านรัฐบัญญัติประกันสุขภาพพกพาและรัฐบัญญัติความรับผิดชอบ (Health Insurance Portability and Accountability Act : HIPAA) ในฐานะที่เป็นความพยายามที่จะเพิ่มความระมัดระวังความเป็นส่วนตัวภายในสถาบันการแพทย์[55]

ก่อนที่จะมีความก้าวหน้าทางเทคโนโลยีสถาบันทางการแพทย์ต้องอาศัยสื่อกลางในการจัดเก็บข้อมูลทางการแพทย์ของแต่ละบุคคล ทุกวันนี้มีการจัดเก็บข้อมูลมากขึ้นภายในฐานข้อมูล

---

[51] Hiller, Mare (1982). " "Patient Care Management Systems, Medical Records, and Privacy: A Balancing Act." " (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1424350). Public Health Reports. 97: 332–45. PMC 1424350 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1424350) – via JSTOR.

[52] Miller, Amalia (2009). " "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." ". Management Science. 55: 1077–1093. doi:10.1287/mnsc.1090.1014 (https://doi.org/10.1287%2Fmnsc.1090.1014) – via JSTOR.

[53] Manager, Web (201 1 -09-28). " Australian Privacy Law & Practice - Key Recommendations for Health Information Privacy Reform" (https://www.alrc.gov.au/news-media/201 1/australian-privacy-law-practice-key-recommendations-health-information-privacy-refor). www.alrc.gov.au. Retrieved 2018-12-03.

[54] Andriole, Katherine P. (201 4). " Security of Electronic Medical Information and Patient Privacy: What You Need to Know" . Journal of the American College of Radiology. 1 1 : 1 21 2–1 21 6. doi:10.1016/j.jacr.2014.09.011 (https://doi.org/10.1016%2Fj.jacr.2014.09.011).

[55] Edemekong, Peter F.; Haydel, Micelle J. (201 8), "Health Insurance Portability and Accountability Act (HIPAA)" (https://www.ncbi.nlm.nih.gov/books/NBK50001 9/), StatPearls, StatPearls Publishing, PMID 29763195 (https://www.ncbi.nlm.nih.gov/pubmed/29763195), retrieved 2018-12-03

อิเล็กทรอนิกส์[56] การวิจัยแสดงให้เห็น[57] ปลอดภัยกว่าที่จะเก็บข้อมูลไว้ในกระดาษเพราะการขโมยข้อมูลทางกายภาพนั้นยากกว่าในขณะที่ข้อมูลดิจิตอลมีความเสี่ยงต่อการเข้าถึงโดยแฮคเกอร์ (Hacker)[58]

เพื่อที่จะปฏิรูปปัญหาความเป็นส่วนตัวด้านการดูแลสุขภาพในต้นปี ค.ศ. 1990 (พ.ศ. 2533) นักวิจัยได้พิจารณาการใช้บัตรเครดิตและ “Smart Card” เพื่อให้สามารถเข้าถึงข้อมูลทางการแพทย์ของพวกเขาได้โดยไม่ต้องกลัวว่าจะถูกขโมยข้อมูล “Smart Card” อนุญาตให้จัดเก็บและประมวลผลข้อมูลเพื่อจัดเก็บใน Microchip เอกพจน์ แต่ผู้คนกลัวว่าจะมีข้อมูลมากมายที่เก็บไว้ในจุดเดียวที่สามารถเข้าถึงได้ง่าย “Smart Card” นี้ รวมหมายเลขประกันสังคมของบุคคล นี่เป็นส่วนสำคัญของการระบุตัวตนที่สามารถนำไปสู่การขโมยข้อมูลส่วนบุคคลหากฐานข้อมูลถูกละเมิด นอกจากนี้ยังมีความกลัวว่าผู้คนจะกำหนดเป้าหมายบัตรการแพทย์เหล่านี้เพราะพวกเขามีข้อมูลที่สามารถเป็นประโยชน์ต่อบุคคลที่สามที่แตกต่างกันมากมายรวมถึงนายจ้าง บริษัท ยานักการตลาดยาและผู้ตรวจสอบการประกันภัย[59]

เพื่อตอบสนองต่อการขาดความเป็นส่วนตัวทางการแพทย์มีการเคลื่อนไหวเพื่อสร้างการป้องกันความเป็นส่วนตัวทางการแพทย์ที่ดีขึ้น สำนักข้อมูลการแพทย์จึงถูกสร้างขึ้นเพื่อป้องกันการฉ้อโกงประกันภัย แต่มันก็กลายเป็นแหล่งข้อมูลทางการแพทย์ที่สำคัญสำหรับ บริษัท ประกันชีวิต กว่า 750 แห่ง ดังนั้น จึงเป็นสิ่งที่อันตรายมากเนื่องจากเป็นเป้าหมายของการละเมิดความเป็นส่วนตัว แม้ว่าระบบการจัดเก็บข้อมูลอิเล็กทรอนิกส์ของข้อมูลทางการแพทย์จะเพิ่มประสิทธิภาพและลดค่าใช้จ่ายใน

---

[56] Alpert, Sheri,“Smart Cards, Smarter Policy Medical Records, Privacy, and Health Care Reform,” The Hastings Center Report. 23: 13–23. Doi :10.2307/3562918, (1993), (https://doi.org/10.2307%2F3562918) – via JSTOR.

[57] Andriole, Katherine P, “Security of Electronic Medical Information and Patient Privacy: What You Need to Know,” Journal of the American College of Radiology. 11: 1212–1216. doi:10.1016/j.jacr.2014.09.011, (2014), (https://doi.org/10.1016%2Fj.jacr.2014.09.011).

[58] คำนี้เป็นชื่อที่ใช้เรียกพวกที่มีความชำนาญในการใช้คอมพิวเตอร์ไปในทางที่ผิดกฎหมาย เช่น แอบขโมยข้อมูลจากคอมพิวเตอร์ในเครือข่าย หรือแอบแก้ตัวเลขในธนาคารเพื่อถอนเงินออกมาใช้เอง คำว่า hack อาจหมายถึงการแอบปรับแก้หรือดัดแปลงโปรแกรมคอมพิวเตอร์โดยไม่ถูกต้องตามกฎหมาย หรือไม่ก็แก้แล้วยิ่งกลับทำให้แย่ลง ; พจนานุกรมคำศัพท์คอมพิวเตอร์

[59] Alpert, Sheri, “Smart Cards, Smarter Policy Medical Records, Privacy, and Health Care Reform,” The Hastings Center Report. 23: 13–23. Doi :10.2307/3562918, (1993), (https://doi.org/10.2307%2F3562918) – via JSTOR.

การบริหารลง แต่ก็มีแง่ลบที่ต้องพิจารณา ระบบการจัดเก็บข้อมูลทางอิเล็กทรอนิกส์ช่วยให้ข้อมูลของบุคคลนั้นอ่อนไหวต่อบุคคลภายนอกมากขึ้น แม้ว่าข้อมูลของพวกเขาจะถูกเก็บไว้ในการ์ดเอกพจน์ ดังนั้นบัตรทางการแพทย์จึงทำหน้าที่เป็นความปลอดภัยที่ผิดพลาดเนื่องจากไม่ได้ป้องกันข้อมูลของพวกเขาอย่างสมบูรณ์[60]

(3) ประวัติความเป็นส่วนตัวและสุขภาพอิเล็กทรอนิกส์ (EHRs)

สามเป้าหมายของความปลอดภัยของข้อมูลรวมถึงความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ มีความลับความสมบูรณ์และความพร้อมใช้งานองค์กรต่าง ๆ พยายามที่จะบรรลุเป้าหมายเหล่านี้ ซึ่งเรียกว่า “C.I.A Triad” ซึ่งเป็น "การปฏิบัติเพื่อปกป้องข้อมูลจากการเข้าถึงการใช้การเปิดเผยการหยุดชะงักการดัดแปลงการตรวจสอบการบันทึกหรือการทำลาย"[61]

ในบทบรรณาธิการ 2004 (พ.ศ. 2547) ใน Washington Post วุฒิสมาชิกสหรัฐ Bill Frist และ Hillary Clinton สนับสนุนการสังเกตนี้โดยระบุว่า "[ผู้ป่วย] ต้องการ ... ข้อมูลรวมถึงการเข้าถึงบันทึกสุขภาพของตนเอง ... ในเวลาเดียวกันเราต้องมั่นใจว่า ความเป็นส่วนตัวของระบบหรือจะทำลายความน่าเชื่อถือที่ถูกออกแบบมาเพื่อสร้าง" มีรายงานปี 2548 โดย California Health Care Foundation พบว่า

---

[60] In response to the lack of medical privacy, there was a movement to create better medical privacy protection, but nothing has been officially passed. The Medical Information Bureau was thus created to prevent insurance fraud, yet it has since become a significant source of medical information for over 750 life insurance companies; thus, it is very dangerous as it is a target of privacy breachers. Although the electronic filing system of medical information has increased efficiency and administration costs have been reduced, there are negative aspects to consider. The electronic filing system allows for individual's information to be more susceptible to outsiders; even though their information is stored on a singular card. Therefore, the medical card serves as a false sense of security as it does not protect their information completely.

[61] The three goals of information security, including electronic information security, are confidentiality, integrity, and availability. Organizations are attempting to meet these goals, referred to as the C.I.A. Triad, which is the “practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction,”

"ร้อยละ 67 ของผู้ตอบแบบสอบถามระดับชาติรู้สึกว่า 'ค่อนข้าง' หรือ 'กังวลมาก' เกี่ยวกับความเป็นส่วนตัวของเวชระเบียนส่วนตัวของพวกเขา"[62]

ความสำคัญของความเป็นส่วนตัวในเวชระเบียนสุขภาพอิเล็กทรอนิกส์นั้นมีความโดดเด่นด้วยเนื้อเรื่องของพระราชบัญญัติการกู้คืนและการลงทุนใหม่ของอเมริกา (ARRA) ในปี 2009 (พ.ศ. 2552) หนึ่งในบทบัญญัติ (รู้จักกันในนามของเทคโนโลยีสารสนเทศด้านสุขภาพสำหรับเศรษฐกิจและคลินิกสุขภาพ แรงจูงใจที่ได้รับคำสั่งจากแพทย์สำหรับการดำเนินการด้านสุขภาพอิเล็กทรอนิกส์ภายในปี 2558 ผู้สนับสนุนความเป็นส่วนตัวในสหรัฐอเมริกาได้เพิ่มความกังวลเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตเนื่องจากการปฏิบัติทางการแพทย์ที่เปลี่ยนไปจากเวชระเบียนอิเล็กทรอนิกส์ สำนักงานผู้ประสานงานแห่งชาติสำหรับเทคโนโลยีสารสนเทศด้านสุขภาพ (ONC) อธิบายว่ามาตรการความปลอดภัยบางอย่างที่ระบบ EHR สามารถใช้เป็นรหัสผ่านและ Pin Numbers ที่ควบคุมการเข้าถึงระบบดังกล่าวการเข้ารหัสข้อมูลและเส้นทางการตรวจสอบเพื่อติดตาม การเปลี่ยนแปลงที่ทำกับบันทึก[63]

การให้สิทธิการเข้าถึง EHRs แก่ผู้ป่วยนั้นได้รับคำสั่งจากกฎความเป็นส่วนตัวของ HIPAA อย่างเคร่งครัด การศึกษาหนึ่งพบว่าในแต่ละปีมีประมาณ 25 ล้านอนุมัติที่ถูกบังคับสำหรับการเปิดตัวของบันทึกสุขภาพส่วนบุคคล อย่างไรก็ตามนักวิจัยพบว่าภัยคุกคามความปลอดภัยแบบใหม่เปิดออกมา

---

[62] In a 2004 editorial in the Washington Post, U.S. Senators Bill Frist and Hillary Clinton supported this observation, stating" [patients] need...information, including access to their own health records... At the same time, we must ensure the privacy of the systems, or they will undermine the trust they are designed to create," A 2005 report by the California Health Care Foundation found that "67 percent of national respondents felt 'somewhat' or 'very concerned' about the privacy of their personal medical records".

[63] The importance of privacy in electronic health records became prominent with the passage of the American Recovery and Reinvestment Act (ARRA) in 2009. One of the provisions (known as the Health Information Technology for Economic and Clinical Health [HITECH] Act) of the ARRA mandated incentives to clinicians for the implementation of electronic health records by 2015.Privacy advocates in the United States have raised concerns about unauthorized access to personal data as more medical practices switch from paper to electronic medical records. The Office of the National Coordinator for Health Information Technology (ONC) explained that some of the safety measures that EHR systems can utilize are passwords and pin numbers that control access to such systems, encryption of information, and an audit trail to keep track of the changes made to records.

ภัยคุกคามความปลอดภัยและความเป็นส่วนตัวเหล่านี้ ได้แก่ แฮคเกอร์, ไวรัส (Viruses[64]) และหนอนคอมพิวเตอร์ (Worms[65]) ภัยคุกคามความเป็นส่วนตัวเหล่านี้มีความโดดเด่นมากขึ้นจากการเกิดขึ้นของ "Cloud Computing" ซึ่งเป็นการใช้พลังการประมวลผลของคอมพิวเตอร์ที่ใช้ร่วมกัน องค์กรด้านการดูแลสุขภาพกำลังเพิ่มการใช้ Cloud Computing เป็นวิธีจัดการกับข้อมูลจำนวนมาก อย่างไรก็ตามการจัดเก็บข้อมูลประเภทนี้มีความอ่อนไหวต่อภัยธรรมชาติไซเบอร์อาชญากรรมและการก่อการร้ายทางเทคโนโลยีและความล้มเหลวของฮาร์ดแวร์ การละเมิดข้อมูลด้านสุขภาพคิดเป็นร้อยละ 39 ของการละเมิดทั้งหมดในปี พ.ศ. 2558 ค่าใช้จ่ายด้านความปลอดภัยและการใช้งานด้านไอทีนั้นเป็นสิ่งจำเป็นเพื่อปกป้องสถาบันสุขภาพจากการรักษาความปลอดภัย[66]

---

[64] โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงว่าไวรัสได้เข้าไปผังตัวอยู่ในหน่วยความจำ คอมพิวเตอร์ เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัสแต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่น ๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือ แสดงข้อความวิ่งไปมาบน หน้าจอ เป็นต้น ; https://web.ku.ac.th/schoolnet/snet1/software/virus/index.html

[65] หนอนคอมพิวเตอร์ หรือ คอมพิวเตอร์เวิร์ม หรือบางทีเรียกกันว่าเวิร์ม คือหน่วยย่อยลงมาจากไวรัสคอมพิวเตอร์ ปกติแล้ว หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่นระบบเครือข่ายหรืออินเทอร์เน็ตเป็นต้น หนอนคอมพิวเตอร์สามารถทำลายข้อมูลและแบนด์วิดท์สร้างความเสียหายให้กับคอมพิวเตอร์รวมไปถึงการทำให้คอมพิวเตอร์หยุดทำงานอีกด้วย ; https://th.wikipedia.org/wiki/%E0%B8%AB%E0%B8%99%E0%B8%AD%E0%B8%99%E0%B8%84%E0%B8%AD%E0%B8%A1%E0%B8%9E%E0%B8%B4%E0%B8%A7%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C

[66] Angst, Corey M., Emily S. Block, John D' Arcy, and Ken Kelley. 201 7. "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches." MIS Quarterly 41(3):893–916.

ในลำดับต่อไปได้ทำการศึกษาถึงมาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีทางการแพทย์ และข้อมูลส่วนบุคคลของผู้ป่วย ทั้งในประเทศระบบกฎหมายจารีตประเพณี (Common Law System) ได้แก่ เครือรัฐออสเตรเลีย สหราชอาณาจักร สหรัฐอเมริกา และประเทศระบบกฎหมายลายลักษณ์อักษร (Civil Law System) ได้แก่ สหภาพยุโรป (ยุโรปภาคพื้นทวีป) และสหพันธ์สาธารณรัฐเยอรมนี ซึ่งมีรายละเอียดดังนี้

3.2 สหภาพยุโรป (European Union : EU)

[67]สหภาพยุโรปมีหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจแบ่งเป็นสองกลุ่มคือ กฎหมายเฉพาะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งวางหลักการคุ้มครองข้อมูลส่วนบุคคลประการต่าง ๆ ไว้โดยเฉพาะ และกฎหมายเกี่ยวกับสิทธิมนุษยชน ซึ่งวางหลักทั่วไปหรือหลักกว้าง ๆ ในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลไว้ในส่วนนี้จะได้ชี้ให้เห็นกรอบกฎหมายยุโรปที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลทั้งสองกลุ่มดังนี้

(1) หลักกฎหมายเฉพาะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล Directive 95/46/EC หรือ Directive 95/46/ECon the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of such Data เป็นกฎเกณฑ์ที่บัญญัติขึ้นโดยคณะกรรมาธิการยุโรป European Economic Community ใน ค.ศ. 1995 (พ.ศ. 2538) Directive นี้ถือเป็นหลักเกณฑ์ต้นแบบ (Model) อันเป็นที่มาของการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกต่าง ๆ ในยุโรป

Directive 95/46/EC มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในความเป็นอยู่ส่วนตัวอันเนื่องจากการประมวลผลข้อมูลส่วนบุคคลตามที่บัญญัติไว้อย่างชัดเจนในมาตราที่ 1 นอกจากนี้ อารัมภบทที่ 2 ยังได้อธิบายเพิ่มเติมว่า “ระบบประมวลผลข้อมูลนั้นถูกออกแบบมาเพื่ออำนวยประโยชน์แก่มนุษย์... ระบบเหล่านี้ต้องเคารพสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยไม่เลือกสัญชาติหรือถิ่นที่อยู่ของบุคคลนั้นโดยเฉพาะสิทธิในความเป็นส่วนตัว”

นอกจากนี้ ในอารัมภบทที่ 10 ได้อธิบายว่า “ประมวลกฎหมายภายในประเทศว่าด้วยการประมวลข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐาน โดยเฉพาะสิทธิใน

---

[67] รองศาสตราจารย์คณาธิป ทองรวีวงศ์, รายงานวิจัยฉบับสมบูรณ์ เรื่อง การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน The Personal Data Protection Law Reform for ASEAN, น. 46.

ความเป็นส่วนตัว ซึ่งได้รับความเห็นชอบในมาตรา 8 ของอนุสัญญาเพื่อคุ้มครอง สิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรปและในหลักทั่วไปของกฎหมายประชาคม ด้วยเหตุนั้นการปรับกฎหมายเหล่านี้ให้สอดคล้องกันจะต้องมิทำให้การคุ้มครองที่พึงได้ของพวกเขานั้นย่อหย่อนลง แต่ในทางกลับกันต้องแสวงหาวิธีที่จะรับรองการคุ้มครองขั้นสูงในประชาคม" ดังนั้นจะเห็นได้ว่า กฎหมายสหภาพยุโรปมุ่งเน้นให้เกิดความเป็นเอกภาพของกฎหมายคุ้มครองข้อมูลของประเทศในยุโรป

สำหรับหลักการที่สำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้น Directive 95/46/EC มีดังนี้

1. ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

2. ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (Specified, Explicit and Legitimate Purposes) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์

3. ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (Adequate) ไม่มากเกินความจำเป็น (Not Excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

4. ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และในกรณีจำเป็นต้องเป็นปัจจุบันด้วย

5. ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของไว้นานเกินไปอีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนั้น ยังได้วางหลัก ข้อมูลชนิดที่มีความอ่อนไหว (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสม

หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลใน Directive 95/46/EC โดยทั่วไปแล้วจะเห็นได้ว่า มีเนื้อหาที่กว้างขวางกว่าหลักการคุ้มครองข้อมูลส่วนบุคคลใน OECD Guidelines เช่น ได้มีการเพิ่มเติมหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลชนิดที่มีความอ่อนไหว (Sensitive Data) ว่าห้ามมิให้มีการประมวลผลข้อมูลดังกล่าวเว้นแต่จะเข้ากรณีข้อยกเว้น หลักเกณฑ์การแจ้งรายละเอียดเกี่ยวกับการประมวลผลต่อองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคล สิทธิในการ "Op – Out" สำหรับการนำข้อมูลส่วนบุคคลไปใช้เพื่อประโยชน์ในการทำการตลาดแบบตรง (Direct Marketing) เป็นต้น

ข้อยกเว้นตามกฎหมาย

มาตรา 26 (1) Directive 95/46/EC อนุญาตให้มีการโอนข้อมูลส่วนบุคคลได้หากเข้ากรณีดังต่อไปนี้

a) เจ้าของข้อมูลยินยอมให้มีการโอนข้อมูลอย่างชัดแจ้ง

b) การโอนข้อมูลเป็นสิ่งจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลหรือการดำเนินการก่อนการเข้าสัญญาตามที่เจ้าของข้อมูลร้องขอ

c) การโอนข้อมูลเป็นสิ่งจำเป็นต่อการหาข้อสรุปของสัญญาหรือการปฏิบัติตามสัญญาซึ่งทำเพื่อผลประโยชน์ของเจ้าของข้อมูลที่ได้จัดทำขึ้นระหว่างผู้ควบคุมข้อมูลและบุคคลภายนอก

e) การโอนข้อมูลเป็นสิ่งจำเป็นในการคุ้มครองผลประโยชน์สำคัญของเจ้าของข้อมูล

f) การโอนข้อมูลโดยเก็บบันทึกข้อมูลซึ่งตามกฎหมายหรือระเบียบมีหน้าที่ให้ต่อสาธารณชนและซึ่งเปิดให้มีการเข้าค้นหาข้อมูลได้ทั้งโดยบุคคลทั่ว ๆ ไปหรือโดยบุคคลใดบุคคลหนึ่งซึ่งสามารถแสดงได้ว่าตนมีประโยชน์ส่วนได้เสียที่ชอบด้วยกฎหมายโดยเฉพาะภายใต้ขอบเขตว่าประโยชน์ดังกล่าวนั้นจะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้โดยกฎหมายที่ให้เปิดเผยในกรณีนั้น ๆ

(2) หลักกฎหมายสิทธิมนุษยชนยุโรป หลักกฎหมายเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลปรากฏในกฎหมายสิทธิมนุษยชนของยุโรป ดังนี้

อนุสัญญาสิทธิมนุษยชนยุโรป (The European Convention on Human Rights หรือ ECHR)

มาตรา 8 มีหลักว่า “บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองในชีวิตส่วนตัวครอบครัว ที่อยู่อาศัย และการสื่อสาร หน่วยงานของรัฐจะไม่แทรกแซงในการที่บุคคลจะใช้สิทธิดังกล่าว เว้นแต่เป็นการแทรกแซงบนพื้นฐานของกฎหมายที่มีความจำเป็นตามระบอบประชาธิปไตยที่เกี่ยวข้องกับประโยชน์ด้านความมั่นคงของรัฐ ความปลอดภัยสาธารณะ..เพื่อป้องกันอาชญากรรม เพื่อปกป้องสุขภาพหรือศีลธรรม หรือเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น”[68]

---

[68] Article 8–Right to respect for private and family life1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Article 8 ECHR)

ข้อบังคับ EU ใหม่เกี่ยวกับการปกป้องข้อมูลส่วนบุคคล : ผู้ป่วยมีความหมาย[69]

ในเดือนพฤษภาคม ค.ศ. 2016 (พ.ศ. 2559) สหภาพยุโรปได้ใช้ระเบียบใหม่ (EU) 2016/679 ในการปกป้องข้อมูลส่วนบุคคล Forum ผู้ป่วยชาวยุโรปได้สนับสนุนอย่างแข็งขันสำหรับวิธีการที่สมดุลเพื่อปกป้องความเป็นส่วนตัวของผู้ป่วยในขณะที่มั่นใจว่าข้อมูลของผู้ป่วยสามารถใช้ร่วมกันเพื่อวัตถุประสงค์ด้านการดูแลสุขภาพและการวิจัยตั้งแต่การเผยแพร่ข้อเสนอสำหรับกฎระเบียบในปี 2012 ได้รับข้อมูลที่ดีขึ้นเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของพวกเขาและให้ความรับผิดชอบที่ชัดเจนยิ่งขึ้นต่อบุคคลและองค์กรที่ใช้ข้อมูลส่วนบุคคล[70]

เอกสารนี้สรุปความหมายของกฎหมายใหม่นี้จากมุมมองของผู้ป่วยและวิธีการที่องค์กรของผู้ป่วยสามารถมีส่วนร่วมในการรับรองว่าสิทธิของผู้ป่วยในการรักษาความเป็นส่วนตัวการแบ่งปันข้อมูลและการเข้าถึงข้อมูลด้านสุขภาพของพวกเขา[71]

ข้อมูลส่วนบุคคล คือ [72]ข้อมูลส่วนบุคคลคือข้อมูลเกี่ยวกับบุคคลธรรมดาที่อนุญาตหรือสามารถระบุตัวบุคคลได้ มันเป็นสิ่งสำคัญที่จะต้องแยกแยะระหว่างข้อมูลที่สามารถระบุตัวตนได้ (แม้ว่าจะเป็นรหัสที่สำคัญ) และข้อมูลที่ถูกเปิดเผยโดยไม่ระบุชื่ออย่างสมบูรณ์เนื่องจากข้อบังคับนี้ใช้กับข้อมูลในอดีตและไม่ใช่ในภายหลัง (การบรรยาย 36) มันอาจเป็นข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลไม่

---

[69] The new EU Regulation on the protection of personal data: what does it mean for patients?

[70] In May 2016, the European Union adopted a new Regulation (EU) 2016/679 on the protection of personal data. The European Patients' Forum has actively advocated for a balanced approach to protect patients' privacy while ensuring patient's data can be shared for healthcare and research purposes since the publication of the proposal for a regulation in 2012. The final Regulation provides more rights to citizens to be better informed about the use made of their personal data, and gives clearer responsibilities to people and entities using personal data.

[71] This document outlines what this new legislation means from a patients' perspective and how patients' organisations can contribute to ensuring that patients' rights to privacy, data sharing, and accessing their health data are implemented optimally.

[72] Personal data is information about a particular natural person that allows, or could allow identifying the person. It is important to distinguish between identifiable data (even if it is key coded) and data that is rendered completely anonymous, as the Regulation applies to the former, and not the later (Recital 36). It may be any information relating to an individual, whether it relates to his or her private, professional or public life. To be covered by the Regulation the data need to be collected and used by someone else (a person or legal entity).

ว่าจะเกี่ยวข้องกับชีวิตส่วนตัวอาชีพหรือสาธารณะ เพื่อให้ครอบคลุมโดยกฎระเบียบข้อมูลจะต้องมีการรวบรวมและใช้งานโดยบุคคลอื่น (บุคคลหรือนิติบุคคล)

(3) สิทธิตามกฎหมายของสหภาพยุโรปแก่ผู้ป่วยเกี่ยวกับข้อมูล

กฎระเบียบใหม่พยายามที่จะช่วยให้ประชาชนมีสิทธิที่จะได้รับแจ้งและทำให้พวกเขาควบคุมข้อมูลส่วนบุคคลได้มากขึ้น สิทธิเหล่านี้มีผลบังคับใช้กับผู้ป่วยในการดูแลสุขภาพ พวกเขายังใช้ในการวิจัยแม้ว่าในกรณีนี้อาจมีการยกเว้นตามสัดส่วนที่กำหนดโดยสหภาพยุโรปหรือประเทศสมาชิก เช่นการถอนข้อมูลผู้ป่วยอาจมีผลต่อผลการวิจัยและคุณภาพ[73]

ตารางที่ 3.1 สิทธิตามกฎหมายของสหภาพยุโรปแก่ผู้ป่วยเกี่ยวกับข้อมูล

สิทธิ คือ	**หมายเลขมาตรา**	**ความหมายสำหรับผู้ป่วย**	**สิ่งที่ต้องระวัง (การจำกัดสิทธิ)**
การเข้าถึงข้อมูลส่วนบุคคลของตนเอง	ข้อบรรยาย 63 มาตรา 15	- สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของคุณเองเป็นส่วนหนึ่งของสิทธิขั้นพื้นฐานในการปกป้องข้อมูล - สิทธิในการเข้าถึงเวชระเบียนของคุณมีการระบุไว้อย่างชัดเจนในระเบียบใหม่ - หากคุณขอสำเนาข้อมูลส่วนบุคคลที่กำลังดำเนินการโดยผู้ควบคุมข้อมูลเกี่ยวกับ	- ผู้ควบคุมสามารถเรียกเก็บค่าธรรมเนียมสำหรับค่าใช้จ่ายในการจัดการในการจัดหาข้อมูลเมื่อคุณร้องขอมากกว่าหนึ่งครั้ง มาตรา 12 นอกจากนี้ยังอธิบายว่ามีค่าใช้จ่ายสามารถเรียกเก็บเงินเมื่อมีการร้องขอข้อมูลคือ “ไม่มีมูลความจริง” หรือซ้ำ - หากคุณให้ข้อมูลของคุณในบริบทของการวิจัยทาง

[73] The new regulation seeks to empower citizens with rights to be informed and puts them more in control of their personal data. These rights apply to patients in healthcare. They also apply in research, though in this case there may be some proportionate exemptions defined by the European Union or Member States, as for example withdrawing a patients' data could have consequences on the research results and quality.

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		คุณพวกเขาจะต้องให้ข้อมูลนั้นแก่คุณ - กฎข้อบังคับสนับสนุนให้มีการกำหนดวิธีการเข้าถึงจากระยะไกลเช่นบันทึกสุขภาพอิเล็กทรอนิกส์ - ผู้ควบคุมมีสิทธิตรวจสอบข้อมูลประจำตัวของคุณก่อนที่จะให้ข้อมูลแก่คุณ	วิทยาศาสตร์อาจมีการยกเว้นสิทธินี้
สิทธิในการเคลื่อนย้ายข้อมูล / เพื่อถ่ายโอนข้อมูลของคุณจากตัวควบคุมข้อมูลหนึ่งไปยังอีกตัวหนึ่ง	มาตรา 20	- เมื่อคุณยินยอมที่จะให้ข้อมูลสุขภาพของคุณและอยู่ในรูปแบบที่เครื่องอ่านได้ (เช่นในรูปแบบอิเล็กทรอนิกส์) คุณสามารถขอรับสำเนาเพื่อถ่ายโอนไปยังหน่วยงานหรือบุคคลอื่นได้และคุณยังสามารถเรียกร้องให้ จะถูกโอนโดยตรงสำหรับคุณ	- เมื่อการประมวลผลข้อมูลสุขภาพของคุณเกิดขึ้นในพื้นที่อื่นนอกเหนือจากความยินยอมอย่างชัดแจ้งของคุณสิทธินี้จะไม่มีผลบังคับใช้ซึ่งจะจำกัดไว้ในลักษณะสำคัญ - ไม่มีข้อผูกมัดที่ชัดเจนสำหรับผู้ควบคุมเพื่อให้แน่ใจว่าข้อมูลสามารถถ่ายโอนได้อย่างง่ายดาย

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		- อาจเป็นผลดีและกระตุ้นให้ผู้ควบคุม (โรงพยาบาล แพทย์) ตรวจสอบให้แน่ใจว่าข้อมูลอยู่ในรูปแบบที่สามารถถ่ายโอนได้ง่าย	
	มาตรา 21	- ภายใต้ข้อบังคับใหม่คุณสามารถคัดค้านการประมวลผลข้อมูลของคุณโดยผู้ควบคุมภายใต้สถานการณ์เหล่านี้ - หากการประมวลผลที่เกิดขึ้นสำหรับงานดำเนินการในความสนใจของประชาชน (มาตรา 6 วรรค 1 (e)) - หากการประมวลผลที่เกิดขึ้นเพื่อวัตถุประสงค์ที่ถูกต้องของการควบคุม (มาตรา 6 วรรค 1 (f)) - หากเกิดขึ้นในบริบทของการตลาดทางตรง	- ในการวิจัยคุณสามารถคัดค้านการดำเนินการได้เว้นแต่จะมีความจำเป็นสำหรับงานที่ดำเนินการด้วยเหตุผลเพื่อประโยชน์สาธารณะ (มาตรา 21 วรรค 6)

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
สิทธิในการแก้ไขหรือลบข้อมูล	มาตรา 16	- คุณสามารถขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง (เช่นในเวชระเบียนของคุณ) และกรอกข้อมูลที่ไม่สมบูรณ์ให้สมบูรณ์	
สิทธิในการลบ (เรียกว่า“ สิทธิที่จะถูกลืม”)	มาตรา 17	- คุณสามารถลบข้อมูลของคุณได้ สิ่งนี้เรียกว่า“ สิทธิที่จะถูกลืม” โดยเฉพาะอย่างยิ่งในกรณีนี้หาก - คุณได้เพิกถอนความยินยอมและผู้ควบคุมข้อมูลไม่มีเหตุผลอื่นใดในการประมวลผลข้อมูลของคุณ - หากไม่มีวัตถุประสงค์ในการประมวลผลอีกต่อไปตามหลักการของการจัดเก็บที่ จำกัด และการย่อขนาดข้อมูล - หากการประมวลผลไม่ชอบด้วยกฎหมายตั้งแต่แรก	- มีความเสื่อมเสียต่อสิทธิของคุณที่จะลบข้อมูลในการวิจัยและการดูแลสุขภาพ

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		- เมื่อผู้ควบคุมเปิดเผยข้อมูลต่อสาธารณะเช่น ทางออนไลน์เขาต้องดำเนินการตามขั้นตอนที่สมเหตุสมผลเพื่อให้แน่ใจว่าผู้ควบคุมรายอื่นจะลบการเชื่อมโยง ฯลฯ เพื่อที่จะใช้สิทธิของคุณ	
สิทธิในกรณีที่มีการละเมิด	มาตรา 34	- หากมีการละเมิดความปลอดภัยและข้อมูลส่วนบุคคลของคุณถูกเปิดเผยเข้าถึงหรือทำลายอย่างไม่เหมาะสมผู้ควบคุมข้อมูลควรแจ้งให้คุณทราบเกี่ยวกับการละเมิด หากเป็นการคุกคามสิทธิหรือเสรีภาพของคุณ เว้นแต่จะได้ใช้มาตรการอื่นเพื่อปกป้องข้อมูล (เช่น คีย์การเข้ารหัสข้อมูล) นอกจากนี้ควรแจ้งหน่วยงานกำกับดูแลในประเทศของตนถึงการละเมิด	- สิ่งสำคัญ คือ ต้องตรวจสอบให้แน่ใจว่าหน่วยงานกำกับดูแลได้รับแจ้งอย่างถูกต้องเกี่ยวกับการคุกคามสิทธิและเสรีภาพที่เกิดจากการเปิดเผยข้อมูลด้านสุขภาพหรือพันธุกรรมที่ไม่เหมาะสม
สิทธิในการร้องเรียนและการเยียวยาทางศาลที่มีประสิทธิผล	มาตรา 77, 79, 82	– แต่ละประเทศสมาชิกมีหน่วยงานกำกับดูแลสำหรับการปกป้องข้อมูล คุณมีสิทธิยื่นเรื่องร้องเรียนกับ	- สิทธิในการร้องเรียน และการเยียวยาทางศาลที่มีประสิทธิผล - สิทธิในการได้รับค่าชดเชย

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
และสิทธิในการได้รับค่าชดเชย		หน่วยงานเหล่านี้ในกรณีที่มีการละเมิดสิทธิในการปกป้องข้อมูลของคุณและหน่วยงานกำกับดูแลจะจัดเตรียมแบบฟอร์มเพื่ออำนวยความสะดวกในขั้นตอนการร้องเรียน หากการร้องเรียนเกี่ยวกับกรณีการแลกเปลี่ยนข้อมูลข้ามพรมแดนจะมีความร่วมมือระหว่างหน่วยงานกำกับดูแล http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. ดูรายชื่อหน่วยงานคุ้มครองข้อมูลได้ที่นี่: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm	

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		- นอกจากนี้คุณยังมีสิทธิที่จะ “การเยียวยาตามกระบวนการยุติธรรมอย่างมีประสิทธิผล” : คุณมีสิทธิที่จะให้สิทธิของคุณถูกบังคับโดยศาลยุติธรรมเมื่อสิทธิของคุณไม่ได้รับการเคารพ - หากมีการควบคุมข้อมูลละเมิดระเบียบนี้และทำให้คุณเกิดความเสียหายไม่ว่าจะเป็นวัสดุหรือไม่คุณมีสิทธิที่จะได้รับการชดเชยในกรณีนี้ คุณควรยื่นเรื่องร้องเรียนในด้านหน้าของศาล	
สิทธิในการรับทราบ / ความโปร่งใส	มาตรา 13 และ 14	- ผู้ควบคุมข้อมูลมีภาระผูกพันที่จะต้องให้ข้อมูลบางอย่างแก่คุณ พวกเขาต้องจัดเตรียมไว้ในรูปแบบที่กระชับโปร่งใสเข้าใจได้ง่ายและเข้าถึงได้ง่ายโดยใช้ภาษาที่ชัดเจนและชัดเจน หากพวกเขารวบรวมข้อมูลจากคุณโดยตรงพวกเขาจะต้องให้ข้อมูลต่อไปนี้แก่คุณในเวลาที่พวกเขา	- เพื่อให้ข้อมูลนี้แก่เจ้าของข้อมูล เมื่อคำขอข้อมูลของเจ้าของข้อมูล“ ไม่มีมูลความจริง” หรือซ้ำซากผู้ควบคุมสามารถเรียกเก็บเงินจากคุณเพื่อให้ข้อมูลนี้ (มาตรา 12)

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		รวบรวมข้อมูลสุขภาพของคุณ: - ข้อมูลประจำตัวของผู้ติดต่อหรือผู้ควบคุม - วัตถุประสงค์ในการประมวลผลข้อมูลของคุณ - ระยะเวลาที่ข้อมูลจะถูกจัดเก็บ - หากพวกเขาตั้งใจจะถ่ายโอนข้อมูลในประเทศอื่น - หากพวกเขาต้องการประมวลผลข้อมูลของคุณเพื่อวัตถุประสงค์อื่นที่ไม่ใช่ข้อมูลเดิม - สิทธิของคุณในฐานะเจ้าของข้อมูล - ในกรณีที่คุณไม่ได้ให้ข้อมูลโดยตรงผู้ควบคุมข้อมูลจำเป็นต้องให้ข้อมูลข้างต้นแก่คุณรวมทั้งข้อมูลเพื่อระบุแหล่งที่มาของข้อมูลและแหล่งข้อมูลนี้สามารถเข้าถึงได้โดยสาธารณะหรือไม่ หรือไม่มีการรวบรวมข้อมูลประเภท	

สิทธิ คือ	หมายเลขมาตรา	ความหมายสำหรับผู้ป่วย	สิ่งที่ต้องระวัง (การจำกัดสิทธิ)
		ใด (เช่น หากเป็นข้อมูลสุขภาพของคุณ)	

ที่มา: EPF European Patients Forum

3.3 สหพันธ์สาธารณรัฐเยอรมนี (Federal Republic Germany)

การคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี อยู่ภายใต้บทบัญญัติของรัฐธรรมนูญเยอรมัน (German Constitution) ซึ่งเป็นกรอบการคุ้มครองที่สำคัญสำหรับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองโดยตรงจากบทบัญญัติของรัฐธรรมนูญ ซึ่งห้ามมิให้มีการเข้าไปแทรกแซงในสิทธิส่วนบุคคล เช่น ในกรณีที่ข้อมูลนั้นเกี่ยวกับสิทธิขั้นพื้นฐานของบุคคลอื่นหรือของบุคคลที่สาม โดยในกฎหมายพื้นฐานฉบับนี้ (Basic Law or Grundgesetz)[74] ได้ให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ได้แก่ จดหมาย (Letter) หรือวัตถุทางไปรษณีย์ (Post) และการติดต่อสื่อสาร ทั้งนี้ การจำกัดความเป็นส่วนตัวดังกล่าวอาจทำได้ภายใต้บทบัญญัติของกฎหมายเท่านั้น[75]

กฎหมายคุ้มครองข้อมูลในสหพันธ์สาธารณรัฐเยอรมนีเกิดขึ้นครั้งแรกเป็นกฎหมายระดับรัฐ (State Law) โดยเกิดขึ้นในรัฐเฮสเซน (Hessen) ในปี ค.ศ. 1970 (พ.ศ. 2513) ถือว่าเป็นกฎหมายฉบับแรกของโลก ต่อมาในปี ค.ศ. 1977 (พ.ศ. 2520) ได้มีการตรากฎหมายในระดับประเทศ (Federal Data Protection Act) ซึ่งกฎหมายฉบับนี้ได้มีการทบทวนและแก้ไขในปี ค.ศ. 1990, 1994 และ 1997

[74] กฎหมายสูงสุดหรือรัฐธรรมนูญของประเทศเยอรมนีเรียกว่า กรุนด์เกเซ็ทท์ (Grundgesetz) หรือแปลตรงตัวได้ว่า "กฎหมายพื้นฐาน" ถูกบัญญัติขึ้นในปี 1949 ; https://th.wikipedia.org/wiki/

[75] Grundgesetz “Basic Law” (German Constitution) (May 23, 1949-Last amended August 31, 1990; English translation) Article 10 (Privacy of letters, posts, and telecommunications: amended 24 June 1968).

ตามลำดับ[76] ในปี ค.ศ. 2001 (พ.ศ. 2544) ได้มีการทบทวนกฎหมายนี้อีกครั้งเพื่อให้เป็นไปตามแนวทางของข้อบังคับสหภาพยุโรป[77] และการทบทวนแก้ไขอีกครั้งในปี ค.ศ. 2002 (พ.ศ. 2545)

ต่อมาสหพันธ์สาธารณรัฐเยอรมนี ได้มีการทบทวนแก้ไขครั้งสุดท้าย ในปี 2017 (พ.ศ. 2560) คือ Federal Data Protection Act 2018 (BDSG) (พ.ศ. 2561) หรือรัฐบัญญัติคุ้มครองข้อมูลของรัฐบาลกลาง ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยครอบคลุม การเก็บรวบรวม การประมวลผล และการใช้ ซึ่งใช้บังคับกับทั้งภาครัฐและเอกชน กล่าวคือ สหพันธ์สาธารณรัฐเยอรมนีมีการบังคับใช้ Federal Data Protection Act 2018 (พ.ศ. 2561) (BDSG) หรือรัฐบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (พ.ศ. 2561) เป็นปัจจุบัน เพื่อให้คุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

3.3.1 Federal Data Protection Act 2018 (BDSG) (รัฐบัญญัติคุ้มครองข้อมูลของรัฐบาลกลาง (BDSG))

Federal Data Protection Act 2018 (พ.ศ. 2561) (BDSG) หรือรัฐบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (พ.ศ. 2561) เป็นกฎหมายคุ้มครองข้อมูลของรัฐบาลกลางที่ร่วมกับกฎหมายคุ้มครองข้อมูลของรัฐสหพันธรัฐเยอรมันและระเบียบข้อบังคับเฉพาะพื้นที่อื่น ๆ จะควบคุมการเปิดเผยข้อมูลส่วนบุคคล ซึ่งได้รับการประมวลผลด้วยตนเองหรือจัดเก็บไว้ในระบบไอที มีวัตถุประสงค์ในบัญญัติขึ้นเพื่อปกป้องสิทธิของบุคคลในความเป็นส่วนตัวที่ถูกทำลายโดยการจัดการข้อมูลส่วนบุคคลของตน ซึ่งใช้บังคับกับการรวบรวม ประมวลผล และการใช้ข้อมูลส่วนบุคคลโดย 1. หน่วยงานสาธารณะของสหพันธ์ 2. หน่วยงานสาธารณะของแลนเดอร์ (Länder) ตราบเท่าที่การคุ้มครองข้อมูลส่วนบุคคลไม่อยู่ภายใต้กฎหมายที่ดิน (Land legislation)

ซึ่ง Federal Data Protection Act 2018 (พ.ศ. 2561) (BDSG) หรือรัฐบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (พ.ศ. 2561) มีมาตราน่าศึกษา ดังนี้

หมวด 5 การกำหนด

(1) หน่วยงานของรัฐต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล สิ่งนี้จะใช้กับหน่วยงานสาธารณะตามที่กำหนดไว้ในข้อ 2 (5) ซึ่งมีส่วนร่วมในการแข่งขัน

---

[76] Federal Data Protection Act (BDSG) January 27, 1997 (Bundesgestzblatt, Part I, No 7, February 1, 1997, Amended in 1990, http://www.datenchutz-berlin.de.gesestze/bdsg/bdsgeng.htm

[77] Federal Data Protection Act (BDSG) January 27, 1997 (Bundesgestzblatt, Part I, No 7, February 1, 1997, Amended in 1990, http://www.datenchutz-berlin.de.gesestze/bdsg/bdsgeng.htm

(2) เจ้าหน้าที่คุ้มครองข้อมูลเพียงคนเดียวอาจถูกกำหนดให้กับหน่วยงานสาธารณะหลายแห่ง โดยคำนึงถึงโครงสร้างและขนาดขององค์กร

(3) ให้กำหนดเจ้าหน้าที่คุ้มครองข้อมูลตามคุณสมบัติทางวิชาชีพ โดยเฉพาะอย่างยิ่ง ความรู้ความชำนาญด้านกฎหมายและแนวปฏิบัติด้านการคุ้มครองข้อมูล และความสามารถในการปฏิบัติงานตามมาตรา 7

(4) เจ้าหน้าที่คุ้มครองข้อมูลอาจเป็นพนักงานของหน่วยงานสาธารณะ หรือปฏิบัติงานตามสัญญาบริการ

(5) หน่วยงานสาธารณะต้องเผยแพร่รายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลและแจ้งไปยังกรรมาธิการแห่งสหพันธรัฐเพื่อการปกป้องข้อมูลและเสรีภาพของข้อมูล (Federal Commissioner for Data Protection and Freedom of Information)[78]

มาตรา 7 หน้าที่

(1) นอกเหนือจากงานที่ระบุไว้ในระเบียบข้อบังคับ (EU) 2016/679 เจ้าหน้าที่คุ้มครองข้อมูลต้องมีอย่างน้อยงานต่อไปนี้:

1. แจ้งและให้คำแนะนำแก่สาธารณชนและพนักงานที่ดำเนินการปฏิบัติตามรัฐบัญญัตินี้และกฎหมายคุ้มครองข้อมูลอื่น ๆ รวมถึงกฎหมายที่ประกาศใช้บังคับตามคำสั่ง (EU) 2016/680

2. ติดตามการปฏิบัติตามรัฐบัญญัตินี้และกฎหมายคุ้มครองข้อมูลอื่น ๆ รวมถึงกฎหมายที่ประกาศใช้คำสั่ง (EU) 2016/680 และนโยบายของหน่วยงานรัฐที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วน

---

[78] Federal Data Protection Act 2018 (BDSG), Section 5 Designation

(1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Section 2 (5) which take part in competition.

(2) A single data protection officer may be designated for several public bodies, taking account of their organizational structure and size.

(3) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Section 7.

(4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

(5) The public body shall publish the contact details of the data protection officer and communicate them to the Federal Commissioner for Data Protection and Freedom of Information.

บุคคล รวมถึงการกำหนดความรับผิดชอบ การสร้างการรับรู้และการฝึกอบรมของพนักงานซึ่งเกี่ยวข้องในการดำเนินการประมวลผล และการตรวจสอบที่เกี่ยวข้อง

3. ให้คำแนะนำเกี่ยวกับการประเมินผลกระทบต่อการคุ้มครองข้อมูลและติดตามการดำเนินการตามมาตรา 67 ของรัฐบัญญัตินี้

4. ให้ความร่วมมือกับหน่วยงานกำกับดูแล;

5. ทำหน้าที่เป็นจุดติดต่อหน่วยงานกำกับดูแลเกี่ยวกับประเด็นที่เกี่ยวข้องกับการประมวลผลรวมถึงการให้คำปรึกษาก่อนอ้างถึงในมาตรา 69 ของรัฐบัญญัตินี้และให้คำปรึกษาตามความเหมาะสมในเรื่องอื่น ๆ[79]

มาตรา 47 หลักการทั่วไปสำหรับการประมวลผลข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลจะต้อง

1. ดำเนินการอย่างถูกต้องตามกฎหมายและเป็นธรรม

2. เก็บรวบรวมไว้เพื่อจุดประสงค์ที่ถูกต้องตามกฎหมายและชัดเจนและไม่ประมวลผลในลักษณะที่ไม่เข้ากันกับวัตถุประสงค์เหล่านั้น

---

[79] Federal Data Protection Act (BDSG), Section 7 Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection officer shall have at least the following tasks:

1. to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680;

2. to monitor compliance with this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3. to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Section 67 of this Act;

4. to cooperate with the supervisory authority;

5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Section 69 of this Act, and to consult, where appropriate, with regard to any other matter.

3. เพียงพอที่เกี่ยวข้องและไม่มากเกินไปในความสัมพันธ์กับวัตถุประสงค์ที่พวกเขากำลังดำเนินการ

4. ถูกต้อง และกรณีจำเป็นให้มีการอัพเดตอยู่เสมอ; ทุกขั้นตอนที่เหมาะสมจะต้องดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องโดยคำนึงถึงวัตถุประสงค์ในการประมวลผลจะถูกลบหรือแก้ไขโดยไม่ล่าช้า;

5. เก็บไว้ในรูปแบบที่อนุญาตให้ระบุตัวของวิชาข้อมูลสำหรับไม่เกินเป็นสิ่งจำเป็นสำหรับวัตถุประสงค์ในการประมวลผล;

6. ดำเนินการในลักษณะที่ช่วยให้มั่นใจถึงความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม รวมถึงการป้องกันการประมวลผลโดยไม่ได้รับอนุญาตหรือผิดกฎหมายและต่อต้านการสูญเสียทำลายหรือความเสียหายโดยไม่ได้ตั้งใจโดยใช้มาตรการทางเทคนิคหรือองค์กรที่เหมาะสม[80]

มาตรา 67 การประเมินผลกระทบต่อการคุ้มครองข้อมูล

(1) ในกรณีที่ประเภทของการประมวลผลโดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีใหม่และคำนึงถึงธรรมชาติขอบเขตบริบทและวัตถุประสงค์ของการประมวลผลมีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงอย่างมากต่อผลประโยชน์ที่ได้รับการคุ้มครองตามกฎหมายของวิชาข้อมูลผู้ควบคุมจะต้องดำเนินการประเมินผลกระทบของการดำเนินการประมวลผลที่มองเห็นเกี่ยวกับเรื่องข้อมูล

---

[80] Federal Data Protection Act (BDSG), Section 47 General principles for processing personal data

Personal data shall be

1. processed lawfully and fairly;

2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

3. adequate, relevant and not excessive in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

(2) การประเมินร่วมกันอาจกล่าวถึงชุดของการดำเนินการประมวลผลที่คล้ายกันซึ่งมีความเสี่ยงที่ใกล้เคียงกัน

(3) ผู้ควบคุมจะต้องเกี่ยวข้องกับการกำกับดูแลของรัฐบาลกลางในการประเมินผลกระทบ

(4) การประเมินผลกระทบจะต้องรับสิทธิของบุคคลที่ได้รับผลกระทบจากการประมวลผลและต้องมีอย่างน้อยดังต่อไปนี้

1. คำอธิบายอย่างเป็นระบบของการดำเนินการประมวลผลที่มองเห็น และวัตถุประสงค์ของการประมวลผล;

2. การประเมินความจำเป็นและสัดส่วนของการดำเนินการเกี่ยวกับวัตถุประสงค์ของตน

3. การประเมินความเสี่ยงต่อผลประโยชน์ที่ได้รับความคุ้มครองตามกฎหมายของหัวข้อข้อมูล และมาตรการที่แสดงถึงความเสี่ยง รวมถึงมาตรการรักษาความปลอดภัย มาตรการรักษาความปลอดภัย และกลไกต่าง ๆ เพื่อให้มั่นใจในการปกป้องข้อมูลส่วนบุคคล และแสดงให้เห็นถึงการปฏิบัติตามกฎหมาย

(5) ในกรณีที่จำเป็นผู้ควบคุมจะต้องดำเนินการทบทวนเพื่อประเมินว่าการประมวลผลจะดำเนินการตามการประเมินผลกระทบต่อการคุ้มครองข้อมูลหรือไม่[81]

---

[81] Federal Data Protection Act (BDSG), Section 67 Conducting a data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a substantial risk to the legally protected interests of data subjects, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the data subjects.

(2) A joint assessment may address a set of similar processing operations that present similar substantial risks.

(3) The controller shall involve the Federal Commissioner in carrying out the impact assessment.

(4) The impact assessment shall take the rights of the data subjects affected by the processing into account and shall contain at least the following:

1. a systematic description of the envisaged processing operations and the purposes of the processing;

2. an assessment of the necessity and proportionality of the processing operations in relation to their purposes;

3. an assessment of the risks to the legally protected interests of the data subjects; and

มาตรา 83 ค่าตอบแทน

(1) หากผู้ควบคุมข้อมูลทำให้เจ้าของข้อมูลได้รับความเสียหายจากการประมวลผลข้อมูลส่วนบุคคลที่ละเมิดพระราชบัญญัตินี้หรือกฎหมายอื่นที่เกี่ยวข้องกับการประมวลผลนี้ ผู้ควบคุมหรือนิติบุคคลจะต้องจ่ายค่าชดเชยให้กับเจ้าของข้อมูล ภาระหน้าที่ในการจ่ายค่าชดเชยนี้จะไม่มีผลบังคับใช้หากในกรณีของการประมวลผลที่ไม่ใช่แบบอัตโนมัติ ความเสียหายไม่ได้เกิดจากความผิดพลาดโดยผู้ควบคุม

(2) เจ้าของข้อมูลอาจร้องขอการชดเชยทางการเงินที่เหมาะสมสำหรับความเสียหายที่ไม่ใช่สาระสำคัญ

(3) หากในกรณีของการประมวลผลข้อมูลส่วนบุคคลแบบอัตโนมัติ ไม่สามารถระบุได้ว่าผู้ควบคุมคนใดทำให้เกิดความเสียหาย ผู้ควบคุมแต่ละรายหรือนิติบุคคลจะต้องรับผิด

(4) มาตรา 254 แห่งประมวลกฎหมายแพ่ง ให้ใช้บังคับกับความประมาทเลินเล่อในส่วนของเจ้าของข้อมูล

(5) ให้นำบทบัญญัติการจำกัดที่กำหนดไว้สำหรับการกระทำที่ละเมิดในประมวลกฎหมายแพ่งมาใช้บังคับตามข้อจำกัดทางกฎหมาย[82]

---

4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law.

(5) Where necessary, the controller shall carry out a review to assess whether processing is performed in accordance with the data protection impact assessment.

[82] Federal Data Protection Act 2018 (BDSG), Section 83 Compensation

(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation.

3.4 เครือรัฐออสเตรเลีย (Commonwealth of Australia)

เครือรัฐออสเตรเลีย มีระบบทางด้านสุขภาพที่ดีแห่งหนึ่งของโลก โดยมีการพิจารณาข้อมูลด้านสุขภาพของประชากร การรักษา และมีการเปลี่ยนแปลงระบบจากเดิมที่บันทึกข้อมูลของผู้ป่วยไว้ในรูปแบบกระดาษหรือเอกสาร ต่อมาพัฒนาเป็นระบบที่ผู้ดูแลระบบข้อมูลซึ่งสามารถเข้าถึงและแบ่งปันข้อมูลทางด้านสุขภาพได้อย่างเป็นปัจจุบัน มีความน่าเชื่อถือ และมีความปลอดภัย ซึ่งสามารถดำเนินการได้ด้วยระบบ E-Health

องค์การอนามัยโลก ได้กำหนดให้ E-Health เป็น “การใช้เทคโนโลยีการสื่อสาร และเทคโนโลยีสารสนเทศในด้านสาธารณสุข” ในทางปฏิบัติมากขึ้น E-Health เป็นวิธีการสร้างความมั่นใจว่าข้อมูลด้านสุขภาพที่ถูกต้องนั้นได้มอบให้แก่บุคคลที่เหมาะสม ณ สถานที่และเวลาที่เหมาะสมในที่ปลอดภัย เพื่อวัตถุประสงค์ในการปรับคุณภาพและประสิทธิภาพของการให้บริการด้านสุขภาพให้เหมาะสมที่สุด E-Health ควรถูกมองว่าเป็นทั้งโครงสร้างพื้นฐานที่สำคัญที่สนับสนุนการแลกเปลี่ยนข้อมูลระหว่างผู้เข้าร่วมทุกคนในระบบการดูแลสุขภาพของออสเตรเลียและเป็นตัวขับเคลื่อนหลักและตัวขับเคลื่อนผลลัพธ์ด้านสุขภาพที่ดีขึ้นสำหรับชาวออสเตรเลียทุกคน[83]

3.4.1 E-Health

เมื่อวันที่ 1 กรกฎาคม ค.ศ. 2012 (พ.ศ. 2555) รัฐบาลเครือรัฐออสเตรเลียได้เปิดตัวระบบบันทึกสุขภาพอิเล็กทรอนิกส์ที่ควบคุมด้วยตัวเอง (PCEHR) (E-Health)[84] เมื่อระบบดำเนินการอย่างสมบูรณ์ระบบจะรวมข้อมูลสรุปทางอิเล็กทรอนิกส์ที่จัดทำโดยผู้ให้บริการด้านการดูแลสุขภาพซึ่งได้รับ

---

[83] The World Health Organisation defines E-Health as ‘the combined use of electronic communication and information technology in the health sector.’ In more practical terms, E-Health is the means of ensuring that the right health information is provided to the right person at the right place and time in a secure, electronic form for the purpose of optimising the quality and efficiency of health care delivery. E-Health should be viewed as both the essential infrastructure underpinning information exchange between all participants in the Australian health care system and as a key enabler and driver of improved health outcomes for all Australians. ; National E-Health Strategy SUMMARY December 2008. Australian Health Ministers' Conference, website www.ahmac.gov.au, p.1.

[84] “Australian Government - Department of Health and Ageing,” (http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-governance#.UZbkq5UWFFJ). PCEHR Governance. Retrieved 18 May 2013.

การเสนอชื่อพร้อมกับบันทึกย่อที่ผู้บริโภคมอบให้ นอกจากนี้ข้อมูลสรุปจะรวมข้อมูลเกี่ยวกับการแพ้ของแต่ละบุคคล อาการไม่พึงประสงค์ การฉีดวัคซีน การวินิจฉัยและการรักษา บันทึกของผู้บริโภคจะทำงานเป็นไดอารี่ทางการแพทย์ส่วนบุคคลซึ่งบุคคลเท่านั้นที่สามารถดูและแก้ไข[85] ระบบการเลือกไม่ให้คนอื่นเลือกว่าจะลงทะเบียนบันทึก E-Health หรือไม่[86]

เมื่อเดือนมกราคม ค.ศ. 2016 (พ.ศ. 2559) กรมสุขภาพเครือจักรภพแห่งการเปลี่ยนแปลง PCEHR ชื่อของบันทึกสุขภาพ

3.4.1.1 ความเป็นส่วนตัว

1. การจัดการ

Personally Controlled Electronic Health Records Act 2012 (พ.ศ. 2555) และ Principles under the Privacy Act 1988 (พ.ศ. 2541) บังคับวิธีการบันทึกข้อมูล E-Health มีการจัดการและการป้องกัน[87] ผู้ประกอบการระบบ PCEHR ปฏิบัติตามหลักการความเป็นส่วนตัวของข้อมูลในพระราชบัญญัติความเป็นส่วนตัวปี 1988 (พ.ศ. 2541) (Commonwealth) รวมถึงกฎหมายความเป็นส่วนตัวของรัฐหรือดินแดนใด ๆ[88] นโยบายความเป็นส่วนตัวกำหนดแอปพลิเคชันของการรวบรวมข้อมูลส่วนบุคคลโดยผู้ดำเนินการระบบ คำชี้แจงนี้รวมถึงคำอธิบายเกี่ยวกับประเภทของข้อมูลส่วนบุคคลที่รวบรวมข้อมูลที่ใช้สำหรับและวิธีการจัดเก็บข้อมูล คำแถลงครอบคลุมมาตรการในสถานที่เพื่อ

---

[85] "National E-Health Transition Authority (NEHTA)," (http://www.nehta.gov.au/our-work/pcehr). Our Work - PCEHR. Retrieved 18 May 2013.

[86] "Australian Government - Department of Health and Ageing," (http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-benefits#.UZcW8pUWHFJ). Expected benefits of the national PCEHR system. Retrieved 18 May 2013.

[87] "Australian Government – ComLaw," (http: / / www. comlaw. gov. au/ Details/ C201 2A00063) . Personally Controlled Electronic Health Records Act 2012. Retrieved 18 May 2013.

[88] "Australian Government - Office of the Australian Information Commissioner," (http://www.privacy.gov.au/material s/types/infosheets/view/6541). Information Privacy Principles under the Privacy Act 1988. Retrieved 18 May 2013.

ปกป้องข้อมูลส่วนบุคคลจากการใช้ในทางที่ผิดการสูญเสียการเข้าถึง โดยไม่ได้รับอนุญาตการดัดแปลงและการเปิดเผย[89]

2. มาตรการความปลอดภัย

มาตรการรักษาความปลอดภัยรวมถึงหลักฐานการตรวจสอบเพื่อให้ผู้ป่วยสามารถดูว่าใครได้เข้าถึงเวชระเบียนของพวกเขาพร้อมกับเวลาที่มีการเข้าถึงบันทึก มาตรการอื่น ๆ รวมถึงการใช้ และการเข้ารหัสเช่นเดียวกับการเข้าสู่ระบบและรหัสผ่านที่ปลอดภัย บันทึกของผู้ป่วยจะถูกระบุโดยใช้รหัสสุขภาพส่วนบุคคล (IHI) ที่ได้รับมอบหมายจาก เมดิแคร์ (Medicare)[90] ผู้ให้บริการ IHI[91],[92]

3. ปัญหา

การสำรวจทั่วประเทศปี พ.ศ. 2555 ในเครือรัฐออสเตรเลียประเมินความเป็นส่วนตัวเกี่ยวกับการตัดสินใจด้านการดูแลสุขภาพของผู้ป่วยซึ่งอาจส่งผลกระทบต่อการดูแลผู้ป่วย ผลการวิจัย

---

[89] “Australian Government - Department of Health and Ageing,” (http://www.ehealth.gov.au/internet/ehealth/publishin g.nsf/Content/ehealth_privacy). Privacy. Retrieved 18 May 2013.

[90] Medicare เป็นระบบการดูแลสุขภาพของออสเตรเลียที่ให้บริการโรงพยาบาลการแพทย์และทัศนมาตรแก่ชาวออสเตรเลียทุกคนโดยไม่เสียค่าใช้จ่ายหรือต้นทุนต่ำ ผลประโยชน์ที่คุณจะได้รับจะขึ้นอยู่กับค่าธรรมเนียมที่กำหนดโดยรัฐบาลออสเตรเลีย ในขณะที่เมดิแคร์ให้การเข้าถึงการรักษาฟรีในฐานะผู้ป่วยสาธารณะในโรงพยาบาลของรัฐ แต่คุณสามารถเลือกประกันสุขภาพเอกชนได้ฟรี; https://www.comparingexpert.com.au/health-insurance/medicare/

[91] “Australian Government - Department of Health and Ageing,” (http://www.ehealth.gov.au/internet/ehealth/publishin g.nsf/Content/ehealth_privacy). Privacy. Retrieved 18 May 2013.

[92] Showell, CM, “Citizens, patients and policy: a challenge for Australia's national electronic health record,” Health Information Management Journal. 40 (2): 39–43. doi:10.1177/183335831104000206 (https://doi. org/10.11 77%2F183335831104000206). PMID 28683627, (2011), (https://www.ncbi.nlm.nih.gov/pubmed/28683627). http://www.himaa.org.au/members/journal (http://www.himaa.org.au/members/journal/HIMJ_40_2_2011/HIMJ%2 040-2%20Showell%20Challenge%20for%20national%20e-health%20record.pdf)

ระบุว่า ร้อยละ 49.1 ของผู้ป่วยชาวออสเตรเลียระบุว่าพวกเขาได้ระงับหรือระงับข้อมูลจากผู้ให้บริการด้านการดูแลสุขภาพของพวกเขาตามความกังวลเรื่องความเป็นส่วนตัว[93]

3.4.1.2 ความยินยอมส่งผลกระทบต่อความเป็นส่วนตัว

ข้อกังวลประการหนึ่งคือการควบคุมส่วนบุคคลของบันทึก E-Health ผ่านการยินยอมไม่รับประกันการปกป้องความเป็นส่วนตัว เป็นที่ถกเถียงกันอยู่ว่าคำจำกัดความที่แคบ 'การอนุญาต' หรือ 'ข้อตกลง' ไม่ได้ให้ความคุ้มครองความเป็นส่วนตัวและไม่ได้เป็นตัวแทนในกฎหมายของเครือรัฐออสเตรเลีย ระบบบันทึกสุขภาพอิเล็กทรอนิกส์ที่ควบคุมด้วยตัวเอง (PCEHR) ช่วยให้แพทย์สามารถรับความยินยอมจากการมีส่วนร่วมของผู้บริโภคในระบบ อย่างไรก็ตามความต้องการของผู้บริโภคอาจไม่เป็นไปตาม นักวิจารณ์ยืนยันว่าคำจำกัดความที่กว้างขึ้นของ 'ความยินยอมที่ได้รับการบอกกล่าว' นั้นเป็นสิ่งที่จำเป็นเนื่องจากมันครอบคลุมการจัดหาข้อมูลที่เกี่ยวข้อง โดยผู้ประกอบการด้านการดูแลสุขภาพและการทำความเข้าใจข้อมูลนั้นโดยผู้ป่วย[94]

3.4.1.3 ความหมายที่เป็นไปได้ของการเปิดเผยข้อมูลผู้ป่วยที่ไม่พึงประสงค์

ข้อมูล 'การรั่วไหล' ถูกมองว่ามีศักยภาพที่จะกีดกันทั้งผู้ป่วยและแพทย์จากการเข้าร่วมในระบบ นักวิจารณ์ยืนยันว่าโครงการ PCEHR นั้นสามารถทำงานได้หากมีการดูแลอย่างต่อเนื่องที่ปลอดภัยและมีประสิทธิภาพภายในความสัมพันธ์ของผู้ป่วย / แพทย์ซึ่งไว้วางใจ หากผู้ป่วยขาดความไว้วางใจในการรักษาความลับของข้อมูล E-Health พวกเขาอาจระงับข้อมูลที่ละเอียดอ่อนจากผู้ให้บริการด้านการดูแลสุขภาพ แพทย์อาจลังเลที่จะเข้าร่วมในระบบที่พวกเขาไม่แน่ใจเกี่ยวกับความสมบูรณ์ของข้อมูล[95]

---

[93] Anonymous, “e-Health,” Australian Nursing Journal. 20 (2): 20(2012).

[94] Spriggs, Merle; Arnold, Michael V; Pearce, Christopher M; Fry, Craig (2012). “Ethical questions must be considered for electronic health records,” (http://vuir.vu.edu.au/10529/) (Submitted manuscript). Journal of Medical Ethics. 38 (9): 535–539. doi:10.1136/medethics-2011-100413 (https://doi.org/10.1136%2Fmedethics-2011-100413). PMID 22573881 (https://www.ncbi.nlm.nih.gov/pubmed/22573881).

[95] Liaw, S. T; Hannan, T, “Can we trust the PCEHR not to leak?,” (2011), (https://www.mja.com.au/public/issues/195 _04_150811/lia10586_letter_fm.html). The Medical Journal of Australia. 195 (4): 222. doi:10.5694/j.13265377.2011.tb03287.x (https://doi.org/10.5694%2Fj.1326-5377.2011.tb03287.x). PMID 21843131 (https://www.nc bi.nlm.nih.gov/pubmed/21843131).

3.4.1.4 การป้องกันที่เพียงพอสำหรับการปกป้องข้อมูลผู้ป่วย

ผู้เชี่ยวชาญด้านความปลอดภัยได้สอบถามขั้นตอนการลงทะเบียนซึ่งผู้ลงทะเบียนจะต้องให้หมายเลขบัตร Medicare และชื่อและวันเกิดของสมาชิกในครอบครัวเพื่อยืนยันตัวตน ผู้มีส่วนได้ส่วนเสียบางส่วนได้รับการหยิบยกขึ้นมาเกี่ยวกับความซับซ้อนโดยธรรมชาติของคุณสมบัติการเข้าถึงที่จำกัดเพื่อเตือนว่าการเข้าถึงเนื้อหาบันทึก PCEHR อาจเกี่ยวข้องกับการถ่ายโอนข้อมูลไปยังระบบท้องถิ่นซึ่งการควบคุมการเข้าถึง PCEHR จะไม่ใช้อีกต่อไป[96]

3.5 สหราชอาณาจักร (United Kingdom : UK)

บริการสุขภาพแห่งชาติจะเพิ่มขึ้นโดยใช้บันทึกสุขภาพอิเล็กทรอนิกส์แต่จนกระทั่งเมื่อเร็ว ๆ นี้ ระเบียนที่จัดขึ้นโดยองค์กรที่พลุกพล่านของแต่ละบุคคล เช่น ผู้ประกอบการทั่วไป Trusts พลุกพล่าน ทันตแพทย์และร้านขายยาไม่ได้เชื่อมโยง แต่ละองค์กรมีหน้าที่รับผิดชอบในการปกป้องข้อมูลผู้ป่วยที่รวบรวม Care Dataโปรแกรมซึ่งเสนอเพื่อดึงข้อมูล Anonymised จากการผ่าตัด GP เป็นฐานข้อมูลกลาง กระตุ้นความขัดแย้ง ในปี 2003 (พ.ศ. 2546) พลุกพล่านได้ดำเนินการเพื่อสร้างรีจิสทรีอิเล็กทรอนิกส์แบบรวมศูนย์ของเวชระเบียน ระบบมีการป้องกันโดยสหราชอาณาจักรของรัฐบาลเกตเวย์ซึ่งถูกสร้างขึ้น โดยไมโครซอฟท์ โปรแกรมนี้เรียกว่าการพัฒนาระเบียนอิเล็กทรอนิกส์และโปรแกรมการดำเนินการ (ERDIP) โปรแกรมแห่งชาติพลุกพล่านด้านไอทีถูกวิพากษ์วิจารณ์เพราะขาดความปลอดภัยและขาดความเป็นส่วนตัวของผู้ป่วย มันเป็นหนึ่งในโครงการที่ก่อให้เกิดคณะกรรมการข้อมูลเพื่อเตือน[97] เกี่ยวกับอันตรายของประเทศ "เดินละเมอ" ในที่สังคมเฝ้าระวัง กลุ่มแรงกดดันตรงข้ามกับบัตร

---

[96] Showell, CM, “Citizens, patients and policy: a challenge for Australia's national electronic health record,” Health Information Management Journal. 40 (2): 39–43. doi:10.1177/183335831104000206, (2011), (https://doi.org/10.11 77%2F183335831104000206). PMID 28683627 (https://www.ncbi.nlm.nih.gov/pubmed/28683627). http://www.himaa.org.au/members/journal (http://www.himaa.org.au/members/journal/HIMJ_40_2_2011/HIMJ%2 040-2%20Showell%20Challenge%20for%20national%20e-health%20record.pdf)

[97] Amoore, Louise & Ball, Kirstie & Graham, Stephen & Green, Nicola & Lyon, David & Murakami Wood, David & Norris, Clive & Pridmore, Jason & Raab, Charles & Rudinow Saetnan, Ann. (2006). A Report on the Surveillance Society. (https://www.researchgate.net/publication/241917099_A_Report_on_the_Surveillance_Society)

ประจำตัวประชาชน ยังรณรงค์ต่อต้านการลงทะเบียนส่วนกลางหนังสือพิมพ์นำเสนอเรื่องราวเกี่ยวกับคอมพิวเตอร์ที่สูญหายและหน่วยความจำ แต่ปัญหาที่พบบ่อยและยาวนานกว่านั้นก็คือพนักงานเข้าถึงระเบียนที่พวกเขาไม่มีสิทธิดู พนักงานสามารถดูบันทึกกระดาษได้เสมอและในกรณีส่วนใหญ่ไม่มีบันทึกการติดตาม ดังนั้นระเบียนอิเล็กทรอนิกส์ทำให้สามารถติดตามได้ว่าใครเข้าถึงข้อมูลใดบ้าง พลุกพล่านเวลส์ได้สร้างระบบตรวจสอบอัจฉริยะแห่งชาติแบบบูรณาการซึ่งให้ "ช่วงของรายงานที่สร้างขึ้นโดยอัตโนมัติออกแบบมาเพื่อตอบสนองความต้องการของคณะกรรมการสุขภาพในท้องถิ่นของเราและเชื่อถือได้ทันทีระบุปัญหาที่อาจเกิดขึ้นได้ การให้คำปรึกษาของ Maxwell Stanleyจะใช้ระบบที่เรียกว่า “Patient Data Protect” (ขับเคลื่อนโดย VigilancePro) ซึ่งสามารถตรวจจับรูปแบบ - เช่น มีคนกำลังเข้าถึงข้อมูลเกี่ยวกับญาติหรือเพื่อนร่วมงานของพวกเขา[98]

(1) รูปแบบการกำกับ

CRIS ย่อมาจาก the Clinical Record Interactive Search System หรือระบบค้นหาทางคลินิกบันทึกโต้ตอบ เป็น Software Solution ที่ลบข้อมูลจากเวชระเบียนอิเล็กทรอนิกส์ที่อาจระบุตัวบุคคลจากนั้นจะสร้างฐานข้อมูลที่ไม่ระบุตัวตนซึ่งองค์กร NHS สามารถใช้สำหรับการวิจัย[99]

ข้อมูลสำหรับการวิจัย

ข้อมูลที่ไม่ระบุชื่อหรือไม่ระบุตัวตนจากเวชระเบียนมีประโยชน์มากสำหรับการวิจัย ข้อมูลจำนวนมากถูกบันทึกไว้ในบันทึกเหล่านี้โดยเฉพาะอย่างยิ่งบันทึกข้อความฟรีและสามารถช่วยให้องค์กรเข้าใจได้ดีขึ้นว่ามีการส่งมอบการดูแลอย่างไรสาเหตุของโรคและประสิทธิผลของการแทรกแซงและการรักษาด้วยยา ข้อมูลที่ไม่ระบุตัวตนนี้สามารถช่วยตอบคำถามเหล่านี้ทั้งหมด[100]

---

[98] “Paperless NHS supplement: Data protection – it's a breach of trust,” (http://www.hsj.co.uk/resource-centre/supple ments/paperless-nhs-supplement-data-protection-its-a-breach-of-trust/5083120.article#.VT_-Zoq4_eM). Health Service Journal. 13 March 2015. Retrieved 28 April 2015.

[99] CRIS stands for the Clinical Record Interactive Search system. It is a software solution that removes information from an electronic medical record that might identify an individual. It then produces a de-identified database that an NHS organisation can use for research.

[100] Anonymous or de-identified data from medical records can be very useful for research. Significant amounts of information are recorded in these records, particularly the free text notes, and can help organisations better understand how care is being delivered, the causes of disease and the effectiveness of interventions and medications. This de-identified data can help answer all these questions.

สำหรับการประชุมแบบตัวต่อตัวจะต้องมีการวิจัยและ the Clinical Record Interactive Search System (CRIS) สามารถช่วยในกระบวนการนี้ได้เช่นกัน ตัวอย่าง เช่น NHS Trust ต้องการพูดคุยกับผู้ป่วยโรคจิตเภทที่เป็นเพศหญิงและมีอายุระหว่าง 25 - 45 ปี พวกเขาสามารถใช้ the Clinical Record Interactive Search System (CRIS) เพื่อค้นหาฐานข้อมูลที่ไม่ระบุตัวตนและค้นหาว่ามีกี่คนที่มีคุณสมบัติตรงตามเกณฑ์นี้ หากคนเหล่านี้ได้รับความยินยอมจากพวกเขาจะได้รับการติดต่อเกี่ยวกับโครงการวิจัยที่เกี่ยวข้องกระบวนการพิเศษสามารถดำเนินการเพื่อให้นักวิจัยได้ติดต่อกับบุคคลเหล่านี้ (และเหล่านี้เท่านั้น) หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการนี้และ / หรือเกี่ยวกับการติดต่อเกี่ยวกับงานวิจัยที่เกี่ยวข้องให้ติดต่อ NHS Trust ในพื้นที่ของคุณ หน้าแรกมีรายการ Trusts ทั้งหมดที่เกี่ยวข้องกับลิงค์ไปยังเว็บไซต์ของพวกเขาและที่ที่คุณสามารถหารายละเอียดของวิธีการติดต่อ[101]

(2) ข้อมูลที่ไม่ระบุตัวตน

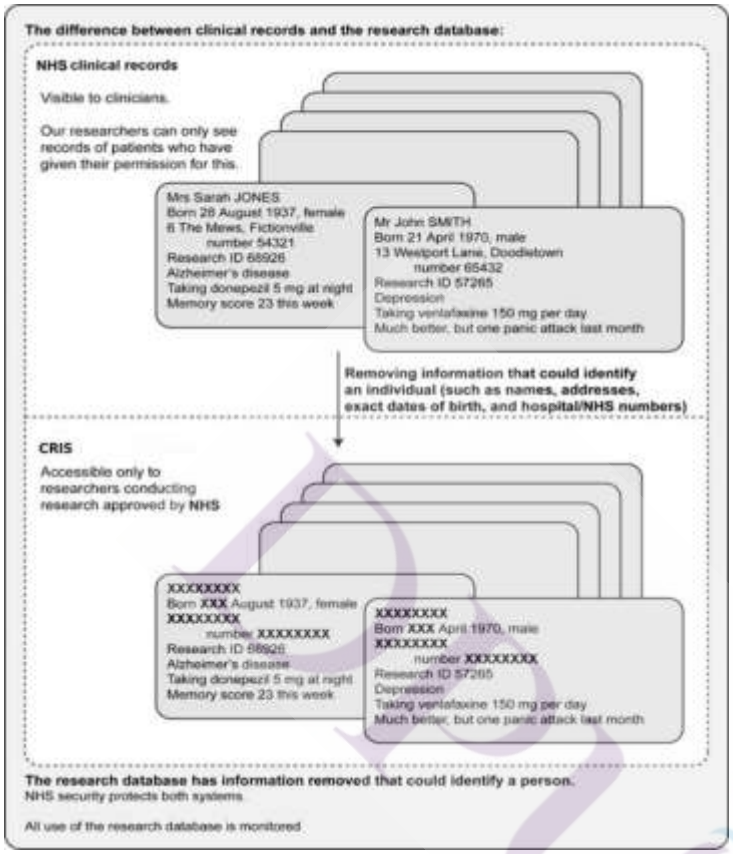
ข้อมูลที่มีการลบข้อมูลถูกปิดบังหรือแก้ไขเพื่อปกป้องความเป็นส่วนตัวของผู้ป่วย รายการ เช่น ชื่อนามสกุลหมายเลขโทรศัพท์ที่อยู่และหมายเลข NHS จะถูกลบออกหรือปิดบังเพื่อลดโอกาสที่ผู้ป่วยสามารถระบุได้จากข้อมูล[102]

---

[101] For some research face to face meetings are required and CRIS can help in this process too. If for example an NHS Trust wants to speak to patients with schizophrenia who are female and between the ages of 25-45 they can use CRIS to search the anonymous database and find out how many people they have who fit this criteria. If these people have given their consent to be contacted about relevant research projects, a special process can be carried out to allow the researchers to get in contact with these (and only these) individuals. To find out more about this process and/or about being contacted about relevant research work, get in touch with your local NHS Trust. The home page has a list of all the Trusts involved with links to their websites and where you can find details of how to get in touch.

[102] This is data which has had information removed, masked or modified to protect patient privacy. Items such as name, surname, telephone numbers, addresses and NHS numbers will all be removed or masked to minimise any chance a patient could be identified from the data.

ภาพที่ 3.1 แสดงความแตกต่างการเก็บข้อมูล



ที่มา: เว็บไซต์ https://crisnetwork.co/

(3) ผู้เข้าถึงข้อมูล

องค์กร National Health Service (NHS)[103] ที่ดำเนินการ The Clinical Record Interactive Search System (CRIS) จะมีกระบวนการที่เข้มงวดเพื่อควบคุมผู้ซึ่งสามารถเข้าถึงฐานข้อมูลได้ ผู้ใช้ทุกคนจะต้องลงทะเบียนเพื่อใช้ CRIS โดยแสดงหลักฐานที่เหมาะสมของสัญญาและการฝึกอบรมที่เสร็จ

[103] National Health Service (NHS) หรือระบบบริการสุขภาพแห่งชาติที่ทำให้มีหลักประกันสุขภาพถ้วนหน้า ในประเทศอังกฤษเกิดขึ้นในปี ค.ศ.1948 ในขณะที่โครงสร้างที่เป็นกระทรวงสาธารณสุข ซึ่งในปัจจุบันเรียกว่า Department of Health (DH) ม

สิ้นตามที่กำหนดโดยองค์กร NHS ของ host พวกเขาจะต้องได้รับคำร้องขออนุมัติโครงการเพื่อเข้าถึงข้อมูลใด ๆ[104]

(4) ผู้ติดตาม / ดูแล CRIS

ผู้ดูแลระบบ CRIS ในพื้นที่จะดูแลการทำงานของระบบในแต่ละวัน ระบบรวบรวมการดำเนินการทั้งหมดที่ดำเนินการกับ CRIS ผ่านบันทึกการตรวจสอบ สิ่งนี้ทำให้ผู้ดูแลระบบ CRIS และองค์กรสามารถทราบได้อย่างชัดเจนว่าผู้ใช้ CRIS ใช้ระบบอย่างไร นอกจากนี้คณะกรรมการตรวจสอบในพื้นที่ซึ่งประกอบด้วยผู้ป่วยและตัวแทนพนักงานจะตรวจสอบการใช้งานของ CRIS ตรวจสอบใบสมัครโครงการ (คุณไม่สามารถเข้าถึงข้อมูลใด ๆ โดยไม่ได้รับการอนุมัติโครงการ) และตรวจสอบให้แน่ใจว่านโยบายและการปฏิบัติต่าง ๆ นโยบาย[105]

Trust ทั้งหมดที่เป็นส่วนหนึ่งของเครือข่าย CRIS ก็เป็นส่วนหนึ่งของกลุ่มธรรมาภิบาลแห่งชาติ กลุ่มอยู่ในสถานที่เพื่อดูแลการทำงานอย่างปลอดภัยของ CRIS และกำหนดกระบวนการและขั้นตอนการทำงานของการค้นหาแบบรวม (ดูข้อมูลเพิ่มเติมเกี่ยวกับการรวมกลุ่มด้านล่าง) ข้อกำหนดเหล่านี้อยู่ในข้อตกลงการแบ่งปันข้อมูล UK-CRIS และสมาชิก NHS Trust แต่ละคนได้ลงนามในสำเนาของข้อตกลง กลุ่มจะจัดให้มีการทบทวนขั้นตอนการดำเนินงานมาตรฐานสำหรับ CRIS และการประเมินผลกระทบความเป็นส่วนตัว (การประเมินความเสี่ยงด้านความเป็นส่วนตัว) ของแพลตฟอร์มอย่างต่อเนื่องเพื่อให้แน่ใจว่าได้รับการปรับปรุงด้วยนโยบายการกำกับดูแลข้อมูลและมาตรฐานความปลอดภัย[106]

---

[104] Each NHS organisation running CRIS will have a strict process in place to control who can access the database. All end users will need to register to use CRIS, providing any appropriate evidence of contracts and training completed as defined by the host NHS organisation. They will also need to have a project application approved to gain access to any data.

[105] A local CRIS administrator will oversee the day to day running of the system. The system captures all actions carried out on CRIS via an audit log. This enables the CRIS administrator and the organisation to know exactly how CRIS users are using the system. Additionally, a local oversight committee made up of patient and staff representatives will monitor the use of CRIS, review project applications (you cannot access any data without an approved project) and ensure policies and practices are up to date with the latest legislative and organisational security policies.

[106] All the Trusts that are part of the CRIS network are also part of a national governance group. The group is in place to oversee the safe running of CRIS and determine the processes and procedures for how federated

ภาพที่ 3.2 แสดงการเก็บข้อมูล

ที่มา: เว็บไซต์ https://crisnetwork.co/

search works (find out more about federation below). These terms are captured in the UK-CRIS Data Sharing Agreement and each member NHS Trust have signed a copy of the agreement. The group will provide ongoing review of the standard operating procedures for CRIS and the privacy impact assessment (a privacy risk assessment) of the platform to ensure it is kept up to date with developing information governance policies and security standards. You can find out more about this group and the documents mentioned through the contact page on this website.

(5) เวชระเบียนผู้ป่วยเป็นฐานข้อมูล[107]

ระบบการจัดเก็บข้อมูลแบบเรียลไทม์ก่อนบันทึกเวชระเบียนที่ King's College Hospital ในไม่ช้าก็แสดงให้เห็นถึงความจำเป็นในการวางแผนข้อมูลผู้ป่วยในระดับสูง ระบบการจัดเก็บข้อมูลนั้นเพียงพอสำหรับการใช้งานแบบเรียลไทม์ แต่ในไม่ช้า Batch Systems ทุกประเภทเริ่มปรากฏขึ้นและแม้แต่แอปพลิเคชันแบบเรียลไทม์ก็ซื้อไฟล์เก็บถาวรของตนเอง การกระจายตัวของชุดข้อมูลที่เกี่ยวข้องนี้จะแนะนำวิธีแก้ไขปัญหาฐานข้อมูล ระเบียนผู้ป่วยที่ใช้คอมพิวเตอร์อาจเป็น “ธรรมชาติ” สำหรับเทคโนโลยีฐานข้อมูลเนื่องจากมีการจำลองข้อมูลจำนวนมากข้ามระบบข้อมูลในบริการด้านสุขภาพ เนื้อหาของจดหมายอ้างอิงพูดจากผู้ปฏิบัติการทั่วไปถึงคลินิกหรือในทางกลับกันควรได้รับการบันทึกไว้ที่ใดที่หนึ่งเป็นส่วนใหญ่ มีตัวอย่างมากมายทั้งในหน่วยงานด้านการดูแลสุขภาพ - โรงพยาบาลศูนย์สุขภาพ ฯลฯ[108]

เพื่อเป็นการแก้ปัญหาในการจัดเก็บข้อมูลทางการแพทย์ของผู้ป่วย จึงสร้างระบบข้อมูลขึ้นมา ดังนี้

1. ระบบข้อมูลทางการแพทย์แบบผู้ป่วยเป็นรายวันค่อย ๆ เปลี่ยนข้อมูลเวชระเบียนที่เป็นเอกสารจำนวนมากและเพื่อเพิ่มความเร็วในการไหลเวียนของข้อมูลทั่วทั้งบริการสุขภาพ[109]

---

[107] The patient medical record as a database ; B. E. Jones and M. A. Ould ; King's College Hospital Computer Centre, 97 Denmark Hill, London SE59RS

[108] An early real-time filing system for medical records at King's College Hospital soon demonstrated a need for planning patient-based information on a grand scale. The filing system was adequate for the early real-time applications but soon all kinds of patient-based batch systems began to appear, and even real-time applications acquired their own archive files. This fragmentation of related data sets suggests a database solution. Computerised patient records may be a 'natural' for database technology since there is so much replication of data across the information systems in the health care services. The content of a referral letter, say, from General Practitioner to Clinic, or vice versa, should largely be recorded somewhere already. There are numerous examples of this kind both within the units of health care—hospitals, health centres, etc.—and across them.

[109] 1. A day-to-day, patient-based medical information system gradually to replace much of the paper-based medical records, and to speed the flow of information throughout the health care services.

ระบบข้อมูลแบบวันต่อวัน[110]

พื้นที่นี้เป็นส่วนที่สำคัญที่สุดในการออกแบบเนื่องจากเป็นบริเวณที่มีการรวบรวมและแจกจ่ายฐานข้อมูลจำนวนมาก นี่คือคุณภาพของฐานข้อมูลที่จัดตั้งขึ้นและมีคุณค่า[111]

ระบบข้อมูลแบบวันต่อวันนั้นมีความเข้าใจเป็นอย่างดีในแง่ที่ว่าคอมพิวเตอร์มีผลกระทบแล้วโดยเฉพาะในห้องปฏิบัติการของโรงพยาบาล ที่นี่เรามีความกังวลเกี่ยวกับรูปแบบที่ใหญ่ขึ้นและน้อยลงด้วยระบบรายละเอียดในวอร์ด คลินิก การผ่าตัด ฯลฯ[112]

2. ระบบจัดเก็บข้อมูลระยะยาวที่สนับสนุนเวชระเบียนผู้ป่วยตลอดชีวิตและเชื่อมต่อกับการรักษาพยาบาลทุกรูปแบบ[113]

ระบบข้อมูลระยะยาว[114]

จุดประสงค์คือการสร้างเวชระเบียนคอมพิวเตอร์สำหรับผู้ป่วยแต่ละรายเผิน ๆ นี่เป็นกลยุทธ์ที่ชัดเจนซึ่งเป็นไปได้มากขึ้นกับการกำเนิดของคอมพิวเตอร์ มันควรจะเป็นไปได้ที่จะได้รับอาหารเสริมที่มีคุณค่าในประวัติศาสตร์ของผู้ป่วยแบบดั้งเดิมประหยัดเวลาของแพทย์หรือปรับปรุงการดูแลผู้ป่วยหรือทั้ง 2 อย่าง บันทึกระยะยาวควรเพิ่มมิติอื่นให้กับความเป็นไปได้ของการวิเคราะห์ทางคลินิกของฐานข้อมูล ในทางปฏิบัติมีปัญหาหลายอย่างและประเภทของผลประโยชน์ที่คาดว่าจะต้องใช้เวลาหลายปีกว่าจะรู้[115]

---

[110] The day-to-day information system

[111] This is by far the most important area of design because it is where the bulk of the database is gathered and distributed. Here the quality of the database is established and so is its value.

[112] The day-to-day information system is already well understood in the sense that computers have already made some impact, particularly in hospital laboratories. Here we are concerned with a larger pattern and less with the detailed systems in wards, clinics, surgeries, etc.

[113] 2. A longer-term information storage system supporting the patient medical record for life and interfacing with all forms of medical care.

[114] The long-term information system

[115] The intention is to build up a computer-based medical recordfor - life for each patient. Superficially this is an obvious strategy which becomes more feasible with the advent of computers. It should be possible to derive valuable supplements to the traditional patient history, saving doctors' time or improving patient care or both. The long term record should also add another dimension to the possibilities of clinical analysis of the database. In practice, there are various problems and the kind of benefits expected must take many years to be realised

วัตถุประสงค์ในด้านนี้คือการพัฒนาโครงสร้างข้อมูลผู้ป่วยเพิ่มเติมในฐานข้อมูลที่เรียกว่าส่วนหน้าซึ่งจะให้ข้อมูลที่จำเป็นสำหรับเวชระเบียนทุกชีวิต แต่ไม่ใช่รายละเอียด แน่นอนเรายังไม่ได้สร้างมากกว่าความคิดที่คลุมเครือของข้อมูลที่สำคัญคืออะไร แต่เราคาดว่าจะสร้างบางส่วนผ่านระบบข้อมูลวันนี้ ดังนั้นในขณะนี้โครงสร้างและเนื้อหาของฐานข้อมูลระยะยาวส่วนใหญ่จะได้มาจากระบบแบบวันต่อวัน แม้ว่าส่วนหลังจะเป็นส่วนย่อยของอดีต[116]

การเก็บรักษาข้อมูลเป็นเวลานาน อาจเป็น 70 ปี แนะนำอีกสองปัญหาของการรักษาความเกี่ยวข้องและความเข้ากันได้ซึ่งอยู่นอกเหนือขอบเขตของบทความนี้[117]

3. ฐานข้อมูลที่เหมาะสมสำหรับการวิเคราะห์ทางคลินิกและการบริหารประเภทต่าง ๆ[118]

ระบบข้อมูลสถิติ[119]

ความท้าทายของการวิเคราะห์ทางคลินิกและการบริหารต้องพิจารณาอย่างรอบคอบ ปัญหาคือว่าระบบข้อมูลที่สนับสนุนแทนที่จะสั่งการบันทึกทางการแพทย์ไม่สามารถแม่นยำหรือสมบูรณ์ได้ เทคนิคคอมพิวเตอร์อาจเปรียบเทียบได้ดีกับระบบกระดาษในแง่นี้ แต่ก็ไม่ได้พูดอะไรมาก[120]

หากระบบข้อมูลแบบวันต่อวันทำงานได้ดีกับผู้ใช้จะมีการไหลของข้อมูลแบบสองทางระหว่างฐานข้อมูลและผู้ใช้และมีเหตุผลที่จะสมมติว่าคุณภาพของข้อมูลที่บันทึกไว้จะดีขึ้นอย่างมาก หากระบบคอมพิวเตอร์รวบรวมข้อมูลที่ไม่มีการป้อนกลับจริงให้กับผู้ใช้ฐานข้อมูลนั้นไม่สามารถถือว่า

---

[116] Our objective in this area must be to develop an additional patient data structure, within the database, called the front end, which is to provide the essential data required of each life-long medical record but not the detail. Of course, we have yet to establish more than a vague notion of what the essential data is but we do expect to generate some of it via the day-today information system. Thus, for the time being, the structure and content of the long-term information base will be mainly derived from the day-to-day system—although the latter is logically a subset of the former.

[117] Preservation of data for long periods—perhaps 70 years— introduces two further problems of maintaining relevance and compatibility, which are beyond the scope of this paper.

[118] 3. An information base suitable for various types of clinical and administrative analysis.

[119] The statistical information system

[120] The challenge of clinical and administrative analysis requires careful consideration. The problem is that an information system that supports rather than dictates to the medical record cannot ever be either wholly accurate or complete. Computer techniques may compare favourably with paper systems in this respect, but that is not saying much.

ดีสำหรับการวิเคราะห์ได้ ไม่ว่าคุณภาพของข้อมูลจะเป็นอย่างไรเทคนิคทางสถิติที่ใช้ในฐานข้อมูลควรคล้ายกับการสำรวจสำมะโนประชากรมากกว่าการนับโดยตรงของการรับเข้าเรียนเป็นต้นจากนั้นจนถึงจุดนี้ปริมาณของฐานข้อมูลที่แท้จริงสามารถคาดหวังได้ว่าจะขจัดปัญหาคุณภาพข้อมูล[121]

การวิเคราะห์ฐานข้อมูลทำให้เกิดปัญหาเฉพาะของความเข้ากันได้ของข้อมูลและควรเขียนรหัสตามที่ถกเถียงกันในบางครั้ง แต่เราไม่สนใจประเด็นเหล่านี้[122]

ความเป็นส่วนตัว

คณะกรรมการที่อายุน้อยกว่าในอังกฤษและกระทรวงสาธารณสุขการศึกษาและสวัสดิการในสหรัฐอเมริกาเพิ่งรายงานผลการตรวจสอบของพวกเขาเกี่ยวกับความเป็นส่วนตัวของฐานข้อมูลและพลเมือง[123]

มันเป็นความคิดเห็นที่บอกเล่าเกี่ยวกับความกำกวมของเรื่องที่คณะกรรมการที่อายุน้อยกว่ารู้สึกว่าไม่จำเป็นต้องมีความเร่งด่วนในแง่ของการควบคุมอย่างละเอียดและได้นำเสนอเอกสารคำแนะนำที่เต็มไปด้วย 'Shoulds' ในขณะที่ชาวอเมริกัน ด้วยความจำเป็น ในการวิเคราะห์ขั้นสุดท้ายข้อมูลจะเป็นข้อมูลส่วนตัวเช่นเดียวกับที่ผู้ใช้เตรียมที่จะทำ[124]

---

[121] If the day-to-day information system integrates well with users, there will be two-way information flow between the database and users and it is reasonable to suppose that the quality of information recorded will improve dramatically. If the computer system collects data with no real feed-back to users, then the database cannot be regarded as good for analysis. Whatever the quality of data the statistical techniques used on the database should be more akin to census studies than direct counts of admissions, etc. Then, up to a point, the sheer volume of the database can be expected to eliminate problems of data quality.

[122] Analysis of the database does raise specific problems of the compatibility of data and whether data should be coded as is sometimes argued, but we ignore these issues here.

[123] The Younger Committee in England and the Department of Health, Education and Welfare in the United States have both recently reported the findings of their respective investigations into the subject of database privacy and the citizen.

[124] It is a telling comment on the ambiguity of the subject that the Younger Committee feels there is no need for urgency in respect of detailed controls and have presented an advisory document full of 'shoulds' whilst the Americans come to the opposite conclusion and arm their proposals with imperatives. In the final analysis, data will only be as private as its users are prepared to make it.

หลักการของคณะกรรมการที่อายุน้อยจำนวนมากมีความสำคัญสำหรับแพทย์ผู้เชี่ยวชาญด้วยความเคารพต่อประวัติผู้ป่วยมากกว่าข้อกำหนดสำหรับการออกแบบฐานข้อมูล โดยเฉพาะอย่างยิ่งเนื้อหาของฐานข้อมูลวิธีการใช้งานระยะเวลาที่จัดเก็บ ฯลฯ ไม่ได้กำหนดไว้อย่างง่ายดายตามที่มีการแนะนำ ในทางกลับกันการออกแบบฐานข้อมูลสามารถมั่นใจได้ว่ามีค่าใช้จ่ายการควบคุมการเข้าถึงที่เหมาะสมและกลไกอื่น ๆ ในการสนับสนุน[125]

ข้อกำหนดทางกฎหมาย[126]

บริเวณนี้ไม่ได้กำหนดไว้อย่างชัดเจนเช่นกัน ตัวอย่างเช่นข้อมูลผู้ป่วยในและข้อมูลผู้ป่วยนอกของโรงพยาบาลต้องเก็บไว้เป็นเวลาหกปีหลังจากที่ผู้ป่วยเข้ารับการรักษาครั้งสุดท้ายที่โรงพยาบาลเวชระเบียนสำหรับชีวิตดูเหมือนจะตอบสนองความต้องการประเภทนี้เกือบจะตามคำจำกัดความ

อย่างไรก็ตามปัญหาทางกฎหมายเป็นหลักหนึ่งในการแสดงหลักฐานในกรณีของการดำเนินคดี จากนั้นฐานข้อมูลจะต้องให้ข้อมูลกับสถานะทางกฎหมายของ 'บันทึกที่ได้รับในเวลา' สิ่งนี้แสดงถึงการสร้างบันทึกของผู้ป่วยไปยังสถานะที่เกิดขึ้นในช่วงเวลาหนึ่งโดยเฉพาะและการระบุแหล่งที่มาของเนื้อหาทั้งหมด

ในแง่ปฏิบัติแล้วฐานข้อมูลจะต้องบันทึกว่าใครเป็นผู้เพิ่มและเปลี่ยนแปลงข้อมูลผู้ป่วยและเมื่อใด การเปลี่ยนแปลงความคิดเห็นและอื่น ๆ จะต้องได้รับผลกระทบโดยไม่สูญเสียข้อมูลที่มีการแก้ไขเพื่อให้สามารถสร้างสถานะก่อนหน้าได้[127]

---

[125] Many of the Younger Committee principles are matters for the Medical Profession with respect to patient records, rather than requirements for database design. In particular, database content, how it is used, how long it is kept, etc. are not easily defined as Younger would recommend. On the other hand, the database design can ensure, at some cost, proper access controls and other mechanisms in support of Younger.

[126] Legal requirements

[127] This area is not well defined, either. For example, hospital inpatient and outpatient information must be held for six years after the last attendance at the hospital by the patient. A medical record-for-life appears to meet this kind of requirement almost by definition.

However, the legal problem is essentially one of providing evidence in cases of litigation. Then the database must provide information with the legal status of 'notes taken at the time'. This implies the reconstruction of a patient's record to the state it was in at a particular moment, and identification of the source of all the content.

ข้อจำกัดทางเทคนิค

ในทางปฏิบัติเราต้องวางแผนสำหรับระบบข้อมูลจริงในการกำหนดค่าอย่างง่ายโดยใช้เทคโนโลยีปัจจุบัน[128]

1. จดหมายเหตุ

ในปัจจุบันเป็นไปไม่ได้ที่จะเก็บข้อมูลทั้งหมดไว้ในไฟล์การเข้าถึงโดยตรงแบบออนไลน์ด้วยเหตุผลเรื่องจำนวนมากค่าใช้จ่าย ฯลฯ แม้ว่าการจัดเก็บข้อมูลแบบเข้าถึงโดยตรงจะมีราคาถูกลงและมีขนาดกะทัดรัดมากขึ้นในอนาคตอย่างไม่ต้องสงสัย แต่ก็แทบจะเป็นความจริงอย่างแน่นอนว่าส่วนต่างราคาที่มากจะยังคงมีอยู่ระหว่างเทคนิคดังกล่าวกับการจัดเก็บข้อมูลแบบอนุกรมจำนวนมากเช่นเทปแม่เหล็ก ด้วยเหตุนี้การจัดเก็บข้อมูลประวัติผู้ป่วยที่มีกิจกรรมน้อยจึงเป็นวิธีการจัดเก็บที่ประหยัดกว่าการพยายามเก็บข้อมูลทั้งหมดแบบออนไลน์[129]

ซอฟต์แวร์ฐานข้อมูลจึงต้องมีสิ่งอำนวยความสะดวกสำหรับการย้ายเวชระเบียนของผู้ป่วยจากฐานข้อมูลปัจจุบันไปยังฐานข้อมูลที่เก็บถาวรและในทางกลับกันตามที่กำหนด[130]

2. การเข้าถึง

การเข้าถึงฐานข้อมูลต้องใช้เวลาและทรัพยากรที่ จำกัด และต้องเข้ากันได้กับความต้องการของแอปพลิเคชัน ผู้ใช้ฐานข้อมูลออนไลน์เป็นปัญหาหลักเนื่องจากพวกเขาแย่งชิงทรัพยากร เข้าถึงโดยเฉพาะอย่างยิ่งไปยังฐานข้อมูลจะต้องเกิดขึ้นอย่างรวดเร็วมากพอที่จะตอบสนองการใช้งานใน

In practical terms, then, the database must record who makes additions and changes to the patient data and when. Changes, comments, etc. must be effected without loss of the amended data so that the earlier state can be reconstructed.

[128] Technical constraints in practice, we must plan for a real information system on a simple configuration using current technology.

[129] 1. Archives

It is not possible at present to hold all the data in on-line direct access files for reasons of bulk, expense, etc. Although direct access storage will undoubtedly become cheaper and more compact in future it is almost certainly true that a considerable price differential will still exist between such techniques and mass serial storage such as magnetic tape. In view of this, the archival of low activity patient records is and will remain a more economical approach to storage than attempting to hold all data on-line.

[130] The database software must therefore include facilities for moving patient medical records from the current database to the archive database and vice versa as required.

บรรทัดที่เกี่ยวข้องกับมัน นอกจากนี้ยังต้องไม่ผูกติดกับทรัพยากรคอมพิวเตอร์มากเกินไปมิฉะนั้นจะรบกวนผู้ใช้คอมพิวเตอร์รายอื่น แน่นอนว่าประเภทของการเข้าถึงที่พบบ่อยมากขึ้น ปัจจัยเหล่านี้ก็จะยิ่งมีความสำคัญมากขึ้นเท่านั้น[131]

ซึ่งจะส่งผลกระทบต่อโครงสร้างของฐานข้อมูลบนบรรทัดโหมดทั่วไปของการเข้าถึงฐานข้อมูลออนไลน์ต้องทำงานได้อย่างมีประสิทธิภาพและโครงสร้างสามารถสร้างความแตกต่างได้ทั้งหมด เฉพาะในสถานการณ์ฮาร์ดแวร์ในอุดมคติเท่านั้นที่เป็นปัญหาในการทำแผนที่[132]

3. การกู้คืนฐานข้อมูลออนไลน์

การรักษาความปลอดภัยของฐานข้อมูลที่เก็บถาวรสามารถจัดหาได้ด้วยเทคนิคของปู่ พ่อ - ลูก แต่กลยุทธ์การสำรองข้อมูลสำหรับฐานข้อมูลออนไลน์นั้นเกี่ยวข้องกับข้อควรพิจารณาในการออกแบบอื่น ๆ อย่างแยกไม่ออก[133]

ตามข้อกำหนดด้านความปลอดภัยจะต้องยื่นสำเนาการปรับปรุงฐานข้อมูลอย่างน้อยสองชุดนอกเหนือจากการปรับปรุงเอง สิ่งนี้ให้การสำรองข้อมูลสองระดับ แต่ทำให้เกิดภาระเพิ่มเติมเกี่ยวกับเวลาและทรัพยากรที่เกี่ยวข้องกับการเข้าถึงฐานข้อมูล สิ่งนี้มีผลต่อการพิจารณาโครงสร้างภายใน[134]

---

[131] 2. Accessibility

Access to the database takes finite time and resources, and this must be compatible with the needs of the applications. On-line users of the database are the main problem since they compete for the resources. A particular access to the database must take place quickly enough to satisfy the on-line user who instigated it; it must also not tie up too much of the computer resources else it will interfere with other users of the computer. Of course, the more common the type of access the more critical each of these factors becomes.

[132] This will affect the structure of the on-line database. Common modes of on-line access to the database must operate efficiently and the structure can make all the difference. Only in an idealized hardware situation is this just a mapping problem.

[133] 3. Recovery of the on-line database

Security of the archive database can be provided by grandfather father- son techniques but the back-up strategy for the on-line database is inextricably related to other design considerations.

[134] According to the requirements of security, at least two copies of each update to the database must be filed, in addition to the update itself. This provides the two levels of back-up but places an additional burden on the time and resources involved in database access. This influences considerations of internal structure.

จากมุมมองอื่นต้องคำนึงถึงความเร็วของกระบวนการกู้คืนด้วย ดังนั้นหากฐานข้อมูลได้รับการบำรุงรักษาให้ซ้ำกันทั้งหมด การดำเนินการสำรองข้อมูลระดับแรกจึงเป็นเรื่องเล็กน้อย แต่การทำซ้ำอาจทำให้ทรัพยากรที่มากเกินไปสำหรับการเข้าถึงปกติ[135]

4. การควบคุมการเข้าถึงข้อมูลออนไลน์

จำเป็นต้องมีระบบการจัดการการเข้าถึงเพื่อหลีกเลี่ยงการเข้าถึงฐานข้อมูลที่ทับซ้อนกันบางประเภทโดยผู้ใช้อิสระ ระบบ 'Lockout' ที่นำมาใช้นั้นเกี่ยวข้องกับการพิจารณาทั้งการเข้าถึงและการกู้คืน ตามหลักการแล้วโครงสร้างฐานข้อมูลควรหลีกเลี่ยงการขึ้นต่อกันเชิงตรรกะในคำสั่งข้อมูลจริง แม้ว่าจะเป็นไปไม่ได้ที่จะบรรลุในทางปฏิบัติก็ตาม อย่างไรก็ตามยิ่งความสัมพันธ์เชิงตรรกะยืดข้ามฐานข้อมูลน้อยเท่าไหร่ก็ยิ่งดีเท่านั้น ในกรณีที่เลวร้ายที่สุดฐานข้อมูลทั้งหมดจะต้องถูก 'ล็อก' จากผู้ใช้รายอื่นในขณะที่มีการเข้าถึงออนไลน์แต่ละครั้ง สิ่งนี้น่าจะส่งผลร้ายแรงต่อระบบการสนทนาอย่างมาก ตามหลักการแล้วเราต้องการทำงานให้ต่ำที่สุดเท่าที่ระดับกลุ่ม[136]

---

[135] From another point of view, the speed of the recovery process must be taken into account. Thus if the database is maintained entirely in duplicate, the operation of first level back-up is trivial but the duplication itself may tie up excessive resources for normal access.

[136] 4. Control of access to on-line data

A system of access management is required to avoid certain types of overlapped access to the database by independent users. The 'lockout' system adopted is also related to both access and recovery considerations. Ideally the database structure should avoid logical dependencies across the actual data statements, although this is quite impossible to achieve in practice. However, the less the logical relationships stretch across the database the better. In the worst extreme, the entire database has to be 'locked' out from other users while each online access is performed. This would presumably have a serious effect on a highly conversational system. Lock-outs at patient level might also be impracticable on such a system. Ideally, we would like to work as low as segment level.

ซอฟต์แวร์[137]

ฐานข้อมูลที่กล่าวถึงต้องใช้ซอฟต์แวร์เป็นจำนวนมากสนับสนุนในพื้นที่ต่อไปนี้:

(a) การดูแลทำความสะอาด (การเชื่อมต่อไฟล์เก็บถาวรการจัดระเบียบไฟล์ ฯลฯ)

(b) การบำรุงรักษาที่เก็บถาวร (การเชื่อมต่อฐานข้อมูลปัจจุบันการวิเคราะห์ทางสถิติ)

(c) การเข้าถึงแบบกลุ่ม (รับเข้าและส่งออก[138])

(d) การกู้คืนฐานข้อมูลออนไลน์

(e) การจัดการข้อมูล

การอภิปรายเพิ่มเติมเกี่ยวกับสิ่งเหล่านี้อยู่นอกขอบเขตของบทความนี้

Data Protection Act 1998 (พ.ศ. 2541) (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998)

[139]สหราชอาณาจักรได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ The Data Protection Act of 1998 (พ.ศ. 2541) เป็นรุ่นที่ 3 เริ่มใช้วันที่ 25 พฤษภาคม 2018 (พ.ศ. 2561) ขึ้น

---

[137] Software

The database discussed requires a great deal of software to support it in the following areas:

(a) housekeeping (archive interfacing, file reorganisation, etc.)

(b) archive maintenance (current database interfacing, statistical analysis)

(c) batch access (input and output)

(d) on-line database recovery

(e) data manipulation.

Further discussion of these is outside the scope of this paper.

[138] ในทางคอมพิวเตอร์ หมายถึงการสื่อสารระหว่างระบบประมวลผลสารสนเทศ (เช่นคอมพิวเตอร์) กับโลกภายนอก ซึ่งอาจเป็นมนุษย์หรือระบบประมวลผลสารสนเทศอีกระบบหนึ่ง อินพุตหรือสิ่งรับเข้าคือสัญญาณหรือข้อมูลที่ระบบรับเข้ามา และเอาต์พุตหรือสิ่งส่งออกคือสัญญาณหรือข้อมูลที่ระบบส่งออกไป ศัพท์นี้ใช้เรียกการกระทำเพียงส่วนหนึ่ง กล่าวคือ “การกระทำไอ/โอ” หมายถึงการปฏิบัติการรับเข้าหรือส่งออกสัญญาณหรือข้อมูล บุคคลหนึ่ง (หรือระบบอื่น) สามารถใช้อุปกรณ์ไอ/โอเพื่อสื่อสารกับคอมพิวเตอร์ ตัวอย่างเช่น คีย์บอร์ดหรือเมาส์จัดว่าเป็นอุปกรณ์รับเข้าสำหรับคอมพิวเตอร์ ในขณะที่จอภาพและเครื่องพิมพ์จัดว่าเป็นอุปกรณ์ส่งออกสำหรับคอมพิวเตอร์ ส่วนอุปกรณ์ที่สื่อสารระหว่างคอมพิวเตอร์ด้วยกัน เช่นโมเด็มหรือแผ่นวงจรเครือข่าย โดยปกติสามารถเป็นได้ทั้งอุปกรณ์รับเข้าและส่งออก ; https://th.wikipedia.org/wiki/

[139] Data Protection Act 2018, https://ico.org.uk/for-organisations/data-protection-act-2018/

เป็นกฎหมายกลาง (Comprehensive) พระราชบัญญัติคุ้มครองข้อมูลปี ค.ศ. 2018 (พ.ศ. 2561) ในทุกประเทศสมาชิกเพื่อให้สอดคล้องกับกฎหมายความเป็นส่วนตัวของข้อมูลทั่วยุโรป และมีวัตถุประสงค์เพื่อปรับปรุงกฎหมายคุ้มครองข้อมูลให้มีความทันสมัยมากขึ้น และใช้บังคับได้ ซึ่งเป็นการดำเนินการตามกฎระเบียบการคุ้มครองข้อมูลส่วนบุคคล (GDPR) ของสหราชอาณาจักร

โดย GDPR มีผลโดยตรงในทุกประเทศสมาชิกสหภาพยุโรปและได้ผ่านไปแล้ว ซึ่งหมายความว่าองค์กรต่าง ๆ จะยังคงต้องปฏิบัติตามกฎระเบียบนี้และยังคงต้องพิจารณา GDPR สำหรับภาระหน้าที่ทางกฎหมายส่วนใหญ่ อย่างไรก็ตาม GDPR เปิดโอกาสให้ประเทศสมาชิกมีข้อจำกัดในการจัดทำข้อกำหนดสำหรับวิธีการบังคับใช้ในประเทศ องค์ประกอบหนึ่งของ DPA 2018 คือรายละเอียดของสิ่งเหล่านี้ ดังนั้นจึงเป็นเรื่องสำคัญที่ GDPR และ DPA 2018 จะต้องศึกษาควบคู่กัน

หลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร[140]

แก่นหลักของกฎหมายสหราชอาณาจักร Data Protection Act 1998 ได้วางหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ประการด้วยกัน ซึ่งมีรายละเอียดดังต่อไปนี้[141]

---

[140] สกล อิศรประเสริฐ, “มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล | ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูลส่วนบุคคล,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2553), น. 84- 86

[141] Data Protection Act 1998,

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1) ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลอย่างยุติธรรมและชอบด้วยกฎหมายและการประมวลผลดังกล่าวต้องสอดคล้องกับกฎที่เฉพาะเจาะลงอย่างน้อยหนึ่งกฎ (กฎเพิ่มเติมอาจปรับใช้กับข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง)

2) ข้อมูลส่วนบุคคลจะได้รับเมื่อวัตถุประสงค์ที่ระบุไว้โดยเฉพาะและถูกกฎหมายหนึ่งวัตถุประสงค์ หรือมากกว่า และจะไม่ถูกประมวลผลเพิ่มเติมในลักษณะใด ๆ ที่ขัดกับวัตถุประสงค์นั้นหรือวัตถุประสงค์อื่น ๆ

3) ข้อมูลส่วนบุคคลจะต้องเพียงพอ มีความสอดคล้อง และมีปริมาณที่สัมพันธ์กับวัตถุประสงค์ใด ๆ หรือหลายวัตถุประสงค์ในการประมวลผล

4) ข้อมูลส่วนบุคคลจะต้องถูกต้องและหากจำเป็นต้องมีการปรับปรุงให้ทันสมัยอยู่เสมอ

5) ข้อมูลส่วนบุคคลที่ประมวลผลเพื่อวัตถุประสงค์หรือวัตถุประสงค์ใด ๆ จะไม่ถูกเก็บไว้นานเกินความจำเป็นสำหรับวัตถุประสงค์นั้นหรือวัตถุประสงค์เหล่านั้น

6) ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างสอดคล้องกับสิทธิของเจ้าของข้อมูลตามพระราชบัญญัติเพื่อวัตถุประสงค์

7) มาตรการทางเทคนิคที่เหมาะสมถูกนำมาใช้คัดค้านการประมวลผลเจ้าของข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือผิดกฎหมาย และป้องกันการสูญหายหรือการทำลายและความเสียหายที่มีต่อข้อมูลส่วนบุคคล

8) ข้อมูลส่วนบุคคลจะไม่ถูกถ่ายโอนไปยังประเทศหรือดินแดนนอกเขตเศรษฐกิจยุโรปเว้นแต่ประเทศหรือดินแดนนั้นได้รับการคุ้มครองในระดับที่เพียงพอสำหรับสิทธิและเสรีภาพของเจ้าของข้อมูลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

---

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.6 สหรัฐอเมริกา (United States of America)

[142]สหรัฐอเมริกาเป็นประเทศที่ใช้รูปแบบการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลแบบกฎหมายเฉพาะเรื่อง (Sectoral Law) ซึ่งมีข้อดีที่ทำให้สามารถกำหนดมาตรการ ทางกฎหมายให้เหมาะสมแก่กิจกรรมใดหรือธุรกิจใดเป็นการเฉพาะได้ โดยกฎหมายสำคัญที่ให้ ความคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ได้แก่ รัฐบัญญัติว่าด้วยความเป็นส่วนตัวในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ หรือ The Electronic Communication Privacy Act of 1986 (ECPA) (พ.ศ. 2529)

3.6.1 Health Insurance Portability and Accountability Act of 1996 หรือรัฐบัญญัติประกันสุขภาพแบบพกพาและความรับผิดชอบ ปี 1996 (พ.ศ. 2539) (HIPAA)

เอกสารย่อยทางการพยาบาลเพื่อให้สอดคล้องกับมาตรการคุ้มครองทางกายภาพของรัฐบัญญัติประกันสุขภาพพกพาและรัฐบัญญัติความรับผิดชอบ (HIPAA) ตั้งแต่ปี 1974 (พ.ศ. 2517) กฎหมายของรัฐบาลกลางได้ถูกส่งผ่านในสหรัฐอเมริกาเพื่อระบุสิทธิความเป็นส่วนตัวและการปกป้องผู้ป่วย แพทย์และหน่วยงานอื่น ๆ ที่ครอบคลุมถึงข้อมูลทางการแพทย์ หลายรัฐได้ผ่านกฎหมายของตนเองเพื่อพยายามปกป้องความเป็นส่วนตัวทางการแพทย์ของประชาชน กฎหมายระดับชาติที่สำคัญเกี่ยวกับความเป็นส่วนตัวทางการแพทย์คือรัฐบัญญัติประกันสุขภาพพกพาและรัฐบัญญัติความรับผิดชอบปี 1996 (HIPAA) แต่มีข้อถกเถียงมากมายเกี่ยวกับสิทธิการคุ้มครองของกฎหมาย

กฎหมายที่ครอบคลุมมากที่สุดผ่านไปเป็นประกันสุขภาพ Health Insurance Portability and Accountability Act of 1996 (พ.ศ. 2539) (HIPAA) ซึ่งได้รับการแก้ไขในภายหลังในปี ค.ศ. 2013 (พ.ศ. 2556) HIPAA มีมาตรฐานขั้นต่ำของรัฐบาลกลางเพื่อความเป็นส่วนตัวทางการแพทย์ชุดมาตรฐานสำหรับการใช้งานและการเปิดเผยข้อมูลของสุขภาพการป้องกัน ข้อมูล (PHI) และให้บทลงโทษทั้งทางแพ่งและทางอาญาสำหรับการละเมิด

ก่อนหน้า HIPAA มีเพียงกลุ่มคนบางกลุ่มเท่านั้นที่ได้รับการคุ้มครองภายใต้กฎหมายการแพทย์เช่นผู้ติดเชื้อ HIV หรือผู้ที่ได้รับความช่วยเหลือจาก Medicare[143] HIPAA ให้การคุ้มครองข้อมูลด้านสุขภาพและเพิ่มเติมกฎหมายของรัฐและรัฐบาลกลางเพิ่มเติม; แต่ควรเข้าใจว่าเป้าหมายของกฎหมายคือการสร้างสมดุลระหว่างผลประโยชน์ด้านสุขภาพความปลอดภัยและการวิจัยในขณะที่

---

[142] สโรชิณี กลิ่นหอม, “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์,” น. 831.

[143] Sobel, Richard, “The HIPAA Paradox: The Privacy Rule That's Not,” Hastings Center Report. 37: 40– 50. doi:10.1353/hcr.2007.0062, (2007), (https://doi.org/10.1353%2Fhcr.2007.0062) – via JSTOR.

ปกป้องข้อมูลทางการแพทย์ของแต่ละบุคคล หลายครั้งที่ความเป็นส่วนตัวลดลงเพื่อผลประโยชน์ของการวิจัยและสาธารณสุข

ตาม HIPAA หน่วยงานที่ครอบคลุมที่จะต้องปฏิบัติตามคำสั่งของกฎหมายกำหนดเป็นแผนสุขภาพสำนักหักบัญชีการดูแลสุขภาพและผู้ให้บริการด้านการดูแลสุขภาพที่ส่ง PHI ด้วยระบบอิเล็กทรอนิกส์ ผู้ร่วมธุรกิจของหน่วยงานที่ครอบคลุมเหล่านี้ยังอยู่ภายใต้กฎและข้อบังคับของ HIPAA

ในปี ค.ศ. 2008 (พ.ศ. 2551) รัฐสภาคองเกรส (United States Congress) ผ่านรัฐบัญญัติการไม่เลือกปฏิบัติทางข้อมูลทางพันธุกรรมของปี ค.ศ. 2008 (GINA)ซึ่งมีวัตถุประสงค์เพื่อห้ามการเลือกปฏิบัติทางพันธุกรรมสำหรับบุคคลที่แสวงหาการประกันสุขภาพและการจ้างงาน กฎหมายดังกล่าวยังรวมถึงบทบัญญัติที่ได้รับคำสั่งว่าข้อมูลทางพันธุกรรมที่นายจ้างเก็บไว้นั้นเก็บรักษาไว้ในไฟล์แยกต่างหากและห้ามเปิดเผยข้อมูลทางพันธุกรรมยกเว้นในสถานการณ์ที่ จำกัด

ในปี พ.ศ. 2556 หลังจาก GINA ผ่านไปกฎ HIPAA Omnibus ได้แก้ไขกฎ HIPAA เพื่อรวมข้อมูลทางพันธุกรรมในคำจำกัดความของข้อมูลสุขภาพที่ได้รับการคุ้มครอง (PHI) กฎนี้ยังขยาย HIPAA โดยขยายคำจำกัดความของผู้ร่วมธุรกิจให้ครอบคลุมถึงเอนทิตีที่ส่งหรือเข้าถึง PHI เช่น ผู้ค้าไอทีด้านสุขภาพ

ตรงกันข้ามกับความเชื่อที่ได้รับความนิยมรัฐบัญญัติประกันสุขภาพแบบพกพาและความรับผิดชอบ (HIPAA) ไม่ได้ให้ความคุ้มครองความเป็นส่วนตัวทางการแพทย์ที่แข็งแกร่งเนื่องจากมีเพียงกฎระเบียบที่เปิดเผยข้อมูลบางอย่างเท่านั้น[144]

รัฐบาลอนุญาตการเข้าถึงข้อมูลสุขภาพของแต่ละบุคคลสำหรับ "การรักษาการจ่ายเงินและทางเลือกการดูแลสุขภาพโดยไม่ได้รับความยินยอมจากผู้ป่วย" นอกจากนี้กฎ HIPAA นั้นกว้างมากและไม่ปกป้องบุคคลจากภัยคุกคามความเป็นส่วนตัวที่ไม่รู้จัก นอกจากนี้ผู้ป่วยจะไม่สามารถระบุสาเหตุของการละเมิดได้เนื่องจากข้อกำหนดที่ไม่สอดคล้องกัน เนื่องจากการรักษาความลับที่ จำกัด HIPAA อำนวยความสะดวกในการแบ่งปันข้อมูลทางการแพทย์เนื่องจากมีข้อ จำกัด เล็กน้อยจากองค์กรต่าง ๆ ข้อมูลสามารถแลกเปลี่ยนระหว่างสถาบันการแพทย์และสถาบันอื่นที่ไม่ใช่การแพทย์ได้ง่ายเนื่องจากกฎระเบียบเล็กน้อยของ HIPAA – ผลกระทบบางอย่างรวมถึงการสูญเสียงานเนื่องจากการแบ่งปันคะแนนเครดิตหรือการประกัน

---

[144] Sobel, Richard, “The HIPAA Paradox: The Privacy Rule That's Not,” Hastings Center Report. 37: 40– 50. doi:10.1353/hcr.2007.0062, (2007), (https://doi.org/10.1353%2Fhcr.2007.0062) – via JSTOR.

นอกจากนี้แพทย์ไม่จำเป็นต้องเก็บข้อมูลผู้ป่วยไว้เป็นความลับเพราะในหลาย ๆ กรณีการยินยอมของผู้ป่วยเป็นทางเลือก ผู้ป่วยมักไม่รู้ตัวว่าขาดความเป็นส่วนตัวเนื่องจากกระบวนการทางการแพทย์และรูปแบบไม่ได้ระบุอย่างชัดเจนถึงระดับความคุ้มครองของพวกเขา แพทย์เชื่อว่าโดยรวมแล้ว HIPAA จะทำให้เอกสารที่ผิดจรรยาบรรณและไม่เป็นมืออาชีพที่สามารถส่งผลกระทบต่อความเป็นส่วนตัวของบุคคลดังนั้นพวกเขาจึงต้องตอบคำเตือนเกี่ยวกับความเป็นส่วนตัวของพวกเขาเนื่องจากแพทย์ไม่สามารถรับรองความเป็นส่วนตัวของบุคคลได้มีโอกาสสูงที่ผู้ป่วยจะมีโอกาสได้รับการรักษาน้อยลงและแบ่งปันสิ่งที่แพทย์กังวล แต่ละคนได้ขอความยินยอมที่ดีขึ้นโดยถามว่าแพทย์สามารถเตือนพวกเขาก่อนที่จะแบ่งปันข้อมูลส่วนบุคคลใด ๆ ผู้ป่วยต้องการแบ่งปันข้อมูลทางการแพทย์กับแพทย์ของพวกเขา แต่พวกเขากังวลเกี่ยวกับการละเมิดที่อาจเกิดขึ้นซึ่งสามารถเผยแพร่ข้อมูลทางการเงินและข้อมูลที่เป็นความลับอื่น ๆ และด้วยความกลัวพวกเขาระวังที่จะเข้าถึง[145] เพื่อให้การป้องกันที่ดีขึ้นรัฐบาลได้สร้างกรอบการเก็บรักษาข้อมูลที่เป็นความลับซึ่งบางส่วนรวมถึงความโปร่งใสเกี่ยวกับขั้นตอนการเปิดเผยและการปกป้องข้อมูลและการติดตามกฎใหม่เหล่านี้เพื่อให้มั่นใจว่าข้อมูลของผู้คนจะไม่ได้รับผลกระทบ แม้ว่าจะมีกรอบการทำงานหลายประการที่จะทำให้มั่นใจได้ว่าจะได้รับการปกป้องข้อมูลทางการแพทย์ขั้นพื้นฐาน แต่หลายองค์กรไม่มีข้อกำหนดเหล่านี้ในการตรวจสอบ HIPAA ให้ความหวังที่ผิดพลาดแก่ผู้ป่วยและแพทย์เนื่องจากพวกเขาไม่สามารถปกป้องข้อมูลของตนเองได้ ผู้ป่วยมีสิทธิเล็กน้อยเกี่ยวกับสิทธิความเป็นส่วนตัวทางการแพทย์และแพทย์ไม่สามารถรับประกันได้[146]

รัฐบัญญัติประกันสุขภาพพกพาและความรับผิดชอบปี ค.ศ. 1996 (พ.ศ. 2539) (HIPAA) เป็นกฎหมายของรัฐบาลกลางที่กำหนดให้มีการสร้างมาตรฐานระดับชาติเพื่อปกป้องข้อมูลด้านสุขภาพของผู้ป่วยที่มีความอ่อนไหวจากการเปิดเผยโดยไม่ได้รับความยินยอมหรือความรู้จากผู้ป่วย กระทรวงสาธารณสุขและบริการมนุษย์แห่งสหรัฐอเมริกา (HHS) ออกกฎความเป็นส่วนตัว HIPAA เพื่อใช้ข้อกำหนดของ HIPAA กฎความปลอดภัย HIPAA ปกป้องชุดย่อยของข้อมูลที่ครอบคลุมโดยกฎความเป็นส่วนตัว

---

[145] Hosek, Susan, "Privacy of Individual Health Information," Patient Privacy, Consent, and Identity Management in Health Information Exchange: Issues for the Military Health System: 19–30(2013).

[146] Sobel, Richard, "The HIPAA Paradox: The Privacy Rule That's Not," Hastings Center Report. 37: 40–50. doi:10.1353/hcr.2007.0062, (2007), (https://doi.org/10.1353%2Fhcr.2007.0062). JSTOR 4625762 (https://www.jstor.org/st able/4625762). PMID 17844923 (https://www.ncbi.nlm.nih.gov/pubmed/17844923).

3.6.1.1 กฎความเป็นส่วนตัว HIPAA

มาตรฐานกฎความเป็นส่วนตัวระบุถึงการใช้และการเปิดเผยข้อมูลสุขภาพของแต่ละบุคคล (เรียกว่า "ข้อมูลสุขภาพที่ได้รับการป้องกัน") โดยหน่วยงานที่อยู่ภายใต้กฎความเป็นส่วนตัว บุคคลและองค์กรเหล่านี้เรียกว่า "เอนทิตีที่ครอบคลุม" กฎความเป็นส่วนตัวยังมีมาตรฐานสำหรับสิทธิ์ของแต่ละบุคคลในการทำความเข้าใจและควบคุมการใช้ข้อมูลสุขภาพของพวกเขา เป้าหมายหลักของกฎความเป็นส่วนตัวคือเพื่อให้แน่ใจว่าข้อมูลด้านสุขภาพของแต่ละคนได้รับการปกป้องอย่างเหมาะสมในขณะที่อนุญาตให้มีการไหลเวียนของข้อมูลด้านสุขภาพที่จำเป็นในการจัดหาและส่งเสริมการดูแลสุขภาพที่มีคุณภาพสูงและเพื่อปกป้องสุขภาพและความเป็นอยู่ที่ดีของสาธารณะ กฎความเป็นส่วนตัวก่อให้เกิดความสมดุลซึ่งอนุญาตการใช้ข้อมูลที่สำคัญในขณะที่ปกป้องความเป็นส่วนตัวของผู้ที่แสวงหาการดูแลและรักษา

3.6.1.2 กฎความปลอดภัย HIPAA

ในขณะที่กฎความเป็นส่วนตัว HIPAA ปกป้องข้อมูลด้านสุขภาพที่ได้รับการป้องกัน (PHI), กฎความปลอดภัยปกป้องส่วนย่อยของข้อมูลที่ครอบคลุมโดยกฎความเป็นส่วนตัว ชุดย่อยนี้เป็นข้อมูลด้านสุขภาพที่สามารถระบุตัวตนได้ทั้งหมดซึ่งเอนทิตีที่ครอบคลุมจะสร้างรับรักษาหรือส่งในรูปแบบอิเล็กทรอนิกส์ ข้อมูลนี้เรียกว่า "ข้อมูลสุขภาพที่ได้รับการคุ้มครองทางอิเล็กทรอนิกส์" (e-PHI) กฎความปลอดภัยใช้ไม่ได้กับ PHI ที่ส่งผ่านวาจาหรือเป็นลายลักษณ์อักษร เพื่อให้สอดคล้องกับกฎความปลอดภัย HIPAA เอนทิตีที่ครอบคลุมทั้งหมดจะต้องทำสิ่งต่อไปนี้ :

1. รับประกันความลับความสมบูรณ์และความพร้อมของข้อมูลด้านสุขภาพที่ได้รับการคุ้มครองทางอิเล็กทรอนิกส์ทั้งหมด
2. ตรวจจับและป้องกันภัยคุกคามที่คาดว่าจะมีต่อความปลอดภัยของข้อมูล
3. ป้องกันการใช้หรือการเปิดเผยที่ไม่อาจคาดการณ์ได้
4. รับรองการปฏิบัติตามโดยพนักงานของพวกเขา

3.7 ประเทศไทย

การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น มีอยู่ในกฎหมายหลายฉบับ ซึ่งได้รับการบัญญัติไว้ในระดับรัฐธรรมนูญแห่งราชอาณาจักรไทย และกฎหมายระดับพระราชบัญญัติที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

3.7.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้บัญญัติการให้ความคุ้มครองข้อมูลส่วนบุคคล ในหมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทย มาตรา 32 ซึ่งกำหนดให้สิทธิแก่บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว และในวรรคสองได้บัญญัติเกี่ยวกับการกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

แม้ว่ารัฐธรรมนูญจะได้มีการบัญญัติรับรองสิทธิในข้อมูลส่วนบุคคลไว้โดยชัดแจ้ง แต่เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและมีผลในการปฏิบัติ จึงควรมีการกำหนดมาตรการและรายละเอียด ในการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะในกฎหมายลำดับรอง เช่น พระราชบัญญัติ เพื่อให้ประชาชน ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล หรือบุคคลที่เกี่ยวข้องกับการจัดเก็บข้อมูล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิมากยิ่งขึ้น

3.7.2 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550

พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ได้บัญญัติเกี่ยวกับข้อมูลของผู้เข้ารับบริการทางการแพทย์ ซึ่งคือ ข้อมูลด้านสุขภาพของบุคคล ซึ่งเป็นข้อมูลส่วนบุคคลที่ไม่สามารถเปิดเผยได้เว้นแต่ได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลนั้น

โดยได้บัญญัติเกี่ยวข้อมูลด้านสุขภาพของบุคคล ไว้ในหมวด 1 สิทธิและหน้าที่ด้านสุขภาพ มาตรา 7 ข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคล นั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้

3.7.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่มีผลกระทบต่อผู้คนในปัจจุบันเป็นอย่างมาก โดยมีความสำคัญที่มุ่งเน้นไปที่องค์กร หน่วยงาน หรือนิติบุคคล เพื่อให้มีมาตรฐานในการจัดการข้อมูลส่วนบุคคลอย่างมีความเหมาะสมและเพียงพอ หากต้องมีการใช้ข้อมูลส่วนบุคคล ทั้งนี้ก็เพื่อป้องกันความเสี่ยงที่จะมีผลกระทบไปถึงการรักษาความลับ (Confidentiality)

ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ที่ก่อให้เกิดแนวโน้มให้เกิดผลกระทบเชิงลบหรือความเสียหายในระดับบุคคลหรือองค์กร

[147]สาเหตุหลักที่ประเทศไทยต้องมี พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากสหภาพยุโรป (European Union: EU) ได้ออก GDPR (General Data Protection Regulation) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล บังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2561 ซึ่งนอกจากมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว ผู้ประกอบการในไทยที่ต้องติดต่อรับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ นอกจากนี้คือความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีผลกระทบต่อการค้าระหว่างประเทศและการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลย่อมทำให้เสียโอกาสและความเชื่อมั่นจากกลุ่มประเทศในสหภาพยุโรป และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัวเรื่อง Data Protection เพราะเหตุการณ์ใหญ่ ๆ ที่เกิดขึ้นแล้ว เช่น การรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้ เฟซบุ๊ก (Facebook) หลายล้านบัญชี เป็นต้น

สาระสำคัญของ พระราชบัญญัติฉบับนี้ มี 3 ประเด็นหลัก ดังนี้

1. เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น กล่าวคือ ต้องขออนุมัติจากเจ้าของข้อมูลก่อน เช่น หากแอปพลิเคชันหนึ่งจะเก็บข้อมูลบัตรเครดิตของเราไว้ในระบบ ก็ต้องมีข้อความให้เรากดยืนยันเพื่อยินยอม พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวม และการใช้ หากเราไม่ยินยอมให้ใช้ข้อมูลบัตรเครดิต ผู้ให้บริการแอปพลิเคชันนั้นก็ไม่สามารถใช้ข้อมูลบัตรเครดิตของเราได้

2. ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล เช่น สถานพยาบาลจะต้องเก็บข้อมูลของผู้ป่วยให้เป็นความลับและไม่เปิดเผยให้กับผู้อื่น ธนาคารต้องเก็บรักษาข้อมูลเกี่ยวกับรายการถอน

3. เจ้าของข้อมูลมีสิทธิถอนความยินยอม ขอให้ลบหรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล

---

[147] “Acinfotec,” https://www.acinfotec.com/2019/07/23/data-protection-law-2562/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้นิยามความของ “ข้อมูลส่วนบุคคล” และกรณีไม่ให้เปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล บัญญัติไว้ดังนี้

มาตรา 6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

องค์ประกอบของบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลประกอบไปด้วยองค์ประกอบหลักสามข้อ คือ

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลระบุไปถึง

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 19 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดใน

วัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

นอกจากนี้ยังมีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ซึ่งกำหนดเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคล[148]ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) กำหนด โดยกำหนดหน่วยงานและกิจการที่ไม่อยู่ในบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไว้ในบัญชีท้าย พระราชกฤษฎีกา (7) กิจการด้านการแพทย์และสาธารณสุข

---

[148] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6 “ผู้ควบคุมข้อมูลส่วนบุคคล,” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3.7.4 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ในปัจจุบันนี้ประเทศไทย มีกฎหมายทีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลใช้บังคับอยู่แต่กฎหมายฉบับนี้เป็นเพียงการคุ้มครองข้อมูลส่วนบุคคลเฉพาะหน่วยงานของรัฐเท่านั้น ซึ่งก็คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งประกาศใช้ เมื่อวันที่ 2 กันยายน พ.ศ. 2540 และประกาศลงในราชกิจจานุเบกษา เล่ม 114 ตอนที่ 46 ก. หน้า 1 ลงวันที่ 10 กันยายน 2540[149] ความสำคัญของพระราชบัญญัติฉบับนี้ คือ ในระบอบประชาธิปไตย การให้ประชาชนมีโอกาสกว้างขวางในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐเป็นสิ่งจำเป็นเพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความจริงอันเป็นการส่งเสริมให้มีความเป็นรัฐบาล โดยประชาชนมากยิ่งขึ้นสมควรกำหนดให้ประชาชนมีสิทธิได้รู้ข้อมูลข่าวสารของราชการ โดยมีข้อยกเว้นอันไม่ต้องเปิดเผยที่แจ้งชัดและจำกัดเฉพาะข้อมูลข่าวสารที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือ ต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้เพื่อพัฒนาระบบประชาธิปไตยให้มั่นคงและจะยังผลให้ประชาชนมีโอกาสรู้ถึงสิทธิหน้าที่ของตนอย่างเต็มที่

มาตรา 4 ในพระราชบัญญัตินี้

“ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงานบรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

---

[149] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

มาตรา 15 ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน

(4) การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด

(5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร…

มาตรา 25 ภายใต้บังคับมาตรา 14 และมาตรา 15 บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา 9 วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้...

3.7.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ปัจจุบันเทคโนโลยีด้านต่าง ๆ มีความก้าวหน้าเพื่อให้เท่าทันต่อสถานการณ์ปัจจุบัน แต่ในอดีตประมาณ ก่อน ปี พ.ศ. 2550 ประเทศไทยได้ดำเนินการติดต่ออินเทอร์เน็ตในปี พ.ศ. 2530 ในลักษณะของการใช้บริการจดหมายอิเล็กทรอนิกส์แบบแลกเปลี่ยนถุงเมล์เป็นครั้งแรก โดยการใช้งานอินเทอร์เน็ตชนิดเต็มรูปแบบตลอด 24 ชั่วโมง ในประเทศไทยนั้นเกิดขึ้นเมื่อเดือน กรกฎาคม ปี พ.ศ. 2535[150]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติของกฎหมายที่พัฒนาขึ้นให้สอดคล้องกับเทคโนโลยีคอมพิวเตอร์ที่มีผลกระทบกับวิถีชีวิตของบุคคลในสังคมอย่างมาก คอมพิวเตอร์มีผลต่อพฤติกรรมของมนุษย์ใน หลายรูปแบบและได้มีการใช้คอมพิวเตอร์เป็นเครื่องมือสื่อสาร ซึ่งกฎหมายฉบับนี้มีเจตนารมณ์ คือ การกำหนดฐานความผิดและบทลงโทษ รวมทั้งการกำหนดเกี่ยวกับอำนาจพนักงาน เจ้าหน้าที่ ผู้ให้บริการ และผู้ใช้บริการ โดยครอบคลุมถึงการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะต่าง ๆ โดยเน้นการเจาะระบบคอมพิวเตอร์ หรือเจาะข้อมูลคอมพิวเตอร์ที่มีผลกระทบต่อความลับ (Confidentiality) ความครบถ้วน (Integrity) สภาพพร้อม

[150] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ใช้งาน (Availability)[151] ต่อมาได้มีประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความเกี่ยวกับคอมพิวเตอร์ในปัจจุบันซึ่งมีรูปแบบการระทำความที่มีความซับซ้อนมากยิ่งขึ้นตามความพัฒนาของเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วเช่นเดียวกัน จึงต้องมีการแก้ไขเพิ่มเติมในฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดนั้น อีกทั้งการปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์

คำนิยาม ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่เกี่ยวข้อง

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

3.7.6 ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายแพ่งและพาณิชย์ของประเทศไทย ได้มีการบัญญัติถึงความผิดฐานกระทำละเมิด ซึ่งอาจนำความเสียหายที่เกิดจากการเปิดเผยข้อมูลส่วนบุคคลมาปรับใช้ได้โดยกฎหมายได้กำหนดให้การกระทำดังกล่าวมีความรับผิดตามที่ได้บัญญัติไว้ในมาตรา 420 ซึ่งมีสาระสำคัญ คือ ผู้ใดจงใจหรือประมาทเลินเล่อ กระทำต่อบุคคลอื่นโดยผิดกฎหมาย ให้เขาเสียหายถึงแก่ชีวิต ร่างกาย อนามัย เสรีภาพ ทรัพย์สิน หรือสิทธิอย่างใดอย่างหนึ่ง ถือว่าผู้นั้นกระทำละเมิดต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น[152]

---

[151] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

[152] ประมวลกฎหมายแพ่งและพาณิชย์ (แก้ไขเพิ่มเติม ฉบับที่ 22 พ.ศ. 2558), มาตรา 420

อย่างไรก็ตาม ความผิดตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 แม้จะระบุไว้ว่าการกระทำต่อบุคคลอื่นโดยผิดกฎหมายอันเป็นการละเมิด แต่ก็ไม่ได้ครอบคลุมถึงความคุ้มครองในเรื่องข้อมูลส่วนบุคคลเอาไว้อย่างชัดเจน และหากเป็นการได้ข้อมูลส่วนบุคคลโดยมิได้เกิดความเสียหายอย่างชัดแจ้ง ก็ไม่เป็นความผิดตามมาตรานี้ อีกทั้งไม่มีโทษทางอาญาเพื่อลงโทษผู้กระทำผิดเข็ดหลาบอีกด้วย

บทที่ 4
วิเคราะห์เปรียบเทียบการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ เฉพาะกรณีข้อมูลส่วนบุคคลของผู้ป่วย

ในบทนี้จะทำการวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยของประเทศไทยกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยต่างประเทศ โดยผู้วิจัยได้นำข้อมูลและหลักกฎหมายที่เกี่ยวข้องทั้งของต่างประเทศและในประเทศไทยมาเปรียบเทียบกัน เพื่อให้เห็นถึงการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย เมื่อมีเทคโนโลยีมาเกี่ยวข้อง ซึ่งจะนำไปสู่การแก้ไข ปรับปรุงกฎหมาย ทั้งยังรวมถึงการมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยนี้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยได้ดำเนินการศึกษา ดังต่อไปนี้

4.1 วิเคราะห์การควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วยในราชอาณาจักรไทย

4.1.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

ประเทศไทยในปัจจุบันมีกฎหมายว่าด้วยความคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะในบางเรื่อง แต่ไม่มีกฎหมายฉบับใดที่บัญญัติขึ้นโดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลสำหรับทางด้านการแพทย์ เมื่อนำหลักความคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศและกฎหมายฉบับต่าง ๆ ที่ได้บัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมาวิเคราะห์และเปรียบเทียบ ซึ่งจะพบว่าแม้รัฐธรรมนูญแห่งราชอาณาจักรไทยได้มีการบัญญัติการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดแจ้งก้ตาม แต่เป็นลักษณะการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับกว้าง เพื่อให้ประชาชนทุกคนในประเทศได้รับความคุ้มครองให้สิทธิที่พึงมีพึงได้เป็นการทั่วไป เนื่องจากการมีบทบัญญัติความคุ้มครองในลักษณะเป็นการเฉพาะและมีรายละเอียดของหลักเกณฑ์หรือมาตรการต่าง ๆ ไว้ในรัฐธรรมนูญได้ นอกจากนี้เพียงบทบัญญัติในรัฐธรรมนูญเพียงอย่างเดียวก็ไม่อาจให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยได้อย่างเพียงพอ ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและมีผลในการปฏิบัติ จึงควรมีการกำหนดมาตรการและรายละเอียด ในการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ เพื่อให้ประชาชนซึ่งเข้ารับ

บริการทางการแพทย์ ไม่ว่าในรูปแบบผู้ป่วยนอกหรือผู้ป่วยในก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคล[153] ผู้ประมวลผลข้อมูลส่วนบุคคล[154] หรือบุคคลที่เกี่ยวข้องกับการจัดเก็บข้อมูล จึงจะทำให้การคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์มีความปลอดภัยในข้อมูลส่วนบุคคลของผู้ป่วยมากยิ่งขึ้น

4.1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นอกจากนี้ยังมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมุ่งเน้นความสำคัญไปที่องค์กร หน่วยงาน หรือนิติบุคคล เพื่อให้มีมาตรฐานในการจัดการข้อมูลส่วนบุคคลอย่างมีความเหมาะสมและเพียงพอ ซึ่งมีความคุ้มครองข้อมูลส่วนบุคคลโดยมั่งเน้นว่า เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น อีกนัยหนึ่งคือการเปิดเผยข้อมูลหรือกระทำการอย่างใด ๆ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน และผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล แต่อย่างไรก็ตามยังมีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ซึ่งได้กำหนดเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล แก่ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้มีความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล[155] ซึ่งต้องครอบคลุมถึง

1) มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)
2) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และ
3) มาตรการป้องกันทางกายภาพ (Physical Safeguard)

---

[153] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

[154] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 “ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินกสรดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

[155] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563, นิยาม “ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control)[156] ซึ่งในปัจจุบันนี้ มีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางหมวด เป็นระยะเวลา 1 ปี จนถึงวันที่ 31 จนถึงวันที่ 31 พฤษภาคม 2564 โดยในหมวดที่ยกเว้นดังกล่าวนั้น ยกเว้นกิจการด้านการแพทย์และสาธารณสุข ซึ่งส่งผลให้ข้อมูลส่วนบุคคลของผู้ป่วยซึ่งใช้บริการทางแพทย์ อาจไม่ได้รับความคุ้มครองข้อมูลส่วนบุคคลที่ให้ไว้แก่โรงพยาบาล

โดยหลักการในทางปฏิบัติข้อมูลส่วนบุคคลของผู้ป่วยซึ่งบันทึกลงในเวชระเบียนอิเล็กทรอนิกส์นั้น ผู้ที่ดูแลข้อมูลดังกล่าวจึงเป็นบุคลากรทางการแพทย์ โดยข้อมูลส่วนบุคคลของผู้ป่วยนั้นแม้แพทย์ซึ่งจะเป็นเจ้าของไข้ของผู้ป่วยก็ไม่สามารถเปิดเผยข้อมูลของผู้ป่วยแก่บุคคลอื่นได้ โดยเมื่อแพทย์ได้ทำการบันทึกข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องดำเนินการส่งข้อมูลของผู้ป่วยไปที่เวชระเบียนซึ่งมีเจ้าหน้าที่ของโรงพยาบาลเป็นผู้ดูแลข้อมูลดังกล่าว ซึ่งเจ้าหน้าที่เวชระเบียนถือว่ามีหน้าที่ในการรักษาข้อมูลส่วนบุคคลของผู้ป่วยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากมีหน้าเก็บรวบรวมข้อมูล รวมการไม่เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากความยินยอม ซึ่งหากพิจารณากรณีที่ข้อมูลส่วนบุคคลของผู้ป่วยถึงเปิดเผยแก่ภายนอกโดยปราศจากความยินยอมของผู้ป่วยไม่ว่าโดยวิธีการอย่างใด ๆ เจ้าหน้าที่เวชระเบียนซึ่งถือเป็นผู้ดูแลข้อมูลนั้นย่อมมีความรับผิดต่อข้อมูลของผู้ป่วย และในกรณีนี้โรงพยาบาลซึ่งเจ้าหน้าที่เวชระเบียนนั้นปฏิบัติหน้าที่จึงจำต้องพิจารณาว่าข้อมูลส่วนบุคคลของผู้ป่วยเป็นกรรมสิทธิ์ของโรงพยาบาลด้วยหรือไม่ ดังนั้นเมื่อไม่มีการกำหนดมาตรการการให้ความคุ้มครองหรือหน่วยงานที่ต้องรับผิดชอบต่อข้อมูลส่วนบุคคลของผู้ป่วยไว้โดยชัดแจ้งจึงยังคงเป็นปัญหาในการพิจารณา

แต่อย่างไรก็ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐานและให้ความคุ้มครองโดยกว้าง ๆ แต่ไม่ได้กล่าวถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยที่ถูกจัดเก็บในรูปแบบอิเล็กทรอนิกส์ หรือเวชระเบียนอิเล็กทรอนิกส์ นอกจากนี้ไม่ได้กล่าวถึงข้อมูลที่มีอ่อนไหว (Sensitive Data) ซึ่งจะต้องมีความคุ้มครองข้อมูลประเภทนี้อย่างมีมาตรฐานและมีความเหมาะสม ซึ่งการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยอย่างมีหลักเกณฑ์ หรือกำหนดมาตรการที่ให้ความคุ้มครองที่มีความน่าเชื่อถือ และปลอดภัย เป็นการให้ความเชื่อมั่นแก่ผู้ป่วยซึ่งเป็นเจ้าของข้อมูล

---

[156] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม Ministry of Digital Economy and Society, "ดีอีเอส คลอดประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล," https://www.mdes.go.th/news/detail/

กรณีข้อมูลส่วนบุคคลทางการแพทย์ของผู้ป่วยซึ่งบันทึกไว้ในเระเบียนอิเล็กทรอนิกส์โดยบุคคลากรทางแพทย์นั้น และมีการส่งต่อข้อมูลระหว่างโรงพยาบาลเพื่อส่งข้อมูลของผู้ป่วยจากอีกโรงพยาบาลหนึ่งซึ่งมีข้อมูลของผู้ป่วยไปยังโรงพยาบาลอีกแห่งหนึ่งซึ่งผู้ป่วยดำเนินการรักษาอันเนื่องจากเป็นเหตุฉุกเฉิน หรือการย้ายโรงพยาบาลเพื่อให้ความต่อเนื่องในการรักษาเป็นไปอย่างมีประสิทธิภาพนั้น การใช้ระบบเครือข่ายอิเล็กทรอนิกส์ซึ่งเป็นเทคโนโลยีการสื่อสารทางการแพทย์จึงเป็นเส้นทางในการส่งข้อมูลที่สะดวก และรวดเร็ว แต่อย่างไรก็ตามก็มีความเสี่ยงที่ข้อมูลของผู้ป่วยจะถูกเข้าถึงหรือเปิดเผยได้ ซึ่งปัจจุบันนี้เห็นว่าในประเทศไทยยังคงขาดบุคลากรและหน่วยงานที่รับผิดเกี่ยวกับการให้ความคุ้มครองต่อข้อมูลส่วนบุคคลของผู้ป่วย เพื่อพิจารณากระบวนการโอนข้อมูลของผู้ป่วยไปมาระหว่างโรงพยาบาล โดยต้องมีผู้ควบคุมข้อมูลและประมวลผลข้อมูลแจ้งต่อเจ้าของข้อมูล และประเมินความเหมาะสมในการโอนข้อมูล นอกจากนี้ในกรณีมีการกระทำที่เกิดขึ้นโดยไม่รับอนุญาตควรมีบทลงโทษต่อการกระทำนั้น

4.1.3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัติขึ้นโดยมีเจตนารมณ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคล แต่มีข้อจำกัดในการให้ความคุ้มครองอยู่ เนื่องจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้ความคุ้มครองเพียงเฉพาะข้อมูลข่าวสารที่อยู่ในความครอบครองและควบคุมดูแลของหน่วยงานรัฐเพียงอย่างเดียวเท่านั้น แต่ไม่ครอบคลุมไปถึงข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน ซึ่งมีปริมาณข้อมูลในการจัดเก็บไม่ต่างไปจากข้อมูลของหน่วยงานภาครัฐ เช่น ข้อมูลส่วนบุคคลของผู้ป่วยในโรงพยาบาลเอกชน ข้อมูลของลูกค้าธนาคารซึ่งไม่ใช่ของภาครัฐ ข้อมูลของพนักงานในบริษัทหรือองค์กรในภาคเอกชนอื่น ๆ หรือข้อมูลของสมาชิกเพื่อรับบริการในด้านต่าง ๆ เช่น สมาชิกร้านอาหาร สมาชิกร้านต่าง ๆ เพื่อรับส่วนลดหรือสะสมแต้มจากการใช้บริการ ส่วนพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ให้ความคุ้มครองทางด้านสุขภาพของบุคคล และเก็บรักษาความลับของผู้ป่วย ไม่ให้ผู้คนอื่น ๆ ใดนำไปเปิดเผยในประการที่น่าจะสร้างความเสียหายแก่บุคคลผู้เป็นเจ้าของข้อมูล แต่ไม่ได้มีกล่าวถึงในความคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

4.1.4 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีบทบัญญัติเพื่อให้สอดคล้องกับเทคโนโลยีคอมพิวเตอร์ และเจตนารมณ์ในการกำหนดฐานความผิดและบทลงโทษรวมทั้งการกำหนดเกี่ยวกับอำนาจพนักงาน เจ้าหน้าที่ ผู้ให้บริการ และผู้ใช้บริการโดยครอบคลุมถึงการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะต่าง ๆ โดยเน้นการเจาะระบบคอมพิวเตอร์ หรือเจาะข้อมูลคอมพิวเตอร์ที่มีผลกระทบต่อ ความลับ (Confidentiality) ความ

ครบถ้วน (Integrity) สภาพพร้อมใช้งาน (Availability) กรณีมีบุคคลเจาะระบบข้อมูลอิเล็กทรอนิกส์ โดยที่เจ้าของข้อมูลไม่ได้อนุญาต เช่น การปล่อยไวรัส มัลแวร์ หรือแฮกเกอร์ เพื่อเข้าถึงข้อมูลโดยมีวัตถุประสงค์เพื่อขโมย หรือทำให้ข้อมูลได้รับความเสียหายนั้นได้มีการกำหนดความรับผิดไว้ในมาตรา 5 - มาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่ในกรณีที่มีบุคคลเจาะเข้าไปในระบบอิเล็กทรอนิกส์เพื่อเข้าถึงฐานข้อมูลที่ทางโรงพยาบาล แพทย์ และเจ้าหน้าที่ดำเนินการให้ความควบคุมดุแลข้อมูลส่วนบุคคลของผู้ป่วยเพื่อเข้ารับบริการทางการแพทย์มิได้กำหนดถึงมาตรการเยียวยาทางแพ่งแก่เจ้าของข้อมูลซึ่งได้รับความเสียหายไว้

การรักษาทางการแพทย์โดยใช้เทคโนโลยีทางการแพทย์นั้น มีการใช้กันอย่างแพร่หลายในสถานพยาบาลต่าง ๆ เมื่อเทคโนโลยีมีความก้าวหน้า การเก็บข้อมูล นำเข้า และส่งออกนั้นยอมต้องมีการเชื่อมต่อกับระบบออนไลน์ ทำให้สามารถทำการบันทึกข้อมูลได้อย่างรวดเร็วมากยิ่งขึ้น อีกทั้งการส่งผ่านข้อมูลยังมีความสะดวกรวดเร็วกว่าการจัดเก็บข้อมูลในรูปแบบเก่าที่เป็นแฟ้มเวชระเบียนซึ่งทำให้การสืบค้นเป็นไปด้วยความลำบาก แต่อย่างไรก็ตามการที่เทคโนโลยีมีความก้าวหน้าขึ้นอย่างทุกวันนี้นั้นก็มีผลกระทบด้วยเช่นกัน คือ การเข้าถึงข้อมูลมีความสะดวกรวดเร็วขึ้น แต่ก็อาจถูกเข้าถึงโดยบุคคลอื่นซึ่งไม่ใช่เจ้าของข้อมูลด้วยเช่นกัน และถูกนำออกไปเปิดเผยแก่สาธารณะชน ซึ่งข้อมูลส่วนบุคคลของผู้ป่วยมีข้อมูลส่วนบุคคลที่มีความอ่อนไหวอยู่ด้วย และไม่สามารถเปิดเผยต่อบุคคลอื่นได้ แม้ว่าบุคคลนั้นจะเป็นญาติ หรือคู่สมรสก็ตาม โดยข้อมูลที่มีความจึงมีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บ แต่อาจไม่เพียงพอต่อการคุ้มครองได้อย่างครอบคลุม

โรงพยาบาลเป็นหน่วยงานทางสาธารณที่มีทั้งในภาครัฐและเอกชน ซึ่งให้บริการทางการแพทย์ในการดำเนินการตรวจวินิจฉัยโรค รักษาโรค ป้องกันโรค และกระบวนการฟื้นฟูสมรรถภาพทางร่างกาย และมีหน้าที่ให้การเก็บรักษาข้อมูล และไม่เปิดเผยข้อมูลของผู้ป่วยให้แก่บุคคลที่ไม่ได้เป็นเจ้าของ ซึ่งในปัจจุบันพบว่าข้อมูลส่วนบุคคลของผู้ป่วยถูกจัดเก็บไว้ในรูปแบบของเวชระเบียนอิเล็กทรอนิกส์ การจัดเก็บข้อมูลประวัติของผู้ป่วยของสถานพยาบาล หรือสถานบริการสาธารณสุขในรูปของข้อมูลอิเล็กทรอนิกส์รวมถึงการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างสถานพยาบาล เพื่อประโยชน์ต่อการให้บริการรักษาอย่างต่อเนื่อง เช่น การค้นประวัติย้อนหลังของผู้ป่วยเกี่ยวกับรักษาที่ผ่านมา การจัดเก็บในรูปฐานข้อมูลอกจากง่ายต่อการสืบค้นแล้ว การจัดเก็บยังเป็นไปโดยง่ายกว่าการจัดเก็บเวชระเบียนในแบบเดิมที่เป็นรูปแบบเอกสารกระดาษซึ่งอาจเสียหายจากการจัดเก็บได้ และยังค้นข้อมูลได้ยากกว่าการค้นในนฐานข้อมูลอิเล็กทรอนิกส์ ทำให้ในปัจจุบันโรงพยาบาลใช้รูปแบบการจัดข้อมูลอิเล็กทรอนิกส์

การที่ข้อมูลส่วนบุคคลของผู้ป่วยอยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งทำให้การส่งผ่านมีความสะดวกมากขึ้น แต่อย่างไรก็ตามเมื่อข้อมูลอยู่ในสภาพที่ไม่อาจจับต้องได้จนกว่าจะมีนำข้อมูลออกมาให้รูปเอกสาร ซึ่งมีความเสี่ยงต่อการถูกละเมิดข้อมูลได้จากภัยคุกคามความปลอดภัยในรูปแบบใหม่ คือ การแฮคข้อมูล หรือใช้โปรแกรมคอมพิวเตอร์ให้การแทรกแซงเข้าไปในระบบหรือคอมพิวเตอร์เครื่องอื่น ซึ่งทำให้ข้อมูลที่ถูกเก็บไว้อาจได้รับความเสียจากโปรมแกรมแทรกซ้อนบางอย่าง หรือถูกนำข้อมูลออกไปเปิดเผยโดยผิดกฎหมาย กรณีเช่นนี้จึงจำต้องพิเคราะห์ว่า เมื่อข้อมูลถูกละเมิดโดยบุคคลภายนอก และทำให้เจ้าของอาจได้รับความเสียหาย จึงต้องพิจารณาว่าเหตุนี้เป็นความรับผิดของใครระหว่างโรงพยาบาล หรือบุคลากรทางแพทย์

กรณีเป็นโรงพยาบาลในหน่วยงานของรัฐ จึงต้องพิจารณาจาก พระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539 ซึ่งมีเจตนารมณ์เพื่อสร้างหลักความรับผิดของเจ้าหน้าที่ให้เป็นไปอย่างเป็นเหตุเป็นผล (Rational) กล่าวคือ ภาระหน้าที่ เงินเดือน และความรับผิดของเจ้าหน้าที่นั้น รัฐต้องกำหนดให้ได้สัดส่วนกันอันจะสร้างความเป็นธรรมให้แก่เจ้าหน้าที่และเพิ่มพูนประสิทธิภาพในการปฏิบัติงานของรัฐ และต้องการพิจารณาว่าการกระทำใดจะเป็นการกระทำละเมิดในการปฏิบัติหน้าที่ของเจ้าหน้าที่ สามารถแยกพิจารณาได้ดังนี้ คือ มีการกระทำละเมิดเกิดขึ้น และการละเมิดนั้นกระทำโดยเจ้าหน้าที่ในการปฏิบัติหน้าที่

1. การกระทำละเมิด ตามพระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539 เป็นไปตามมาตรา 420 แห่งประมวลกฎหมายแพ่งและพาณิชย์[157] ซึ่งมีองค์ประกอบ ดังนี้

1) มีการกระทำ หมายถึง การเคลื่อนไหวร่างกายโดยรู้สำนึกในการเคลื่อนไหวนั้น และอยู่ในบังคับของจิตใจผู้กระทำ และรวมถึงการงดเว้นการกระทำที่ตนมีหน้าที่ตามกฎหมายที่ต้องกระทำ และการงดเว้นนั้นเป็นเหตุให้เกิดความเสียหายขึ้น

2) โดยจงใจหรือประมาทเลินเล่อ

- โดยจงใจ หมายถึง รู้สำนึกถึงผลหรือความเสียหายจากการกระทำของตน

- โดยประมาทเลินเล่อ หมายถึง เป็นการกระทำโดยปราศจากความระมัดระวัง ซึ่งบุคคลในภาวะเช่นนั้นจำต้องมี โดยต้องเปรียบเทียบกับบุคคลที่ต้องมีความระมัดระวังตามพฤติการณ์ และตามฐานะในสังคมเช่นเดียวกับผู้กระทำความเสียหาย

---

[157] มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อทำต่อบุคคลอื่น โดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

3) โดยผิดกฎหมาย เป็นการกระทำโดยไม่มีอำนาจหรือไม่มีสิทธิหรือโดยมิชอบด้วยกฎหมาย (Unlawful) และรวมความถึงการใช้อำนาจที่มีอยู่เกินส่วนหรือใช้อำนาจตามกฎหมายเพื่อกลั่นแกล้งผู้อื่น

4) เกิดความเสียหายแก่บุคคลอื่นความเสียหายนั้นจะเป็นความเสียหายที่เกิดแก่ชีวิตร่างกาย อนามัย เสรีภาพ ทรัพย์สิน หรือสิทธิอย่างหนึ่งอย่างใดก็ได้ แต่ต้องเป็นความเสียหายที่แน่นอน ไม่ว่าจะเกิดขึ้นแล้วในปัจจุบันหรือจะเกิดขึ้นในอนาคตก็จะต้องเป็นความเสียหายที่จะเกิดขึ้นอย่างแน่นอน

ในกรณีของโรงพยาบาลเอกชนจะใช้หลักตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 มาใช้พิจารณาความรับผิด

4.2 วิเคราะห์มาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีทางการแพทย์ และข้อมูลส่วนบุคคลของผู้ป่วย ในต่างประเทศ

4.2.1 สหภาพยุโรป

จากการศึกษา สหภาพยุโรป มีหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2 กลุ่ม คือ กฎหมายเฉพาะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งวางหลักการคุ้มครองข้อมูลส่วนบุคคลประการต่าง ๆ ไว้โดยเฉพาะ และกฎหมายเกี่ยวกับสิทธิมนุษยชน ซึ่งวางหลักทั่วไปหรือหลักกว้าง ๆ ในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลไว้ในส่วนนี้จะได้ชี้ให้เห็นกรอบกฎหมายยุโรปที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลทั้งสองกลุ่ม[158]

ซึ่งมีหลักกฎหมายเฉพาะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล Directive 95/46/EC หรือ Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of such Data เป็นกฎเกณฑ์ที่บัญญัติขึ้นโดยคณะกรรมาธิการยุโรป European Economic Community ใน ค.ศ. 1995 (พ.ศ. 2538) Directive นี้ถือเป็นหลักเกณฑ์ต้นแบบ (Model) อันเป็นที่มาของการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกต่าง ๆ ในยุโรป

Directive 95/46/EC มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในความเป็นอยู่ส่วนตัวอันเนื่องจากการประมวลผลข้อมูลส่วนบุคคลตามที่บัญญัติไว้อย่างชัดเจนในมาตราที่ 1 นอกจากนี้ อารัมภบทที่ 2 ยังได้อธิบายเพิ่มเติมว่า

---

[158] รองศาสตราจารย์คณาธิป ทองรวีวงศ์, “รายงานวิจัยฉบับสมบูรณ์ เรื่อง การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน The Personal Data Protection Law Reform for ASEAN,” น. 46.

“ระบบประมวลผลข้อมูลนั้นถูกออกแบบมาเพื่ออำนวยประโยชน์แก่มนุษย์... ระบบเหล่านี้ต้องเคารพสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยไม่เลือกสัญชาติหรือถิ่นที่อยู่ของบุคคลนั้นโดยเฉพาะสิทธิในความเป็นส่วนตัว”

หลักการที่สำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้นDirective 95/46/EC มีดังนี้

1. ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

2. ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (Specified, Explicit and Legitimate Purposes) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์สถิติ หรือวิทยาศาสตร์

3. ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (Adequate) ไม่มากเกินความจำเป็น (Not Excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

4. ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และในกรณีจำเป็นต้องเป็นปัจจุบันด้วย

5. ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของไว้นานเกินไปอีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนั้น ยังได้วางหลัก ข้อมูลชนิดที่มีความอ่อนไหว (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสม

นอกจากนี้ มีข้อบังคับ EU ใหม่เกี่ยวกับการปกป้องข้อมูลส่วนบุคคล

ในเดือนพฤษภาคม ค.ศ. 2016 (พ.ศ. 2559) สหภาพยุโรปได้ใช้ระเบียบใหม่ (EU) 2016/679 ในการปกป้องข้อมูลส่วนบุคคล Forum ผู้ป่วยชาวยุโรปได้สนับสนุนอย่างแข็งขันสำหรับวิธีการที่สมดุลเพื่อปกป้องความเป็นส่วนตัวของผู้ป่วยในขณะที่มั่นใจว่าข้อมูลของผู้ป่วยสามารถใช้ร่วมกันเพื่อวัตถุประสงค์ด้านการดูแลสุขภาพและการวิจัยตั้งแต่การเผยแพร่ข้อเสนอสำหรับกฎระเบียบในปี 2012 ได้รับข้อมูลที่ดีขึ้นเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของพวกเขาและให้ความรับผิดชอบที่ชัดเจนยิ่งขึ้นต่อบุคคลและองค์กรที่ใช้ข้อมูลส่วนบุคคล

จากการศึกษาสหภาพยุโรปมีหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ Directive 95/46/EC หรือ Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 (พ.ศ. 2538) on the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of such Data ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคลธรรมดา โดยเฉพาะอย่างยิ่งสิทธิในความเป็นอยู่ส่วนตัว และกำหนดหลักเกณฑ์ในการ

จัดเก็บข้อมูลส่วนบุคคลให้มีความปลอดภัย และวางหลักการคุ้มครองข้อมูลส่วนบุคคล ประเภทข้อมูลที่มีความอ่อนไหว (Sensitive Data) ซึ่งมีกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสม อีกทั้งมีข้อยกเว้นตามกฎหมายในมาตรา 26 (1) Directive 95/46/EC กำหนดให้สามารถโอนข้อมูลส่วนบุคคลได้หากเจ้าของข้อมูลยินยอมให้โอนข้อมูลได้ และมีหลักเกณฑ์การโอนระหว่างเจ้าของข้อมูลกับผู้ควบคุมประมวลข้อมูล และมีอนุสัญญาสิทธิมนุษยชนยุโรป (The European Convention on Human Rights หรือ ECHR) มาตรา 8 มีหลักว่า บุคคลทุกคนย่อมมีสิทธิได้รับความคุ้มครองความเป็นส่วนตัว โดยไม่สามารถถูกแทรกแซงได้แม้ว่าเป็นหน่วยงานของรัฐก็ตาม เว้นแต่เกี่ยวข้องกับประโยชน์ด้านความมั่นคงของรัฐ ความปลอดภัยสาธารณะเพื่อป้องกันอาชญากรรม เพื่อปกป้องสุขภาพหรือศีลธรรม หรือเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น

[159]ภายหลังสหภาพยุโรป ได้ออกกฎหมายฉบับใหม่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือที่เรียกกันว่า “GDPR” หรือ “General Data Protection Regulation” ซึ่งมีบังคับใช้เมื่อเดือนพฤษภาคม พ.ศ. 2561 โดยมีข้อกำหนดให้องค์กรต่าง ๆ ที่มีธุรกรรมหรือการดำเนินการบนอินเทอร์เน็ตที่มีข้อมูลส่วนบุคคลของผู้บริโภคต้องปฏิบัติตามมาตรการต่าง ๆ ที่เข้มงวดขึ้นเพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวของบุคคล ซึ่งเป็นการปรับปรุงกฎหมายเดิม (EU Data Protection Directive 95/46/EC) ซึ่งใช้บังคับมานานมากว่า 20 ปี ทำให้เกิดการเปลี่ยนแปลงหลักการที่สำคัญดังนี้

1) การกำหนดใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) เป็นข้อมูลส่วนบุคคลของสหภาพยุโรปอยู่ภายใต้ความคุ้มครองไม่ว่าจะอยู่ในที่ใดในโลก

2) กำหนดบทลงโทษสูงขึ้น โดยองค์กรที่กระทำผิดอาจต้องจ่ายค่าปรับสูงถึงอัตราร้อยละ 4ของผลประกอบการรายได้ทั่วโลก

3) กำหนดให้การขอความยินยอมจากเจ้าของข้อมูลต้องชัดเจนและชัดแจ้ง (Clear and Affirmative Consent)

4) กำหนดการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล โดยหน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และประชาชนทราบภายใน 72 ชั่วโมง

---

[159] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, “Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล,” โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, พิมพ์ครั้งที่ 1 (ธันวาคม 2563): น. 17 – 18.

5) กำหนดขอบเขตสิทธิของเจ้าของข้อมูล โดยให้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลจะถูกใช้อย่างไร เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

6) กำหนดรับรองสิทธิในการโอนข้อมูลไปยังผู้ประกอบการอื่น (Right to Data Portability) และ

7) กำหนดรับรองสิทธิที่จะถูกลืม (Right to be Forgotten) เจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้

4.2.2 สหพันธ์สาธารณรัฐเยอรมนี

การคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี อยู่ภายใต้บทบัญญัติของรัฐธรรมนูญเยอรมัน (German Constitution) ซึ่งเป็นกรอบการคุ้มครองที่สำคัญสำหรับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองโดยตรงจากบทบัญญัติของรัฐธรรมนูญ ซึ่งห้ามมิให้มีการเข้าไปแทรกแซงในสิทธิส่วนบุคคล และFederal Data Protection Act 2018 (พ.ศ. 2561) (BDSG) หรือรัฐบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (พ.ศ. 2561) ของรัฐบาลกลาง ซึ่งมีการทบทวนแก้ไขครั้งสุดท้ายในปี 2017 (พ.ศ. 2560) ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ โดยครอบคลุมถึงการเก็บรวบรวมการประมวลผล และการใช้ ซึ่งใช้บังคับกับทั้งภาครัฐและเอกชน ตามมาตรา 67 การประเมินผลกระทบต่อการคุ้มครองข้อมูล ในกรณีที่ประเภทของการประมวลผลโดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีใหม่และคำนึงถึงธรรมชาติขอบเขตบริบทและวัตถุประสงค์ของการประมวลผลมีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงอย่างมากต่อผลประโยชน์ที่ได้รับการคุ้มครองตามกฎหมาย นอกจากนี้ยังกำหนดให้มีเจ้าหน้าที่ซึ่งทำหน้าที่ผู้ควบคุมข้อมูลเพื่อรักษาประโยชน์ของเจ้าของข้อมูลและป้องกันความปลอดภัยแก่ข้อมูลไม่ให้บุคคลภายนอก กำหนดสิทธิของเจ้าของข้อมูลเพื่อป้องกันความปลอดภัยของข้อมูล และเพื่อไม่ให้ข้อมูลเกิดการสูญหาย

นอกจากนี้ Federal Data Protection Act 2018 (พ.ศ. 2561) (BDSG) ยังกำหนดให้หน่วยงานของรัฐต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล และหน่วยงานสาธารณะต้องเผยแพร่รายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลและแจ้งไปยังกรรมาธิการแห่งสหพันธรัฐเพื่อการปกป้องข้อมูลและเสรีภาพของข้อมูล (Federal Commissioner for Data Protection and Freedom of Information) และมีส่วนที่กำหนดบทลงโทษแก่ผู้กระทำความผิดในการดำเนินคดีอาญาหรือความรับผิดทางปกครอง และมาตรการเยียวยาแก่เจ้าของข้อมูลซึ่งได้รับความเสียหายจากการถูกกระทำละเมิดโดยเรียกค่าเสียหายทางแพ่งได้ตามกฎหมายฉบับนี้โดยตรง

4.2.3 เครือรัฐออสเตรเลีย

เครือรัฐออสเตรเลีย เป็นประเทศที่มีระบบทางด้านสุขภาพที่ดีแห่งหนึ่งของโลก มีพระราชบัญญัติบันทึกสุขภาพอิเล็กทรอนิกส์ที่ควบคุมด้วยตัวเอง ค.ศ. 2012 (พ.ศ. 2555) (Personally Controlled Electronic Health Records Act 2012 : PCEHR หรือ E-Health) ซึ่งระบบจะทำการรวมข้อมูลสรุปทางอิเล็กทรอนิกส์ซึ่งจัดทำโดยผู้ให้บริการด้านการดูแลสุขภาพที่ได้รับมอบหมายในการบันทึกข้อมูลของผู้รับบริการทางการแพทย์ โดยจะทำการสรุปข้อมูลเกี่ยวกับผู้รับบริการทางการแพทย์เป็นรายบุคคล ซึ่งมีเพียงผู้ได้รับมอบหมายในบันทึกข้อมูลทางแพทย์เท่านั้นที่สามารถจัดการแก้ไขข้อมูลในระบบได้ และ Personally Controlled Electronic Health Records Act 2012 (พ.ศ. 2555) และพระราชบัญญัติหลักความเป็นส่วนตัว ค.ศ. 1988 (พ.ศ. 2531) (Principles under the Privacy Act 1988) ซึ่งกำหนดวิธีการบันทึกข้อมูลลงใน E-Health โดยมีมาตรการรักษาความปลอดภัย รวมถึงการตรวจสอบว่ามีบุคคลใดเข้าถึงเวชระเบียนของผู้ป่วย ซึ่งจะมีการแจ้งวัน เวลา สถานที่ เข้าถึงข้อมูลนั้น นอกจากนี้ยังมาตรการอื่น ๆเพื่อความปลอดภัยในข้อมูลของผู้ป่วย เช่น การเข้ารหัสเช่นเดียวกับการเข้าสู่ระบบ และรหัสผ่านที่ปลอดภัย โดยบันทึกของผู้ป่วยจะถูกระบุโดยใช้รหัสสุขภาพส่วนบุคคล (IHI) ที่ได้รับจาก Medicare ซึ่งเป็นระบบการดูแลสุขภาพของเครือรัฐออสเตรเลียที่ให้บริการโรงพยาบาลการแพทย์ และต้องลงทะเบียนผู้ป่วยซึ่งจะต้องใช้หมายเลขของ Medicare และมีมาตรการเพื่อปกป้องข้อมูลส่วนบุคคลเพื่อไม่ให้ มีการเข้าถึงข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล และไม่สามารถนำข้อมูลส่วนบุคคลไปดัดแปลงหรือแก้ไข ประการใด ๆ ได้ ในส่วนของมาตรการความปลอดภัยนั้น สามารถให้ผู้ป่วยซึ่งเป็นเจ้าของข้อมูลตรวจสอบได้ว่ามีบุคคลใดเข้าถึงเวชระเบียนหรือไม่ พร้อมทั้งมีการบันทึกข้อมูลการเข้าระบบไว้ นอกจากนี้การจะเข้าสู่ระบบหรือฐานข้อมูลได้จะต้องมีรหัสผ่านเพื่อใช้สำหรับยืนยันตัวตน

4.2.4 สหราชอาณาจักร

สหราชอาณาจักรเป็นประเทศที่ใช้ระบบกฎหมายจารีตประเพณี (Common Law System) ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (พ.ศ. 2541) (The Data Protection Act of 1998) ขึ้นเป็นกฎหมายกลาง (Comprehensive Law) และให้มีความสอดคล้องกับกฎหมายข้อมูลส่วนบุคคลของยุโรป และเพื่อปรับปรุงกฎหมายคุ้มครองข้อมูลให้มีความทันสมัยมากขึ้น โดยบทบัญญัติของกฎหมายฉบับนี้ได้กำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (GDPR) ของสหราชอาณาจักร โดย The Data Protection Act of 1998 (พ.ศ. 2541) หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 ได้วางหลักหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ประการ ดังนี้

1) ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลอย่างยุติธรรมและชอบด้วยกฎหมาย และการประมวลผลดังกล่าวต้องสอดคล้องกับกฎที่เฉพาะเจาะลงอย่างน้อยหนึ่งกฎ (กฎเพิ่มเติมอาจปรับใช้กับข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง)

2) ข้อมูลส่วนบุคคลจะได้รับเมื่อวัตถุประสงค์ที่ระบุไว้โดยเฉพาะและถูกกฎหมายหนึ่งวัตถุประสงค์ หรือมากกว่า และจะไม่ถูกประมวลผลเพิ่มเติมในลักษณะใด ๆ ที่ขัดกับวัตถุประสงค์นั้นหรือวัตถุประสงค์อื่น ๆ

3) ข้อมูลส่วนบุคคลจะต้องเพียงพอ มีความสอดคล้อง และมีปริมาณที่สัมพันธ์กับวัตถุประสงค์ใด ๆ หรือหลายวัตถุประสงค์ในการประมวลผล

4) ข้อมูลส่วนบุคคลจะต้องถูกต้องและหากจำเป็นต้องมีการปรับปรุงให้ทันสมัยอยู่เสมอ

5) ข้อมูลส่วนบุคคลที่ประมวลผลเพื่อวัตถุประสงค์หรือวัตถุประสงค์ใด ๆ จะไม่ถูกเก็บไว้นานเกินความจำเป็นสำหรับวัตถุประสงค์นั้นหรือวัตถุประสงค์เหล่านั้น

6) ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างสอดคล้องกับสิทธิของเจ้าของข้อมูลตามพระราชบัญญัติเพื่อวัตถุประสงค์

7) มาตรการทางเทคนิคที่เหมาะสมถูกนำมาใช้คัดค้านการประมวลผลเจ้าของข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือผิดกฎหมาย และป้องกันการสูญหายหรือการทำลายและความเสียหายที่มีต่อข้อมูลส่วนบุคคล

8) ข้อมูลส่วนบุคคลจะไม่ถูกถ่ายโอนไปยังประเทศหรือดินแดนนอกเขตเศรษฐกิจยุโรป เว้นแต่ประเทศหรือดินแดนนั้นได้รับการคุ้มครองในระดับที่เพียงพอสำหรับสิทธิและเสรีภาพของเจ้าของข้อมูลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

นอกจากนี้ยังมีระบบมีการป้องกันโดยสหราชอาณาจักรของรัฐบาลเกตเวย์ซึ่งถูกสร้างขึ้นโดยบริษัทไมโครซอฟท์ โปรแกรมนี้เรียกว่า “การพัฒนาระเบียนอิเล็กทรอนิกส์และโปรแกรมการดำเนินการ (ERDIP)” และ The Clinical Record Interactive Search System (CRIS) หรือระบบค้นหาทางคลินิกบันทึกโต้ตอบซึ่งคอยจัดการลบข้อมูลจากเวชระเบียนอิเล็กทรอนิกส์ที่อาจระบุตัวบุคคล จากนั้นจะสร้างฐานข้อมูลที่ไม่ระบุตัวตนเพื่อใช้สำหรับการวิจัย เนื่องจากข้อมูลที่ไม่ระบุชื่อหรือไม่ระบุตัวตนจากเวชระเบียนมีประโยชน์มากสำหรับการวิจัย ข้อมูลจำนวนมากถูกบันทึกโดยสามารถบันทึกข้อมูลได้โดยไม่มีค่าใช้จ่าย เช่น องค์กร NHS Trust ต้องการพูดคุยกับผู้ป่วยโรคจิตเภทที่เป็นเพศหญิงและมีอายุระหว่าง 25 - 45 ปี ก็จะใช้ระบบ the Clinical Record Interactive Search System (CRIS) เพื่อค้นหาฐานข้อมูลที่ไม่ระบุตัวตนและค้นหาว่ามีกี่คนที่มีคุณสมบัติตรงตามเกณฑ์กำหนดไว้ซึ่งข้อมูลไม่ระบุตัวตนนี้จะมีการลบข้อมูลเพื่อปกป้องความเป็นส่วนตัวของ

ผู้ป่วย เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ ที่อยู่ และหมายเลข NHS จะถูกลบออกหรือปิดบังไว้ เพื่อลดโอกาสข้อมูลของผู้ป่วยจะถูกเปิดเผยได้

นอกจากนี้องค์กร National Health Service (NHS) ซึ่งเป็นผู้ดำเนินการ The Clinical Record Interactive Search System (CRIS) มีกระบวนที่เข้มงวดเพื่อให้สามารถควบคุมผู้เข้าถึงฐานข้อมูลได้ ซึ่งผู้เข้าใช้ระบบจะต้องลงทะเบียนก่อนเพื่อเข้าใช้ CRIS

ระบบการจัดเก็บข้อมูลทางการแพทย์ของผู้ป่วยที่สามารถแสดงข้อมูลได้อย่างเป็นปัจจุบันทันที แบบออกได้ ดังนี้

1) ระบบข้อมูลทางการแพทย์แบบผู้ป่วยเป็นรายวันค่อย ๆ เปลี่ยนข้อมูลเวชระเบียนที่เป็นเอกสารจำนวนมากและเพื่อเพิ่มความเร็วในการไหลเวียนของข้อมูลทั่วทั้งบริการสุขภาพ

2) ระบบจัดเก็บข้อมูลระยะยาวที่สนับสนุนเวชระเบียนผู้ป่วยตลอดชีวิตและเชื่อมต่อกับการรักษาพยาบาลทุกรูปแบบ

4.2.5 สหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศที่ใช้รูปแบบการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลแบบกฎหมายเฉพาะเรื่อง (Sectoral Law) ซึ่งทำให้สามารถกำหนดมาตรการทางกฎหมายให้มีความเหมาะสม และเป็นการเฉพาะได้ โดยกฎหมายสำคัญที่ให้ความคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ซึ่งมีกฎหมายสำคัญ คือ รัฐบัญญัติประกันสุขภาพพกพาและรัฐบัญญัติความรับผิดชอบ ค.ศ. 1996 (พ.ศ. 2539) (Health Insurance Portability and Accountability Act of 1996 : HIPAA) ซึ่งเป็นกฎหมายของรัฐบาลกลางที่กำหนดให้มีการสร้างมาตรฐานระดับชาติเพื่อปกป้องข้อมูลด้านสุขภาพของผู้ป่วยซึ่งมีความอ่อนไหวจากการเปิดเผยโดยไม่ได้รับความยินยอมจากผู้ป่วย นอกจากนี้ได้วางหลักมาตรฐานของความเป็นส่วนตัวทางการแพทย์ของผู้ป่วย แพทย์ และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับข้อมูลทางการแพทย์ รวมถึงการรักษาข้อมูลส่วนบุคคล รวมทั้งการเปิดเผยข้อมูล ทั้งการกำหนดบทลงโทษในกรณีที่มีการกระทำความผิดทั้งในทางแพ่งและทางอาญากรณีการกระทำความผิดละเมิดข้อมูลส่วนบุคคล

จากการศึกษา รัฐบัญญัติประกันสุขภาพพกพาและรัฐบัญญัติความรับผิดชอบ ค.ศ. 1996 (พ.ศ. 2539) (Health Insurance Portability and Accountability Act of 1996 : HIPAA) เป็นกฎหมายของรัฐบาลกลางที่กำหนดให้มีการสร้างมาตรฐานระดับชาติเพื่อปกป้องข้อมูลด้านสุขภาพของผู้ป่วยที่มีความอ่อนไหวจากการเปิดเผยโดยไม่ได้รับความยินยอมจากผู้ป่วย

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

วิทยานิพนธ์เล่มนี้ ได้ทำการศึกษาและวิเคราะห์ปัญหาทางกฎหมายที่เกี่ยวกับความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย ซึ่งปัจจุบันความก้าวหน้าทางด้านเทคโนโลยีมีความก้าวหน้าเป็นอย่างมาก และถูกนำมาใช้ในธุรกรรมด้านต่าง ๆ ซึ่งรวมถึงด้านการแพทย์และสาธารณสุข โดยประเทศไทยในปัจจุบัน เมื่อเปรียบเทียบกับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศคือ สหภาพยุโรป สหพันธ์สาธารณรัฐเยอรมัน เครือรัฐออสเตรเลีย สหราชณาจักร สหรัฐอเมริกา

ข้อมูลส่วนบุคคลของผู้ป่วย ซึ่งรับบริการทางสาธารณสุข หรือการรับบริการด้านการแพทย์และสาธารณสุขที่ให้โดยตรงแก่บุคคลเพื่อการสร้างเสริมสุขภาพ การป้องกันโรค การตรวจวินิจฉัยโรค การรักษาพยาบาลและการฟื้นฟูสมรรถภาพ ที่จำเป็นต่อสุขภาพและการดำรงชีวิต ทั้งนี้ให้รวมถึงการบริการการแพทย์แผนไทยและการแพทย์ทางเลือกตามกฎหมายว่าด้วยการประกอบโรคศิลปะ ซึ่งผู้เข้ารับบริการหรือผู้ป่วยจะให้ข้อมูลแก่เจ้าหน้าที่โรงพยาบาล เพื่อการขึ้นทะเบียนผู้ป่วยโดยเจ้าหน้าที่โรงพยาบาลจะทำการซักประวัติของผู้ป่วย เพื่อให้ได้เรื่องราวความเจ็บป่วยของผู้ป่วย โดยมีประวัติที่จำเป็นต้องซักถามกับผู้ป่วย ได้แก่ ข้อมูลส่วนตัว อาการสำคัญ ประวัติการเจ็บป่วย ในปัจจุบัน ประวัติการเจ็บป่วยในอดีต ประวัติครอบครัว ซึ่งเป็นประโยชน์ต่อการวินิจฉัยของแพทย์ และการวางแผนการรักษาของแพทย์ โดยข้อมูลดังกล่าวนั้น เป็นข้อมูลด้านสุขภาพของบุคคล ซึ่งไม่สามารถนำไปเปิดเผยอันเป็นประการที่น่าจะทำให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับความเสียหายไม่ได้ เว้นแต่การเปิดเผยของข้อมูลนั้นเป็นไปตามความประสงค์ของบุคคลผู้เป็นเจ้าของข้อมูลโดยตรง แต่ปัญหาสำคัญประการหนึ่งของการปกป้องข้อมูลในรูปแบบอิเล็กทรอนิกส์ คือ ภัยคุกคามด้านความปลอดภัย (Security) ที่มีความเสี่ยงต่อข้อมูลของผู้ป่วยทั้งทางด้านสุขภาพ ชื่อเสียง และทรัพย์สิน ซึ่งเป็นอันตรายต่อข้อมูลที่ถูกบันทึกและเก็บรักษาไว้

เทคโนโลยีการสื่อสารทางการแพทย์มีความสนใจเป็นอย่างมาก เพราะความก้าวหน้าของเทคโนโลยีในปัจจุบันที่มีมากยิ่งขึ้นซึ่งถูกนำมาใช้ในธุรกรรมด้านต่าง ๆ รวมถึงด้านการแพทย์และสาธารณสุข ทางด้านการรักษา ฟื้นฟูสุขภาพของผู้ป่วย รวมถึงการบันทึกและจัดเก็บข้อมูลส่วนบุคคลของผู้ป่วยซึ่งเข้ารับบริการทางการแพทย์ในรูปแบบเวชระเบียนอิเล็กทรอนิกส์ (Electronic

Medical Record – EMR) ซึ่งหมายรวมถึงการให้ความสำคัญเรื่องข้อมูลส่วนบุคคลของผู้ป่วยที่เข้ารับการใช้บริการในสถานพยาบาล การให้ความคุ้มครองในข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพจึงเป็นเรื่องมีความสำคัญเป็นอย่างยิ่งเป็นอันดับต้น ๆ หน่วยงาน หรือองค์กรที่มีความเกี่ยวข้องกับการจัดเก็บ เก็บรักษาข้อมูลส่วนบุคคลไม่ให้รั่วไหล หรือถูกบุคคลภายนอกเข้าถึงข้อมูลที่ไม่สามารถเปิดเผยได้ ซึ่งในปัจจุบันประเทศไทยได้ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล และการคุ้มครองข้อมูลส่วนบุคคลเพื่อมิให้ผู้ที่เข้ารับบริการทางการแพทย์ ซึ่งได้แจ้งข้อมูลแก่ไว้กับสถานพยาบาลในระบบเวชระเบียนอิเล็กทรอนิกส์ จึงมีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ จากการศึกษาพบว่ามีกฎหมายหลายฉบับที่เกี่ยวข้องด้วยแต่สามารถอ้างอิงได้เพียงบางส่วน และยังไม่ครอบคลุมกรณีความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์ ดังนี้

จากการศึกษาพบว่า รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 หมวด 3 มาตรา 32 ได้มีการบัญญัติ การให้ความคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดแจ้งก็ตาม แต่เป็นลักษณะการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับกว้าง เพื่อให้ประชาชนทุกคนในประเทศได้รับความคุ้มครองให้สิทธิที่พึงมีพึงได้เป็นการทั่วไป เนื่องจากไม่มีบทบัญญัติให้ความคุ้มครองในลักษณะเป็นการเฉพาะและมีรายละเอียดของหลักเกณฑ์หรือมาตรการต่าง ๆ ไว้ในรัฐธรรมนูญได้ นอกจากนี้เพียงบทบัญญัติในรัฐธรรมนูญเพียงอย่างเดียวก็ไม่อาจให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยได้อย่างเพียงพอ ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและมีผลในการปฏิบัติ จึงควรมีการกำหนดมาตรการและรายละเอียดในการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ เพื่อให้ประชาชนที่เข้ารับบริการทางการแพทย์ ไม่ว่าในรูปแบบผู้ป่วยนอกหรือผู้ป่วยในก็ตามผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลที่เกี่ยวข้องกับการจัดเก็บข้อมูล และกำหนดหน่วยงานที่รับผิดชอบ จึงจะทำให้การคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์มีความปลอดภัยในข้อมูลส่วนบุคคลของผู้ป่วยมากยิ่งขึ้น

จึงเห็นได้ว่า แม้รัฐธรรมนูญแห่งราชอาณาจักรไทยได้มีการบัญญัติการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดแจ้งก้ตาม แต่เป็นลักษณะการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับกว้าง เพื่อให้ประชาชนทุกคนในประเทศได้รับความคุ้มครองให้สิทธิที่พึงมีพึงได้เป็นการทั่วไป เนื่องจากการมีบทบัญญัติความคุ้มครองในลักษณะเป็นการเฉพาะและมีรายละเอียดของหลักเกณฑ์หรือมาตรการต่าง ๆ ไว้ในรัฐธรรมนูญได้ นอกจากนี้เพียงบทบัญญัติในรัฐธรรมนูญเพียงอย่างเดียวก็ไม่อาจให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยได้อย่างเพียงพอ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมุ่งเน้นความสำคัญไปที่องค์กร หน่วยงาน หรือนิติบุคคล เพื่อให้มีมาตรฐานในการจัดการข้อมูลส่วนบุคคลอย่างมีความเหมาะสม

และเพียงพอ ซึ่งมีความคุ้มครองข้อมูลส่วนบุคคลโดยมั่งเน้นว่า เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น อีกนัยหนึ่งคือการเปิดเผยข้อมูลหรือกระทำการอย่างใด ๆ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน และผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ซึ่งไม่เกี่ยวข้องกับข้อมูล แต่อย่างไรก็ตามยังมีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ซึ่งได้กำหนดเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้มีความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งต้องครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) ซึ่งในปัจจุบันนี้มีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางหมวด เป็นระยะเวลา 1 ปี จนถึงวันที่ 31 พฤษภาคม 2564 โดยในหมวดที่ยกเว้นดังกล่าวนั้น ยกเว้นกิจการด้านการแพทย์และสาธารณสุข ซึ่งส่งผลให้ข้อมูลส่วนบุคคลของผู้ป่วยซึ่งใช้บริการทางแพทย์ อาจไม่ได้รับความคุ้มครองข้อมูลส่วนบุคคลที่ให้ไว้แก่โรงพยาบาล

ในส่วนของความรับผิดที่ข้อมูลส่วนบุคคลของผู้ป่วยถูกแทรกแซง จนทำให้เสียหายไม่ว่าต่อร่างกาย สิทธิ หรือทรัพย์สินก็ตาม โดยนำพระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2534 และมาตรา 420 แห่งประมวลกฎหมายแพ่งและพาณิชย์มาใช้ในพิจารณาความรับผิด และนำหลักเกณฑ์ของต่างประเทศ ซึ่งมีหน่วยงานเป็นการเฉพาะในการดูแลข้อมูลในเวชระเบียนอิเล็กทรอนิกส์ และมีการบันทึกข้อมูลการเข้าสู่ระบบ และตรวจสอบการเข้าสู่ระบบอิเล็กทรอนิกส์

จากการศึกษาวิเคราะห์ระหว่างกฎหมายของประเทศไทยเปรียบเทียบกับกฎหมายต่างประเทศ เช่น สหภาพยุโรป สหพันธ์สาธารณรัฐเยอรมนี เครือรัฐออสเตรเลีย สหราชอาณาจักร และสหรัฐอเมริกา เห็นว่า ประเทศไทยมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการป้องกันข้อมูลส่วนบุคคล แต่อย่างไรก็ตามกฎหมายเหล่านั้นมิได้ครอบคลุมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยที่ได้บันทึกไว้ในเวชระเบียนอิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับกฎหมายของสหภาพยุโรป สหพันธ์สาธารณรัฐเยอรมนี เครือรัฐออสเตรเลีย สหราชณาจักร และสหรัฐอเมริกา ผู้ศึกษาเห็นว่ามีกฎหมายที่เป็นการป้องกันข้อมูลส่วนบุคคลของผู้ป่วยซึ่งถูกบันทึกและจัดเก็บไว้ในรูปแบบ

อิเล็กทรอนิกส์ การกำหนดผู้ควบคุมข้อมูลและหน่วยงานที่รับผิดชอบในการดูแลความปลอดภัยในข้อมูลส่วนบุคคลของผู้ป่วย ทั้งมีการกำหนดโทษและความรับผิดแก่ผู้กระทำผิดซึ่งละเมิดข้อมูลส่วนบุคคลของผู้ป่วย ทั้งในทางอาญา และมาตรการเยียวยาความเสียหายในทางแพ่ง อันเป็นการให้ความเชื่อมั่นและความปลอดภัยแก่ผู้ป่วยซึ่งเป็นเจ้าของข้อมูล

5.2 ข้อเสนอแนะ

จากบทสรุปข้างต้น ผู้วิจัยจึงเห็นควรว่ามาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์ ปัจจุบันประเทศไทยมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการป้องกันข้อมูลส่วนบุคคล แต่มิได้ครอบคลุมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยที่ได้บันทึกไว้ในเวชระเบียนอิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับกฎหมายของสหภาพยุโรป สหพันธ์สาธารณรัฐเยอรมนี เครือรัฐออสเตรเลีย สหราชณาจักร และสหรัฐอเมริกา ผู้ศึกษาเห็นว่ามีกฎหมายที่เป็นการป้องกันข้อมูลส่วนบุคคลของผู้ป่วยซึ่งถูกบันทึกและจัดเก็บไว้ในรูปแบบอิเล็กทรอนิกส์เป็นการเฉพาะ การกำหนดผู้ควบคุมข้อมูลและหน่วยงานที่รับผิดชอบในการดูแลความปลอดภัยในข้อมูลส่วนบุคคลของผู้ป่วย ทั้งมีการกำหนดโทษและความรับผิดแก่ผู้กระทำผิดซึ่งละเมิดข้อมูลส่วนบุคคลของผู้ป่วย ทั้งในทางอาญา และมาตรการเยียวยาความเสียหายในทางแพ่ง อันเป็นการให้ความเชื่อมั่นและความปลอดภัยแก่ผู้ป่วยซึ่งเป็นเจ้าของข้อมูล เพื่อเป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย ควรนำหลักการและกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลของผู้ป่วยในต่างประเทศมาเป็นแนวทางในการบัญญัติหรือปรับปรุงกฎหมายของประเทศไทย เพื่อให้ประเทศไทยมีหลักเกณฑ์ในกรณีดังกล่าวอย่างเป็นสากลและมีมาตรฐาน ซึ่งช่วยสร้างความปลอดภัยในการเก็บรักษา หรือคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย ซึ่งจะเป็นประโยชน์ทางด้านการแพทย์และต่อสังในอนาคต จึงมีข้อเสนอดังนี้

1. ควรมีการบัญญัติกฎหมายที่เกี่ยวกับเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย เพื่อเป็นการสร้างหลักประกันและความมั่นใจให้แก่ผู้มารับบริการทางแพทย์และเพื่อป้องกันไม่ให้ข้อมูลของผู้ป่วยถูกเข้าถึงโดยบุคคลอื่นซึ่งไม่ใช่เจ้าของข้อมูล

2. เพื่อให้กฎหมายมีประสิทธิภาพมากยิ่งขึ้น เห็นควรว่า จำเป็นต้องมีการกำหนดการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยไว้โดยชัดแจ้ง ซึ่งเห็นว่าควรกำหนดหลักเกณฑ์ โดยอาศัยแนวทางของกฎหมายต่างประเทศ

3. มีหลักเกณฑ์ในการพิจารณาความรับผิด กรณีข้อมูลส่วนบุคคลของผู้ป่วยถูกแทรกแซงและได้รับความเสียหาย และกำหนดโทษและความรับผิดทางแพ่งและทางอาญา

4. กำหนดให้มีเจ้าหน้าที่และหน่วยงานที่รับผิดชอบในการป้องกันข้อมูลส่วนบุคคลของผู้ป่วยในเวชระเบียนอิเล็กทรอนิกส์ เพื่อความปลอดภัยของผู้ป่วย

5. แก้ไขปรับปรุงกฎหมายอื่น ๆ ที่เกี่ยวข้องให้มีความสอดคล้องกัน

นอกจากนี้ จากที่ผู้ศึกษาได้ทำการศึกษาค้นคว้าวิจัยมาตรการทางกฎหมายเกี่ยวกับการควบคุมเทคโนโลยีการสื่อสารทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย เห็นว่าพระราชบัญญัติข้อมูลส่วนบุคคล ยังคงมีปัญหาที่น่าศึกษาค้นคว้า 4 ประเด็น ดังนี้

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ไม่ได้มีความคุ้มครองในเวชระเบียนข้อมูลส่วนบุคคลของผู้ป่วย

2. บทบาทของแพทยสภา ในการกำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลของผู้ป่วย

3. ผู้ป่วยเป็นผู้กระทำความผิดอาญาซึ่งอยู่ในเขตอำนาจของศาลไทย กรณีการฝากขังพนักงานสอบสวนมีสิทธิเข้าถึงข้อมูลส่วนบุคคลทางการแพทย์เพื่อลดวันฝากขัง

4. การพิจารณาพักโทษแก่ผู้กระทำความผิด กรณีเป็นผู้ป่วยติดเตียง

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ. “ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน Universal Declaration of Human Rights.” (กรกฎาคม 2551).

กองควบคุมเครื่องมือแพทย์ สำนักงานคณะกรรมการอาหารและยา กระทรวงสาธารณสุข. “หน้าที่ของผู้ประกอบการด้านเครื่องมือแพทย์ ตามพระราชบัญญัติเครื่องมือแพทย์ พ.ศ. 2551. พิมพ์ครั้งที่ 1 : โรงพิมพ์ชุมนุมสหกรณ์การเกษตรแห่งประเทศไทย.” (กันยายน 2555).

กันต์ธนัท รัถยาภานิธิชัยกุล. “Biomedical อุปกรณ์ทางการแพทย์” การกำกับดูแลเครื่องแพทย์ในประเทศไทย.” http://www2.fda.moph.go.th/consumer/ism/ismmenu.asp

คณะอนุกรรมการความปลอดภัยทางรังสี มหาวิทยาลัยมหิดล. แนวปฏิบัติเพื่อความปลอดภัยทางรังสี มหาวิทยาลัยมหิดล Mahidol University Radiation Safety Guidelines. พิมพ์ครั้งที่ 1. ทองสุขพริ้นท์, (กุมภาพันธ์ 2555).

“คอลัมน์ อินโนสเปซ โดย บัซซี่บล็อก หนังสือพิมพ์ คมชัดลึก ฉบับวันที่ 11-12 พฤษภาคม 2562.” https://www.komchadluek.net/news/lifestyle/371309.

ดร.สุธี อยู่สถาพร. “ความรับผิดตามกฎหมายของแพทย์ในการรักษาผู้ป่วยกับหลักวิธีปฏิบัติเพื่อเป็นเลิศทางการแพทย์.” Public Health & Health Laws Journal Vol. 1 January - April 2016.

ดาวัลย์ ขาวสนิท. “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีด้านการเงินการธนาคารพาณิชย์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2561.

นคร เสรีรักษ์. การคุ้มครองข้อมูล : ประสบการเยอรมัน. ม.ป.ท: ม.ป.ท, ม.ป.ป.

นายบรรหาร กำลา นิติกร 3 กลุ่มงานพัฒนากฎหมาย. สรุปสัมมนาทางวิชาการ เรื่อง การคุ้มครองข้อมูลส่วนบุคคล. ม.ป.ท: ม.ป.ท, ม.ป.ป.

นายสาธิต นฤภัย. คู่มือความปลอดภัยในการใช้เครื่องมือและอุปกรณ์ทางการแพทย์ประเภทต่าง ๆ ในโรงพยาบาล พ.ศ. 2550. ม.ป.ท: ม.ป.ท, ม.ป.ป.

พญ.กัลยา ตีระวัฒนานนท์, พญ.ธัญญรัตน์ อโนทัยสินทวี. รายงานฉบับสมบูรณ์สรุปเนื้อหาการประชุมนานาชาติเรื่องเครื่องมือแพทย์ ครั้งที่ 1. พิมพ์ครั้งที่ 1. นนทบุรี : บริษัท เดอะ กราฟิโก ซิสเต็มส์ จำกัด, ม.ป.ป.

รศ.ดร.ศรุดา สมพอง. การบริหารงานสาธารณสุข. พิมพ์ครั้งที่ 1(ฉบับปรับปรุงใหม่). กรุงเทพมหานคร : สำนักพิมพ์มหาวิทยาลัยรามคำแหง, 2558.

รองศาสตรจารย์ นายแพทย์สิทธิพร ศรีนวลนัต. “หลักสิทธิมนุษยชนกับการรักษาผู้ป่วย.” หลักสูตรหลักนิติธรรมเพื่อประชาธิปไตย รุ่นที่ 5 วิทยาลัยศาลรัฐธรรมนูญ สำนักงานศาลรัฐธรรมนูญ. ม.ป.ท: ม.ป.ท, ม.ป.ป.

ศุภากร ด่านถาวรเจริญ. บริษัท Superb Quality Services Co., Ltd. มาทำความรู้จักกับมาตรฐานเครื่องมือแพทย์ (Medical Devices). ม.ป.ท: ม.ป.ท, ม.ป.ป.

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย. พิมพ์ครั้งที่ 1 ตุลาคม 2562.

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย. พิมพ์ครั้งที่ 1 ธันวาคม 2563.

“สยามมีเดีย SIAM MEDIA NEWSPAPER.” http://live.siammedia.org/index.php/article/chit-chat-health/12932

“สรุปใจความสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ผู้ประกอบการควรรู้.” https://www.acinfotec.com/2019/07/23/data-protection-law-2562/

สโรชิณี กลิ่นหอม. “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์.” วิทยานิพนธ์ คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, ม.ป.ป.

สำนักงานนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข. “คู่มือคำแนะนำการบันทึกเวชระเบียนสำหรับแพทย์.” สำนักงานกิจการโรงพพิมพ์องค์การสงเคราะห์ทหารผ่านศึก. พิมพ์ครั้งที่ 1 สิงหาคม 2555.

สัญญา วิริยะอมร พันธุ์. “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกิจอิเล็กทรอนิกส์ของภาครัฐ.” สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2554.

“หมอชาวบ้าน.” https://www.doctor.or.th/

องค์กรวิชาชีพด้านสุขภาพ แพทยสภา สภาการพยาบาล สภาเภสัชกรรม ทันตแพทยสภา สภากายภาพบาบัด สภาเทคนิคการแพทย์ และคณะกรรมการการประกอบโรคศิลปะ. คำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย. (12 สิงหาคม 2558).

ภาษาต่างประเทศ

AMNESTY INTERTIONAL THAILAND. “ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน.” https://www.amnesty.or.th/our-work/hre/udhr/

Acinfotec. website https://www.acinfotec.com/2019/07/23/data-protection-law-2562.

B. E. Jones and M. A. Ould King's College Hospital Computer Centre, 97 Denmark Hill. London Development of medical device policies WHO Medical device technical series

“DHSS News.” website http:// www.medicalhub.org

EPF European Patients Forum. The new EU Regulation on the protection of personal data: what does it mean for patients? A guide for patients and patients’ organisations. p.13 – 16.

WEED. L. L. Medical records. Medical education, and patient care: the problem-oriented record as a basic tool. Cleveland. Ohio : Case Western Reserve University Press, 1971.

National E-Health Strategy SUMMARY December 2008. “Australian Health Ministers,” Conference, website www.ahmac.gov.au

ภาคผนวก

ภาคผนวก ก

Directive 95/46/EC of the European parliament and of the council of 24 October1995 (2538)

Directive 95/46/EC of the European parliament and of the council of 24 October 1995 (2538)

อารัมภบทที่ (1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

อารัมภบทที่ (2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

อารัมภบทที่ (10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1 . This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

ภาคผนวก ข

Federal Data Protection Act (BDSG) 2018 (พ.ศ. 2561)

Federal Data Protection Act (BDSG) 2018 (พ.ศ. 2561)

Section 3

Processing of personal data by public bodies

Public bodies shall be permitted to process personal data if such processing is necessary to perform the task for which the controller is responsible or to exercise official authority which has been vested in the controller.

Chapter 3

Data protection officers of public bodies

Section 5

Designation

(1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Section 2 (5) which take part in competition.

(2) A single data protection officer may be designated for several public bodies, taking account of their organizational structure and size.

(3) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Section 7.

(4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

(5) The public body shall publish the contact details of the data protection officer and communicate them to the Federal Commissioner for Data Protection and Freedom of Information.

Section 6

Position

(1) The public body shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The public body shall support the data protection officer in performing the tasks referred to in Section 7 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The public body shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall directly report to the highest management level of the public body. The data protection officer shall not be dismissed or penalized by the public body for performing his or her tasks.

(4) The dismissal of the data protection officer shall be permitted only by applying Section 626 of the Civil Code accordingly. The data protection officer's employment shall not be terminated unless there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the public body has just cause to terminate without notice.

(5) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under Regulation (EU) 2016/679, this Act and other data protection legislation. The data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject.

(6) Where in the course of their activities data protection officers become aware of data for which the head of a public body or a person employed by such a body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and his or her assistants. The person to whom the right to refuse to give evidence applies for employment-related reasons shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable future. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Section 7

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection officer shall have at least the following tasks:

1. to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680;

2. to monitor compliance with this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3. to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Section 67 of this Act;

4. to cooperate with the supervisory authority;

5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Section 69 of this Act, and to consult, where appropriate, with regard to any other matter.

In the case of a data protection officer ordered by a court, these tasks shall not refer to the action of the court acting in its judicial capacity.

(2) The data protection officer may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

(3) The data protection officer shall in the performance of his or her tasks give due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Part 2

Implementing provisions for processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679

Chapter 1

Legal basis for processing personal data

Sub-chapter 1

Processing of special categories of personal data and processing for other purposes

Section 22

Processing of special categories of personal data

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

1. by public and private bodies if

a) processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations;

b) processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision;

c) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with; or

d) processing is urgently necessary for reasons of substantial public interest;

2. by public bodies if

a) processing is necessary to prevent a substantial threat to public security;

b) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or

c) processing is necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures;

and as far as the interests of the controller in data processing in the cases of no. 1 (d) and no. 2 outweigh the interests of the data subject.

(2) In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;

2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;

3. measures to increase awareness of staff involved in processing operations;

4. designation of a data protection officer;

5. restrictions on access to personal data within the controller and by processors;

6. the pseudonymization of personal data;

7. the encryption of personal data;

8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;

9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Chapter 2

Rights of the data subject

Section 32

Information to be provided where personal data are collected from the data subject

(1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use

1. concerns the further processing of data stored in analogue form, for which the controller directly contacts the data subject through the further processing; the purpose is compatible with the original purpose for which the data were collected in accordance with Regulation (EU) 2016/679; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the information can be regarded as minimal, given the circumstances of the individual case, in particular with regard to the context in which the data were collected;

2. would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;

3. would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a Land, and the controller's interests in not providing the information outweigh the interests of the data subject;

4. would interfere with the establishment, exercise or defence of legal claims, and the controller's interests in not providing the information outweigh the interests of the data subject; or

5. would endanger a confidential transfer of data to public bodies.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 13 (1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing

information. The first and second sentences shall not apply in the cases of subsection 1 nos. 4 and 5.

(3) If notification is not provided in the cases of subsection 1 because of a temporary obstacle, the controller shall meet the obligation to provide information, while taking into account the specific circumstances of processing, within an appropriate period after the obstacle has ceased to exist, but no later than two weeks.

Chapter 5

Penalties

Section 41

Application of provisions concerning criminal proceedings and proceedings to impose administrative fines

(1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 17, 35 and 36 of the Administrative Offences Act shall not apply. Section 68 of the Administrative Offences Act shall apply on the condition that the regional court shall decide if the administrative fine exceeds the amount of one hundred thousand euros.

(2) Unless this Act provides otherwise, the provisions of the Administrative Offences Act and the general laws on criminal procedures, namely the Code of Criminal Procedure and the Judicature Act, shall apply accordingly in proceedings for violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 56 to 58, 87, 88, 99 and 100 of the Administrative Offences Act shall not apply. Section 69 (4), second sentence of the Administrative Offences Act shall apply on the condition that the public prosecutor's office may stop the proceedings only with the approval of the supervisory authority which issued the administrative decision imposing a fine.

Section 42

Penal provisions

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. transferring the data to a third party or
2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or
2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal proceedings against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

Section 43

Provisions on administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offence:

1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

(3) Authorities and other public bodies as referred to in Section 2 (1) shall not be subject to any administrative fines.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

Chapter 6

Legal remedies

Section 44

Proceedings against a controller or processor

(1) Proceedings against a controller or a processor for a violation of data protection law within the scope of Regulation (EU) 2016/679 or the rights of the data subject contained therein may be brought by a data subject before the court in the place where the controller or processor has an establishment. Proceedings pursuant to the first sentence may also be brought before the court in the place where the data subject has his or her habitual residence.

(2) Subsection 1 shall not apply to proceedings against public authorities acting in the exercise of their sovereign powers.

(3) If the controller or processor has designated a representative pursuant to Article 27 (1) of Regulation (EU) 2016/679, this representative shall also be an authorized recipient in civil law proceedings pursuant to subsection 1. Section 184 of the Code of Civil Procedure shall remain unaffected.

Section 46

Definitions

For the purposes of this Act

1. ‘personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymization’ means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

7. ‘controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. ‘recipient’ means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or other law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed;

11. ‘genetic data’ means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

12. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, in particular facial images or dactyloscopic data;

13. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

14. ‘special categories of personal data’

a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

b) genetic data;

c) biometric data for the purpose of uniquely identifying a natural person;

d) data concerning health; and

e) data concerning a natural person’s sex life or sexual orientation;

15. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;

16. ‘international organization’ means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

17. ‘consent’ means any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Section 47

General principles for processing personal data

Personal data shall be

1. processed lawfully and fairly;

2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

3. adequate, relevant and not excessive in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Chapter 2

Legal basis for processing personal data

Section 48

Processing of special categories of personal data

(1) The processing of special categories of personal data shall be allowed only where strictly necessary for the performance of the controller's tasks.

(2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safeguards may be in particular

1. specific requirements for data security or data protection monitoring;
2. special time limits within which data must be reviewed for relevance and erasure;
3. measures to increase awareness of staff involved in processing operations;
4. restrictions on access to personal data within the controller;
5. separate processing of such data;
6. the pseudonymization of personal data;
7. the encryption of personal data; or
8. specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Section 51

Consent

(1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject's consent.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.

(4) Consent shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account. The data subject shall be informed of the intended purpose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

(5) If special categories of personal data are to be processed, the consent must explicitly refer to these data.

Section 53

Confidentiality

Persons employed in data processing shall not process personal data without authorization (confidentiality). They shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Chapter 3

Rights of the data subject

Section 55

General information on data processing

The controller shall provide general and publicly accessible information on

1. the purposes of the processing,
2. the rights of data subjects with regard to the processing of their personal data to access, rectification, erasure and restriction of processing,
3. the names and contact details of the controller and the data protection officer,
4. the right to lodge a complaint with the Federal Commissioner, and
5. the contact details of the Federal Commissioner

Section 57

Right of access

(1) The controller shall inform data subjects on request whether data concerning them are being processed. Data subjects shall also have the right to information about

1. the personal data being processed and the categories to which they belong;
2. the available information on the origin of the data;
3. the purposes of and legal basis for the processing;
4. the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organizations;
5. the period for which the data will be stored, or if that is not possible, the criteria used to determine that period;
6. the existence of the right to rectification or erasure of data or restriction of processing of data by the controller;
7. the right pursuant to Section 60 to lodge a complaint with the Federal Commissioner, and
8. the contact details of the Federal Commissioner.

(2) Subsection 1 shall not apply to personal data recorded only because they may not be erased due to legal or statutory provisions on retention, or only for purposes of monitoring data protection or safeguarding data, if providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

(3) No information shall be provided if the data subject does not provide information enabling the data to be located and if the effort required is therefore disproportionate to the data subject's interest in the information.

(4) Subject to the conditions of Section 56 (2), the controller may dispense with the provision of information pursuant to subsection 1, first sentence, or restrict, wholly or partly, the provision of information pursuant to subsection 1, second sentence.

(5) If the information to be provided relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other

authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

(6) The controller shall notify the data subject, without delay, in writing of any refusal or restriction of access. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The notification pursuant to the first sentence shall include the reasons for the refusal or the restriction unless providing the reasons would undermine the intended purpose of the refusal or restriction of access.

(7) If the data subject is notified pursuant to subsection 6 of the refusal or restriction of access, he or she may exercise his or her right of access also via the Federal Commissioner. The controller shall inform the data subject of this possibility and that, in accordance with Section 60, the data subject may lodge a complaint with the Federal Commissioner or seek a judicial remedy. If the data subject exercises his or her right pursuant to the first sentence, the information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would threaten the security of the Federation or a Land. The Federal Commissioner shall at least inform the data subject that all necessary checks have been conducted or that the Federal Commissioner has conducted a review. This notification may include information as to whether violations of data protection law were found. The notification from the Federal Commissioner to the data subject shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information. The controller may refuse to such provision only as far as and for as long as he or she could dispense with or restrict information pursuant to subsection 4. The Federal Commissioner shall also inform the data subject of his or her right to seek a judicial remedy.

(8) The controller shall document the factual or legal reasons on which the decision is based.

Section 66

Notifying data subjects affected by a personal data breach

(1) If a personal data breach is likely to result in a substantial risk to the legally protected interests of natural persons, the controller shall notify the data subject of the personal data breach without delay.

(2) The notification of the data subject pursuant to subsection 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Section 65 (3) nos. 2 to 4.

(3) Notification shall not be required if any of the following conditions are met:

1. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access them, such as encryption;

2. the controller has taken subsequent measures which ensure that the substantial risk referred to in subsection 1 is no longer likely to exist;

3. it would involve a disproportionate effort; in this case, a public communication shall be made or a similar measure taken to inform the data subjects in an equally effective manner.

(4) If the controller has not informed the data subjects of a personal data breach, the Federal Commissioner may formally determine that, in his or her opinion, the conditions referred to in subsection 3 have not been met. In doing so, the Federal Commissioner shall consider the likelihood of the personal data breach resulting in a high risk as referred to in subsection 1.

(5) The notification of data subjects pursuant to subsection 1 may be delayed, restricted or omitted under the conditions referred to in Section 56 (2) unless the interests of the data subjects outweigh those of the controller owing to the high risk resulting from the personal data breach as referred to in subsection 1.

(6) Section 42 (4) shall apply accordingly.

Chapter 7

Liability and penalties

Section 83

Compensation

(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation.

Section 84

Penal provisions

Section 42 shall apply accordingly to the processing of personal data by public bodies in the context of activities pursuant to Section 45, first, third or fourth sentences

ภาคผนวก ค

Personally Controlled Electronic Health Records Act 2012 (พ.ศ. 2555)

Personally Controlled Electronic Health Records Act 2012 (พ.ศ. 2555)

5 Definitions

In this Act:

consumer means an individual who has received, receives or may receive healthcare.

Note: This is the same as the definition of healthcare recipient in the Healthcare Identifiers Act 2010.

consumer-only notes, in relation to a consumer, means health information included by the consumer in his or her PCEHR and described in the PCEHR system as consumer-only notes (whether using that expression or an equivalent expression).

healthcare means :

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness or disability; or

(iii) to treat the individual's illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Note: This is the same as the definition of health service in the Privacy Act 1988.

healthcare provider means:

(a) an individual healthcare provider; or

(b) a healthcare provider organisation.

healthcare provider organisation means an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).

Note: Because of paragraph (e) of the definition of entity, a healthcare provider organisation could be a part of an entity.

health information means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of healthcare to him or her; or

(iii) healthcare provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing, healthcare; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Note: This is substantially the same as the definition of health information in the Privacy Act 1988.

individual healthcare provider means an individual who:

(a) has provided, provides, or is to provide, healthcare; or

(b) is registered by a registration authority as a member of a particular health profession.

participant in the PCEHR system means any of the following:

(a) the System Operator;

(b) a registered healthcare provider organisation;

(c) the operator of the National Repositories Service;

(d) a registered repository operator;

(e) a registered portal operator;

(f) a registered contracted service provider, so far as the contracted service provider provides services to a registered healthcare provider.

PCEHR means a personally controlled electronic health record.

PCEHR Rules has the meaning given by section 109.

PCEHR system means a system:

(a) that is for:

(i) the collection, use and disclosure of information from many sources using telecommunications services and by other means, and the holding of that information, in accordance with consumers' wishes or in circumstances specified in this Act; and

(ii) the assembly of that information using telecommunications services and by other means so far as it is relevant to a particular consumer, so that it can be made available, in accordance with the consumer's wishes or in circumstances specified in this Act, to facilitate the provision of healthcare to the consumer or for purposes specified in this Act; and

(b) that involves the performance of functions under this Act by the System Operator.

personal information has the same meaning as in the Privacy Act 1988.

personally controlled electronic health record of a consumer means the record of information that is created and maintained by the System Operator in relation to the consumer, and information that can be obtained by means of that record, including the following:

(a) information included in the entry in the Register that relates to the consumer;

(b) health information connected in the PCEHR system to the consumer (including information included in a record accessible through the index service);

(c) other information connected in the PCEHR system to the consumer, such as information relating to auditing access to the record;

(d) back-up records of such information.

9 Definition of identifying information

(1) Each of the following is identifying information of a healthcare provider who is an individual:

(a) the name of the healthcare provider;

(b) the address of the healthcare provider;

(c) the email address, telephone number and fax number of the healthcare provider;

(d) the date of birth, and the date of birth accuracy indicator, of the healthcare provider;

(e) the sex of the healthcare provider;

(f) the type of healthcare provider that the individual is;

(g) if the healthcare provider is registered by a registration authority—the registration authority's identifier for the healthcare provider and the status of the registration (such as conditional, suspended or cancelled);

(h) other information that is prescribed by the regulations for the purpose of this paragraph.

(2) Each of the following is identifying information of a healthcare provider that is not an individual:

(a) the name of the healthcare provider;

(b) the address of the healthcare provider;

(c) the email address, telephone number and fax number of the healthcare provider;

(d) if applicable, the ABN (within the meaning of the A New Tax System (Australian Business Number) Act 1999) of the healthcare provider;

(e) if applicable, the ACN (within the meaning of the Corporations Act 2001) of the healthcare provider;

(f) other information that is prescribed by the regulations for the purpose of this paragraph.

(3) Each of the following is identifying information of an individual, other than an individual in the capacity of a healthcare provider:

(a) if applicable, the Medicare number of the individual;

(b) if applicable, the Veterans' Affairs Department file number of the individual;

(d) the address of the individual;

(e) the date of birth, and the date of birth accuracy indicator, of the individual;

(f) the sex of the individual;

(g) if the individual was part of a multiple birth—the order in which the individual was born;

Example: The second of twins.

(h) if applicable, the date of death, and the date of death accuracy indicator, of the individual.

Division 2—Registering healthcare provider organisations

42 Healthcare provider organisation may apply for registration

(1) A healthcare provider organisation may apply to the System Operator for registration of the healthcare provider organisation.

(2) The application must:

(a) be in the approved form; and

(b) include, or be accompanied by, the information and documents required by the form; and

(c) be lodged at a place, or by a means, specified in the form.

Part 4—Collection, use and disclosure of health information included in a registered consumer's PCEHR

Division 1—Unauthorised collection, use and disclosure of health information included in a consumer's PCEHR

59 Unauthorised collection, use and disclosure of health information included in a consumer's PCEHR

(1) A person must not collect from the PCEHR system health information included in a consumer's PCEHR if the collection by the person is not authorised under Division 2, and the person knows or is reckless as to that fact.

Civil penalty: 120 penalty units.

(2) A person must not use or disclose health information included in a consumer's PCEHR if:

(a) the person obtained the information by using or gaining access to the PCEHR system; and

(b) the use or disclosure is not authorised under Division 2, and the person knows or is reckless as to that fact.

Civil penalty: 120 penalty units.

60 Secondary disclosure

(1) A person must not use or disclose health information included in a consumer's PCEHR if:

(a) the information was disclosed to the person in contravention of subsection 59(2); and

(b) the person knows that, or is reckless as to whether, the disclosure of the information to the person contravened that subsection.

Civil penalty: 120 penalty units.

(2) Subsection (1) does not apply if the person discloses the information for the purpose of an appropriate authority investigating the contravention mentioned in paragraph (1)(a).

Division 2—Authorised collection, use and disclosure

Subdivision A—Collection, use and disclosure in accordance with access controls

61 Collection, use and disclosure for providing healthcare

(1) A participant in the PCEHR system is authorised to collect, use and disclose health information included in a registered consumer's PCEHR if the collection, use or disclosure of the health information is:

(a) for the purpose of providing healthcare to the registered consumer; and

(b) in accordance with:

(i) the access controls set by the registered consumer; or

(ii) if the registered consumer has not set access controls—the default access controls specified by the PCEHR Rules or, if the PCEHR Rules do not specify default access controls, by the System Operator.

(2) Subsection (1) does not authorise a participant in the PCEHR system to collect, use or disclose health information included in consumer-only notes.

Subdivision B—Collection, use and disclosure other than in accordance with access controls

63 Collection, use and disclosure for management of PCEHR system

A participant in the PCEHR system is authorised to collect, use and disclose health information included in a consumer's PCEHR if:

(a) the collection, use or disclosure is undertaken for the purpose of the management or operation of the PCEHR system, if the consumer would reasonably expect the participant to collect, use or disclose the health information for that purpose; or

(b) the collection, use or disclosure is undertaken in response to a request by the System Operator for the purpose of performing a function or exercising a power of the System Operator.

Note: For example, the System Operator might make a request under paragraph (b) for the purposes of section 69 or 70.

64 Collection, use and disclosure in the case of a serious threat

(1) A participant in the PCEHR system is authorised to collect, use and disclose health information included in a registered consumer's PCEHR if:

(a) the participant reasonably believes that:

(i) the collection, use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; and

(ii) it is unreasonable or impracticable to obtain the consumer's consent to the collection, use or disclosure; and

(b) unless the participant is the System Operator—the participant advises the System Operator of the matters in paragraph (a); and

(c) the collection, use or disclosure occurs not later than 5 days after that advice is given.

(2) A participant in the PCEHR system is authorised to collect, use and disclose health information included in a consumer's PCEHR if the participant reasonably believes that the collection, use or disclosure by the participant is necessary to lessen or prevent a serious threat to public health or public safety.

(3) Subsections (1) and (2) do not authorise a participant in the PCEHR system to collect, use or disclose consumer-only notes.

65 Collection, use and disclosure authorised by law

(1) Subject to section 69, a participant in the PCEHR system is authorised to collect, use and disclose health information included in a consumer's PCEHR if the collection, use or disclosure is required or authorised by Commonwealth, State or Territory law.

(2) Subsection (1) does not authorise a participant in the PCEHR system to collect, use or disclose consumer-only notes.

66 Collection, use and disclosure with consumer's consent

(1) A participant in the PCEHR system is authorised to disclose for any purpose health information included in a consumer's PCEHR to the consumer.

(2) A participant in the PCEHR system is authorised to collect, use and disclose for any purpose health information included in a consumer's PCEHR with the consent of the consumer.

67 Collection, use and disclosure by a consumer

A consumer is authorised to collect, use and disclose, for any purpose, health information included in his or her PCEHR.

Note: The information the consumer can collect through the PCEHR system after cancellation of the consumer's registration may be limited.

68 Collection, use and disclosure for indemnity cover

(1) A participant in the PCEHR system is authorised to collect, use and disclose health information included in a consumer's PCEHR for purposes relating to the provision of indemnity cover for a healthcare provider.

(2) Subsection (1) does not authorise a participant in the PCEHR system to collect, use or disclose consumer-only notes.

Part 5—Other civil penalty provisions

74 Registered healthcare provider organisations must ensure certain information is given to System Operator

(1) A registered healthcare provider organisation is liable for a civil penalty if:

(a) an individual requests access to a consumer's PCEHR on behalf or purportedly on behalf of the registered healthcare provider organisation; and

(b) the individual does not give enough information to the System Operator to enable the System Operator to identify the individual who made the request without seeking further information from another person.

Civil penalty: 100 penalty units.

(2) Subsection (1) does not require an individual to give more than the minimum information necessary to identify the individual by name.

Part 6—Civil penalty supporting provisions

Division 1—Civil penalty orders

79 Civil penalty orders

Application for order

(1) The Information Commissioner may apply to a Court for an order that a person who is alleged to have contravened a civil penalty provision pay the Commonwealth a pecuniary penalty.

(2) The Information Commissioner must make the application within 6 years of the alleged contravention.

Court may order person to pay pecuniary penalty

(3) If the Court is satisfied that the person has contravened the civil penalty provision, the Court may order the person to pay to the Commonwealth such pecuniary penalty for the contravention as the court determines to be appropriate.

Note: Subsection (5) sets out the maximum penalty that the court may order the person to pay.

(4) An order under subsection (3) is a civil penalty order.

Determining pecuniary penalty

(5) The pecuniary penalty must not be more than:

(a) if the person is a body corporate—5 times the pecuniary penalty specified for the civil penalty provision; and

(b) otherwise—the pecuniary penalty specified for the civil penalty provision.

(6) In determining the pecuniary penalty, the Court may take into account all relevant matters, including:

(a) the nature and extent of the contravention; and

(b) the nature and extent of any loss or damage suffered because of the contravention; and

(c) the circumstances in which the contravention took place; and

(d) whether the person has previously been found by a court in proceedings under one or more of the following to have engaged in any similar conduct:

(i) this Act;

(ii) the Crimes Act 1914 or the Criminal Code in relation to this Act; and

(e) the steps taken by the person to notify the contravention to appropriate persons (if any); and

(f) the steps taken by the person to prevent further contraventions.

80 Civil enforcement of penalty

(1) A pecuniary penalty is a debt payable to the Commonwealth.

(2) The Commonwealth may enforce a civil penalty order as if it were an order made in civil proceedings against the person to recover a debt due by the person. The debt arising from the order is taken to be a judgement debt.

81 Conduct contravening more than one civil penalty provision

(1) If conduct constitutes a contravention of 2 or more civil penalty provisions, proceedings may be instituted under this Part against a person in relation to the contravention of any one or more of those provisions.

(2) However, the person is not liable to more than one pecuniary penalty under this Part in relation to the same conduct.

82 Multiple contraventions

(1) A Court may make a single civil penalty order against a person for multiple contraventions of a civil penalty provision if proceedings for the contraventions are founded on the same facts, or if the contraventions form, or are part of, a series of contraventions of the same or a similar character.

(2) However, the penalty must not exceed the sum of the maximum penalties that could be ordered if a separate penalty were ordered for each of the contraventions.

83 Proceedings may be heard together

A Court may direct that 2 or more proceedings for civil penalty orders are to be heard together.

84 Civil evidence and procedure rules for civil penalty orders

A Court must apply the rules of evidence and procedure for civil matters when hearing proceedings for a civil penalty order.

85 Contravening a civil penalty provision is not an offence

A contravention of a civil penalty provision is not an offence.

Division 3—Other matters

92 State of mind

(1) In proceedings for a civil penalty order against a person for a contravention of a civil penalty provision (other than a contravention under subsection 90(1)), it is not necessary to prove:

(a) the person's intention; or

(b) the person's knowledge; or

(c) the person's recklessness; or

(d) the person's negligence; or

(e) any other state of mind of the person;

other than as expressly provided in the civil penalty provision concerned.

(2) An expression used in a civil penalty provision that expressly provides for a state of mind has the same meaning as in the Criminal Code.

(3) Subsection (1) of this section does not affect the operation of section 91 (mistake of fact).

ภาคผนวก ง

The Data Protection Act of 2018 (พ.ศ. 2561)

The Data Protection Act of 2018 (พ.ศ. 2561)

Designation of data protection officer

34. (1) The Minister may, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, make regulations requiring controllers, processors, associations or other bodies representing categories of controllers or processors to designate a data protection officer in accordance with Article 37(4).

(2) Regulations under subsection (1) may apply to—

(a) one or more than one class of controller,

(b) one or more than one class of processor, or

(c) one or more than one class of association or other body representing categories of controllers or processors.

(3) In making regulations under subsection (1) the Minister shall have regard to the need for the protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of the foregoing, shall have regard in particular to—

(a) the nature, scope, context and purposes of the processing,

(b) risks arising for the rights and freedoms of individuals,

(c) the likelihood and the severity of such risk for the individuals concerned, and

(d) the costs of implementation of any requirement if it were imposed under that subsection.

Accreditation of certification bodies by Irish National Accreditation Board

35. The Irish National Accreditation Board is the accreditation body for the purposes of

Article 43(1).

Suitable and specific measures for processing

36. (1) Where a requirement that suitable and specific measures be taken to safeguard the fundamental rights and freedoms of data subjects in processing personal data of those subjects is imposed by this Act or regulations made under this Act, those measures may include in particular the following—

(a) explicit consent of the data subject for the processing of his or her personal data for one or more specified purposes,

(b) limitations on access to the personal data undergoing processing within a workplace in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data,

(c) strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed,

(d) specific targeted training for those involved in processing operations, and

(e) having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects—

(i) logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased,

(ii) in cases in which it is not mandatory under the Data Protection Regulation, designation of a data protection officer,

(iii) where the processing involves data relating to the health of a data subject, a requirement that the processing is undertaken by a person referred to in section 52(2),

(iv) pseudonymisation of the personal data, and

(v) encryption of the personal data.

(2) Regulations may be made for either or both of the following purposes—

(a) to identify additional suitable and specific measures (to those referred to in paragraphs (a) to (e) of subsection (1)) that may be taken to safeguard the fundamental rights and freedoms of data subjects in the processing of personal data of those subjects for the purposes of the requirement referred to in subsection (1),

(b) to specify that a measure or measures referred to in paragraphs (a) to (e) of subsection (1) or an additional measure or measures identified under paragraph (a), or both, is or are mandatory in respect of the processing to which they are stated to apply.

(3) Without prejudice to the generality of subsection (2)(a), additional suitable and

specific measures identified in regulations made under that subsection may relate to—

(a) governance structures,

(b) processes or procedures for risk assessment purposes,(c) processes or procedures for the management and conduct of research projects, and

(d) other technical and organisational measures designed to ensure that the processing is carried out in accordance with the Data Protection Regulation and processes for testing and evaluating the effectiveness of such measures.

(4) Regulations under subsection (2) may—

(a) identify different measures for different categories of personal data, different categories of controllers, different types of processing or categories of processing, and

(b) specify that a measure or measures referred to in subsection (2)(b) is or are mandatory in respect of the processing of different categories of personal data, processing by different categories of controllers and in respect of different types of processing or categories of processing.

(5) Subject to subsection (6), regulations may be made under subsection (2)—

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(6) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (2).

(7) The Commission may, on being consulted under subsection (6), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to—

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19(1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(8) In making regulations under subsection (2), the Minister or any other Minister of the Government, as the case may be, shall have regard to the public interest and the need for protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of the foregoing shall have regard to—

(a) the nature, scope, context and purposes of the processing,

(b) risks arising for the rights and freedoms of individuals, and

(c) the likelihood and the severity of the risks for the individuals concerned.

Processing of personal data and special categories of personal data by elected representatives

40. (1) For the purpose of enabling an elected representative to perform his or her functions as such a representative, the processing of personal data and special categories of personal data of a data subject by or on behalf of that representative shall be lawful where he or she receives a request or representation from the data subject or where, in accordance with subsection (2), he or she receives a request or representation from another person on behalf of the data subject.

(2) A person may make a request or representation on behalf of a data subject where the data subject—

(a) has given his or her consent to the making of the request or representation, as the case may be, or

(b) is, by reason of his or her physical or mental incapacity or age, unable to make a request or representation on his or her own behalf.

(3) In processing special categories of personal data under subsection (1), an elected representative shall impose limitations on access to that data to prevent unauthorised consultation, alteration, disclosure or erasure of that data.

(4) For the purpose referred to in subsection (1) and to the extent that disclosure is necessary and proportionate to enable an elected representative to deal with a request or representation referred to in that subsection, subject to suitable and specific measures being taken

to safeguard the fundamental rights and freedoms of the data subject, it shall be lawful for a person to disclose to the representative or a person acting on his or her behalf personal data and special categories of personal data of a data subject who makes the request or representation, or on whose behalf the request or representation is made, as the case may be, to enable that representative respond to that request or representation.

(5) In this section, "elected representative" means—

(a) a member of either House of the Oireachtas,

(b) a member of the European Parliament,

(c) a member of a local authority.

Processing for purpose other than purpose for which data collected

41. Without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—

(a) of preventing a threat to national security, defence or public security,

(b) of preventing, detecting, investigating or prosecuting criminal offences, or

(c) set out in paragraph (a) or (b) of section 47 .

Processing of personal data relating to criminal convictions and offences

55. (1) Without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 and subject to compliance with Article 6(1) and to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject, personal data referred to in Article 10 (in this section referred to as "Article 10 data") may be processed—

(a) under the control of official authority, or

(b) where—

(i) the data subject has given explicit consent to the processing for one or more specified purposes except where the law of the European Union or the law of the State prohibits such processing,

(ii) processing is necessary and proportionate for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,

(iii) processing is—

(I) necessary for the purpose of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or

(II) otherwise necessary for the purposes of establishing, exercising or defending legal rights,

(iv) processing is necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person, or

(v) processing is permitted in regulations made under subsection (3) or is otherwise authorised by the law of the State.

(2) Processing under the control of official authority referred to in subsection (1)(a) includes processing required for the following purposes:

(a) the administration of justice;

(b) the exercise of a regulatory, authorising or licensing function or determination of eligibility for benefits or services;

(c) protection of the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct by, or the unfitness or incompetence of, persons who are or were authorised to carry on a profession or other activity;

(d) enforcement actions aimed at preventing, detecting or investigating breaches of the law of the European Union or the law of the State that are subject to civil or administrative sanctions;

(e) archiving in the public interest, scientific or historical research purposes or statistical purposes where the processing is carried out in accordance with section 42 for those purposes by or on behalf of a public authority or public body.

(3) Without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 and subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject and subject to subsection (7), regulations may be made permitting the processing of Article 10 data where the processing is necessary and proportionate to—

(a) assess the risk of fraud or prevent fraud,

(b) assess the risk of bribery or corruption, or both, or to prevent bribery or corruption, or both, or

(c) ensure network and information systems security, and prevent attacks on and damage to computer and electronic communications systems.

(4) Subject to subsection (5), regulations may be made under subsection (3)—

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(5) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (3).

(6) The Commission may, on being consulted under subsection (5), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to—

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(7) The Minister or any other Minister of the Government, as the case may be, making regulations under subsection (3) shall have regard to the need for the protection of individuals with regard to the processing of their personal data and without prejudice to the generality of that need, have regard to—

(a) the nature, scope and purposes of the processing,

(b) any risks arising for the rights and freedoms of individuals, and

(c) the likelihood of any such risks arising and the severity of such risks.

(8) A person who knowingly or recklessly contravenes this section or any regulations made under subsection (3) shall be guilty of an offence and shall be liable—

(a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(9) In this section, "Article 10 data" shall include personal data relating to the alleged commission of an offence and any proceedings in relation to such an offence.

PART 5

Processing of Personal Data for Law Enforcement Purposes

Chapter 1

Preliminary and general (Part 5)

Interpretation (Part 5)

69. (1) In this Part—

"competent authority", subject to subsection (2), means—

(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or

(b) any other body or entity authorised by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal

offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security;

"controller", subject to subsection (2), means—

(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or

(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated—

(i) by that law, or

(ii) in accordance with criteria specified in that law;

"data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health;

"data protection impact assessment" has the meaning assigned to it by section 84 (1);

"data protection officer" has the meaning assigned to it by section 88 (1);

"data subject" means an individual to whom personal data relate;

"personal data" means information relating to—

(a) an identified living individual, or

(b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to—

(i) an identifier such as a name, an identification number, location data or an online identifier, or

(ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing", of or in relation to personal data, means an operation or a set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, including—

(a) the collection, recording, organisation, structuring or storing of the data,

(b) the adaptation or alteration of the data,

(c) the retrieval, consultation or use of the data,

(d) the disclosure of the data by their transmission, dissemination or otherwise making the data available,

(e) the alignment or combination of the data, or

(f) the restriction, erasure or destruction of the data;

"processor" means an individual who, or a legal person, public authority, agency or other body that, processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment;

"special categories of personal data" means—

(a) personal data revealing—

(i) the racial or ethnic origin of the data subject,

(ii) the political opinions or the religious or philosophical beliefs of the data subject, or

(iii) whether the data subject is a member of a trade union,

(b) genetic data,

(c) biometric data for the purposes of uniquely identifying an individual,

(d) data concerning health, or

(e) personal data concerning an individual's sex life or sexual orientation.

Chapter 2

General principles of data protection

Processing of personal data

71. (1) A controller shall, as respects personal data for which it is responsible, comply with the following provisions:

(a) the data shall be processed lawfully and fairly;

(b) the data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;

(c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) the data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) the data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed;

(f) the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against—

(i) unauthorised or unlawful processing, and

(ii) accidental loss, destruction or damage.

(2) The processing of personal data shall be lawful where, and to the extent that—

(a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70 (1)(a) and the function has a legal basis in the law of the European Union or the law of the State, or

(b) the data subject has, subject to subsection (3), given his or her consent to the processing.

(3) Where the processing of personal data is to be carried out on the basis of the consent of the data subject referred to in subsection (2)(b), the processing shall be lawful only where, and to the extent that—

(a) having been informed of the intended purpose of the processing and the identity of the controller, the data subject gives his or her consent freely and explicitly,

(b) the request for consent is expressed in clear and plain language, and where such consent is given in the context of a written statement that also concerns other matters, the request for consent is presented to the data subject in a manner that is clearly distinguishable from those other matters, and

(c) the data subject may withdraw his or her consent at any time, and he or she shall be informed of this possibility prior to giving consent.

(4) Where a data subject withdraws his or her consent to the processing of personal data pursuant to subsection (3)(c), the withdrawal of consent shall not affect the lawfulness of processing based on that consent prior to the consent being withdrawn.

(5) Where a controller collects personal data for a purpose specified in section 70 (1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as—

(a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and

(b) the processing is necessary and proportionate to the purpose for which the data are being processed.

(6) A controller may process personal data, whether the data were collected by the controller or another controller, for—

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes,

provided that the said processing—

(i) is for a purpose specified in section 70 (1)(a), and

(ii) is subject to appropriate safeguards for the rights and freedoms of data subjects.

(7) A controller shall ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for—

(a) the erasure of the data, or

(b) the carrying out of periodic reviews of the need for the retention of the data.

(8) Where a time limit is established in accordance with subsection (7), the controller shall ensure, by means of procedural measures, that the time limit is observed.

(9) A processor, or any person acting under the authority of the controller or of the processor who has access to personal data, shall not process the data unless the processor or person is—

(a) authorised to do so by the controller, or

(b) required to do so by the law of the European Union or the law of the State,

and then only to the extent so authorised or required, as the case may be.

(10) A controller shall ensure that it is in a position to demonstrate that the processing of personal data for which it is responsible is in compliance with subsections (1) to (8) of this section.

Security measures for personal data

72. (1) In determining appropriate technical or organisational measures for the purposes of section 71 (1)(f), a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.

(2) A controller or processor shall take all reasonable steps to ensure that—

(a) persons employed by the controller or the processor, as the case may be, and

(b) other persons at the place of work concerned,

are aware of and comply with the relevant technical or organisational measures referred to in subsection (1).

Processing of special categories of personal data (Part 5)

73. (1) The processing of a special category of personal data shall be lawful only where—

(a) section 71 is complied with, and

(b) at least one of the following conditions is met:

(i) where the processing is to be carried out on the basis of the consent of the data subject pursuant to section 71 (2)(b), the consent referred to in that paragraph explicitly refers to the special category of personal data concerned;

(ii) the processing is necessary—

(I) to prevent injury or other damage to the data subject or another individual,

(II) to prevent loss in respect of, or damage to, property, or

(III) otherwise to protect the vital interests of the data subject or another individual;

(iii) the personal data to which the processing relates have been made public as a result of steps deliberately taken by the data subject;

(iv) the processing is necessary for—

(I) the administration of justice,

(II) the performance of a function conferred on a person by or under an enactment, or

(III) the performance of a function of the Government or a Minister of the Government;

(v) the processing—

(I) is required for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or

(II) is otherwise required for the purposes of establishing, exercising or defending legal rights;

(vi) the processing is necessary for medical purposes and is carried out by, or under the responsibility of—

(I) a health practitioner, or

(II) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner;

(vii) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law;

(viii) the processing is carried out pursuant to section 71 (6);

(ix) the processing is authorised by regulations made under subsection (2).

(2) Regulations may be made permitting the processing of special categories of personal data for the purposes of subsection (1)(b)(ix) where the processing is necessary for reasons of substantial public interest, and without prejudice to the generality of the foregoing, such regulations shall identify the public interest concerned.

(3) Subject to subsection (4), regulations may be made under subsection (2)—

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(4) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (2).

(5) The Commission may, on being consulted under subsection (4), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and if the Minister or any other Minister of the Government proposes to

proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to—

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(6) The Minister or any other Minister of the Government, as the case may be, making regulations under subsection (2) shall have regard to the need for the protection of individuals with regard to the processing of their personal data and without prejudice to the generality of that need, have regard to—

(a) the nature, scope and purposes of the processing,

(b) the nature of the substantial public interest concerned,

(c) any benefits likely to arise for the data subjects concerned,

(d) any risks arising for the rights and freedoms of such subjects, and

(e) the likelihood of any such risks arising and the severity of such risks.

(7) Where a special category of personal data is processed in accordance with this section, the controller shall ensure that the processing is carried out with appropriate safeguards for the rights and freedoms of the data subject.

(8) In this section—

"health practitioner" has the same meaning as it has in the Health Identifiers Act 2014 ;

"medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of medical care and treatment and the management of healthcare services.

Data protection officer

88. (1) A controller, other than—

(a) a court, or

(b) another independent judicial authority,

acting in its judicial capacity, shall, subject to subsections (2) and (3), appoint a person to carry out the functions specified in subsection (5) in respect of the controller (in this Part referred to as a "data protection officer").

(2) Two or more controllers may, subject to subsection (3), having regard to their organisational structure and size, appoint a single data protection officer to carry out the functions specified in subsection (5) in respect of each of the controllers.

(3) A controller, when appointing a data protection officer, shall do so on the basis of—

(a) the person's expert knowledge of the law and the practice relating to the protection of personal data, and

(b) his or her ability to carry out the functions specified in subsection (5).

(4) Where a controller appoints a data protection officer, the controller shall—

(a) publish or cause to be published the contact details of the data protection officer,

(b) inform the Commission of the appointment of the data protection officer and provide the Commission with his or her contact details,

(c) ensure that the data protection officer—

(i) reports directly, in relation to his or her functions under subsection (5), to the highest level of management of the controller,

(ii) does not receive any instructions regarding the exercise of such functions, and

(iii) is involved in an appropriate and timely manner in all matters relating to the protection of personal data, and

(d) support the data protection officer in performing his or her functions under subsection (5), including by—

(i) providing him or her with the resources that he or she requires to perform those functions,

(ii) ensuring that he or she has access to processing operations carried out by the controller, and

(iii) assisting him or her to maintain his or her expert knowledge in the law and practice relating to the protection of personal data.

(5) The functions of a data protection officer shall include the following:

(a) informing and advising the controller, and the employees of the controller who carry out processing, of their obligations under this Part and under any other law of the European Union or law of the State that relates to the protection of personal data;

(b) monitoring the compliance of the controller with—

(i) this Part,

(ii) any other law of the European Union or law of the State that relates to the protection of personal data, and

(iii) the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities in the controller in relation to the protection of personal data, the raising of awareness and the training of staff involved in processing operations in that regard, and any audit activity related to the protection of personal data;

(c) providing advice, where requested to do so, in relation to the carrying out of a data protection impact assessment in accordance with section 84 and monitoring any steps taken on foot of that assessment;

(d) acting as the contact point for data subjects with regard to all issues related to the processing of their personal data and to the exercise of their rights under this Part;

(e) cooperating with the Commission and acting as a contact point for the Commission for issues related to processing carried out by the controller, including consultation by the controller with the Commission under section 84 .

Chapter 4

Rights, and restriction of rights, of data subject (Part 5)

Rights in relation to automated decision making (Part 5)

89. (1) Subject to subsection (2), a decision that produces an adverse legal effect for a data subject or significantly affects a data subject shall not be based solely on automated processing, including profiling, of personal data that relate to him or her.

(2) Subsection (1) shall not apply where—

(a) the taking of a decision based solely on automated processing is authorised by the law of the European Union or the law of the State and the law so authorising contains appropriate safeguards for the rights and freedoms of the data subject, including the right of the data subject to make representations to the controller in relation to the decision, and

(b) the controller has taken adequate steps to safeguard the legitimate interests of the data subject.

(3) Profiling that results in discrimination against an individual on the basis of a special category of personal data shall be prohibited.

Right to information

90. (1) Subject to subsection (4) and section 94 , a controller shall ensure that the data subject is provided with, or, as appropriate, has made available to him or her, the information specified in subsection (2) in relation to personal data relating to him or her within a reasonable period after the date on which the controller obtains the personal data concerned, having regard to the circumstances in which the data are or are to be processed.

(2) The information to which subsection (1) applies is:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer of the controller, where applicable;

(c) the purpose for which the personal data are intended to be processed or are being processed;

(d) information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data;

(e) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;

(f) in individual cases where further information is necessary to enable the data subject to exercise his or her rights under this Part, having regard to the circumstances in which the personal data are or are to be processed, including the manner in which the data are or have been collected, any such information including:

(i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data;

(ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

(iii) where applicable, each category of recipients of the data.

(3) The information referred to in paragraphs (a) to (e) of subsection (2) may be made available to the data subject by means of publication on the website of the controller.

(4) Without prejudice to section 94 , subsection (1) shall not apply to information specified in subsection (2)—

(a) where the information is already in the possession of the data subject, or

(b) where, in particular in the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the provision of the information proves impossible or would involve a disproportionate effort.

Right of access

91. (1) Subject to subsections (7), (9) and (12) and sections 93 (4)(ii) and 94 , an individual who believes that personal data relating to him or her have been or are being processed by or on behalf of a controller, if he or she so requests the controller by notice in writing shall—

(a) be informed by the controller whether personal data relating to him or her have been or are being processed by or on behalf of the controller, and

(b) where such data have been or are being so processed, be provided by the controller with the following information:

(i) a description of—

(I) the purpose of, and the legal basis for, the processing,

(II) the categories of personal data concerned,

(III) the recipients or categories of recipients to whom the personal data concerned have been disclosed, and

(IV) the period for which the personal data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

(ii) information detailing the right of the data subject to request from the controller the rectification or erasure of the personal data concerned;

(iii) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;

(iv) a communication of the personal data concerned;

(v) any available information as to the origin of the personal data concerned, unless the communication of that information is contrary to the public interest.

(2) A controller shall respond to a request made under subsection (1) and provide the information specified in paragraph (b) thereof to the data subject as soon as may be and, subject to subsections (4) and (5), in any event not later than one month after the date on which the request is made.

(3) When making a request under subsection (1), the individual making the request shall provide the controller with such information as the controller may reasonably require to satisfy itself of the identity of the individual and to locate any relevant personal data or information.

(4) Where a controller has reasonable doubts as to the identity of an individual making a request under subsection (1) or reasonably requires additional information to locate any relevant personal data, it may request such additional information from the data subject as may be necessary to confirm his or her identity or to enable it to locate such personal data or information, as the case may be, and the period of time from the making of such a request for additional information until the request is complied with shall not be reckonable for the purposes of subsection (2).

(5) Where, taking into account the complexity of a request made under subsection (1) and the number of such requests received by the controller, the controller is of the opinion that it requires additional time to consider the request, it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in subsection (2) by such further period not exceeding 2 months as it may specify by notice in writing to the individual making the request.

(6) A notice in writing referred to in subsection (5) shall include the reason for which the controller is of the opinion that it requires additional time to consider the request made under subsection (1).

(7) Where information that a controller would otherwise be required to provide to a data subject pursuant to subsection (1) includes personal data relating to another individual that would reveal, or would be capable of revealing, the identity of the individual, the controller—

(a) shall not, subject to subsection (8), provide the data subject with the information that constitutes such personal data relating to the other individual, and

(b) shall provide the data subject with a summary of the personal data concerned that—

(i) in so far as is possible, permits the data subject to exercise his or her rights under this Part, and

(ii) does not reveal, or is not capable of revealing, the identity of the other individual.

(8) Subsection (7) shall not apply where the individual to whom the personal data that would reveal, or would be capable of revealing, his or her identity, relate consents to the provision of the information concerned to the data subject making a request pursuant to subsection (1).

(9) Subsection (1) shall not apply—

(a) in respect of personal data relating to the data subject that consists of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential, or

(b) to information specified in paragraph (b)(i)(III) of that subsection in so far as a recipient referred to therein is a public authority which may receive data in the context of a particular inquiry in accordance with the law of the State.

(10) Information provided pursuant to a request under subsection (1) may take account of any amendment of the personal data concerned made since the receipt of the request by the controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.

(11) The obligations imposed by subparagraphs (iv) and (v) of subsection (1)(b) shall be complied with by supplying the data subject with a copy of the information concerned in permanent form unless—

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise.

(12) Where a controller has previously complied with a request under subsection (1), the controller is not obliged to comply with a subsequent identical or similar request under that subsection by the same individual unless, in the opinion of the controller, a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(13) In determining for the purposes of subsection (12) whether the reasonable interval specified in that subsection has elapsed, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered.

(14) Where a controller, pursuant to subsection (12) refuses to act upon a request under subsection (1), it shall, as soon as practicable, so notify the data subject in writing.

Right to rectification or erasure and restriction of processing

92. (1) Where a data subject is of the opinion that a controller is processing personal data relating to him or her that are inaccurate, the data subject may make a request in writing to the controller for the controller to rectify the data concerned.

(2) A controller that receives a request under subsection (1) shall, subject to subsections (6), (7) and (9) and section 93 (4)(ii), where it is satisfied that the personal data to which the request relates are inaccurate, rectify the data as soon as may be and in any event no later than one month after the date on which the request is made.

(3) Where a data subject is of the opinion that a controller is processing personal data relating to him or her—

(a) in a manner that contravenes subsections (1) to (6) of section 71 or section 73 (1), or

(b) that are required to be erased by the controller in accordance with a legal obligation to which the controller is subject,

the data subject may make a request in writing to the controller to erase the data concerned.

(4) A controller that receives a request under subsection (3) shall, subject to subsections (6), (7) and (9) and section 93 (4)(ii), where it is satisfied that paragraph (a) or (b) of subsection (3) applies to the personal data to which the request relates, erase the data as soon as may be and in any event no later than one month after the date on which the request is made.

(5) When making a request under subsection (1) or (3), the data subject shall provide such information as the controller may reasonably require to—

(a) satisfy itself as to the identity of the data subject,

(b) locate any relevant personal data, and

(c) satisfy itself as to whether the personal data concerned are inaccurate or as to the basis on which the data should be erased, as the case may be.

(6) Where a controller—

(a) has reasonable doubts as to the identity of an individual making a request under subsection (1) or (3), or

(b) reasonably requires additional information—

(i) to locate any relevant personal data, or

(ii) to satisfy itself as to whether the personal data concerned are inaccurate or as to the basis on which the data should be erased, as the case may be,

it may request such additional information from the data subject as may be necessary to confirm his or her identity or to so locate or satisfy itself, as the case may be, and the period of time from the making of such a request for additional information until the request is complied with shall not be reckonable for the purposes of subsection (2) or (4), as the case may be.

(7) Where, taking into account the complexity of a request made under subsection (1) or (3) and the number of such requests received by the controller, the controller is of the opinion that it requires additional time to consider the request, it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in subsection (2) or (4), as the case may be, by such further period not exceeding 2 months as it may specify by notice in writing to the data subject making the request.

(8) A notice in writing referred to in subsection (7) shall include the reason for which the controller is of the opinion that it requires additional time to consider the request made under subsection (1) or (3), as the case may be.

(9) Where a data subject makes a request under subsection (1) or (3), and—

(a) the accuracy of the data is contested by the data subject and it is not possible to ascertain whether the data are so inaccurate, or

(b) the personal data are required for the purposes of evidence in proceedings before a court or tribunal or in another form of official inquiry,

the controller shall restrict the processing of the data and shall not rectify or erase the data, as the case may be.

(10) Where a controller—

(a) complies with a request under subsection (1) or (3), or

(b) restricts the processing of personal data under subsection (9),

the controller shall, as soon as practicable, notify in writing—

(i) subject to section 94 , the data subject concerned,

(ii) each controller from which the personal data concerned were received, and

(iii) each person to whom the personal data concerned were disclosed,

of the rectification, erasure or restriction concerned, as the case may be.

(11) Where a controller receives a request under subsection (1) or (3), and—

(a) the controller is not satisfied that, as the case may be,—

(i) in relation to a request under subsection (1), the personal data to which the request relates should be rectified pursuant to subsection (2), or

(ii) in relation to a request under subsection (3), the personal data to which the request relates should be erased pursuant to subsection (4),

and

(b) subsection (9) does not apply to the data,

the controller shall, subject to section 94 , as soon as practicable, so notify the data subject in writing.

(12) A notification under subsection (11) shall include—

(a) the reasons for the controller's decision under that subsection, and

(b) information relating to the data subject's right under section 95 to request the Commission to verify the lawfulness of the processing concerned.

(13) Where a person to whom personal data were disclosed is notified under subsection (10) of—

(a) the rectification or erasure of the data pursuant to a request under subsection (1) or (3), as the case may be, or

(b) the restriction of the processing of the data under subsection (9),

the person shall rectify or erase, or restrict the processing of, as the case may be, any of the data concerned that the person has under his or her control in the same manner, and to the same extent, as the controller making the notification has rectified or erased, or restricted the processing of, as the case may be, the data concerned.

(14) Where a controller has restricted the processing of personal data pursuant to subsection (9) and proposes to lift the said restriction, the controller shall inform the data subject prior to the lifting of the restriction.

(15) Where a controller that restricted the processing of personal data pursuant to subsection (9) lifts the said restriction—

(a) the controller shall notify any person who was notified under subsection (10) of the said restriction of the lifting of the restriction as soon as practicable, and

(b) the person so notified shall lift any restriction of the processing of the data concerned implemented under subsection (13) in the same manner, and to the same extent, as the controller making the notification has lifted the restriction on the processing of the data concerned.

(16) This section shall not apply to personal data that are contained in witness statements.

(17) For the purposes of this section, personal data are inaccurate if—

(a) they are incorrect or misleading as to any matter of fact, or

(b) they are incomplete in a material manner.

Communication with data subject

93. (1) Where a controller—

(a) provides or makes available information to a data subject under section 90 ,

(b) provides or makes available information to, or communicates with, a data subject pursuant to a request under section 91 or 92,

the controller shall take all reasonable steps to ensure the information is provided or made available, or the communication is made, as the case may be, in a concise, intelligible and easily accessible form using clear and plain language.

(2) The information or communication, as the case may be, referred to in subsection (1), shall—

(a) be provided to the data subject by appropriate means, including by electronic means, and

(b) in the case of a communication with a data subject pursuant to a request under section 91 or 92 , in so far as is possible, be provided in the same form as that in which the request is made.

(3) A controller shall not impose a charge on a data subject for information provided to him or her under section 90 or, subject to subsection (4)(i), pursuant to a request under section 91 or 92 .

(4) Where a data subject makes a request to a controller under section 91 or 92 that is—

(a) manifestly unfounded, or

(b) excessive in nature, having regard to the number of requests made by the data subject to the controller under those sections,

the controller may—

(i) charge a reasonable fee to the data subject in respect of the request, having regard to the administrative cost to the controller of complying with the request, or

(ii) refuse to act upon the request.

(5) Where a controller, pursuant to subsection (4)(ii), refuses to act upon a request under section 91 or 92 it shall, as soon as practicable, so notify the data subject in writing.

(6) A notification under subsection (5) shall include—

(a) the reasons for which the controller is refusing to act upon the request under section 91 or 92 , as the case may be, pursuant to subsection (4)(ii), and

(b) information relating to the right of the data subject under Chapter 3 of Part 6 to lodge a complaint with the Commission and the contact details of the Commission.

(7) Where, pursuant to subsection (4)(ii), a controller refuses to act upon a request made to the controller by a data subject under section 91 or 92 , it shall be for the controller to demonstrate that the request was manifestly unfounded or excessive in nature.

(8) In this section, a reference to a "data subject" shall be construed as including an individual who makes a request under section 91 (1), irrespective of whether the controller is processing personal data relating to the individual.

Restrictions on exercise of data subject rights (Part 5)

94. (1) Subject to subsection (2), a controller, with respect to personal data for which it is responsible, may restrict, wholly or partly, the exercise of a right of a data subject specified in subsection (4).

(2) Subsection (1) shall apply where the controller is satisfied that restricting the exercise of a right under that subsection constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject for the purposes of—

(a) avoiding obstructing official or legal inquiries, investigations or procedures,

(b) avoiding prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,

(c) protecting public security,

(d) protecting national security, or

(e) protecting the rights and freedoms of other persons.

(3) Without prejudice to the generality of subsection (2), the purposes specified in paragraphs (a) to (e) of subsection (2) include the following:

(a) the prevention, detection or investigation of offences, the apprehension or prosecution of offenders or the effectiveness of lawful methods, systems, plans or procedures employed for the purposes of the matters aforesaid;

(b) the enforcement of, compliance with or administration of any enactment related to a purpose specified in section 70 (1)(a);

(c) ensuring the safety of the public and the safety or security of individuals and property;

(d) ensuring the fairness of criminal proceedings in a court or other tribunal;

(e) ensuring the security of—

(i) a penal institution,

(ii) a children detention school within the meaning of section 3 of the Children Act 2001 ,

(iii) a remand centre designated under section 88 of the Children Act 2001 ,

(iv) the Central Mental Hospital, or

(v) any system of communications, whether internal or external, of the Garda Síochána, the Defence Forces, the Revenue Commissioners or a penal institution;

(f) protecting the life, safety or well-being of any person;

(g) preventing the facilitation of the commission of an offence;

(h) avoiding the prejudice or impairment of national security, defence or the international relations of the State;

(i) avoiding the obstruction or impairment of official or legal inquiries, investigations or procedures or the operation of legal privilege;

(j) the performance by the Commission of its functions.

(4) The rights of a data subject to which subsection (1) applies are:

(a) the right of the data subject under section 90 (1) in so far as relates to information specified in subsection (2)(f) of that section;

(b) the rights of the data subject under paragraphs (a) and (b) of section 91 (1);

(c) the right of the data subject to be notified—

(i) under section 92 (10) of the restriction of the processing of personal data under subsection (9) of that section, or

(ii) under section 92 (11) of a decision not to rectify or erase data pursuant to a request under subsection (1) or (3) of that section, as the case may be.

(5) Subject to subsection (6), where a controller restricts, pursuant to subsection (1), the exercise of the right of a data subject specified in paragraph (b) or (c) of subsection (4), the controller shall notify the data subject in writing of—

(a) the restriction of the exercise of the said right and the reasons for such restriction, and

(b) the right of the data subject—

(i) under section 95 to request the Commission to verify the lawfulness of the processing concerned, or

(ii) under section 128 to seek a judicial remedy in relation to the said restriction.

(6) Subsection (5) shall not apply where to notify the data subject in accordance with that subsection of the matters specified therein would be contrary to a purpose specified in subsection (2).

(7) Where a controller restricts, pursuant to subsection (1), the exercise of the right of a data subject specified in paragraph (b) or (c) of subsection (4), the controller shall—

(a) create and maintain a record in writing of the factual or legal basis for the decision to so restrict the right concerned, and

(b) make such a record available to the Commission, if so requested by the Commission.

(8) Regulations may be made specifying a category of processing to be a category of processing in respect of which the exercise of the rights specified in subsection (4) may, in accordance with subsection (2), be restricted under subsection (1).

(9) Regulations under subsection (8) may be made by—

(a) the Minister, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, or

(b) any other Minister of the Government, following consultation with the Minister, such other Minister of the Government as he or she considers appropriate and the Commission.

(10) The Minister of the Government making regulations under subsection (8) shall have regard to—

(a) the nature, scope and purposes of the category of processing concerned,

(b) whether, having regard to the matters referred to in paragraph (a), the restriction concerned is one to which subsection (2) would apply, and

(c) any risks arising for the rights and freedoms of data subjects.

(11) Regulations made under this section shall—

(a) respect the essence of the right to data protection and protect the interests of the data subject, and

(b) restrict the exercise of data subject rights only in so far as is necessary and proportionate to the aim sought to be achieved.

(12) For the purposes of this section, "penal institution" means—

(a) a place to which the Prisons Acts 1826 to 2015 apply, or

(b) a military prison or detention barrack within the meaning, in each case, of the Defence Act 1954 .

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางสาวจิรัชยา จิ้นสุริวงษ์
ประวัติการศึกษา	พ.ศ. 2558 นิติศาสตรบัณฑิต มหาวิทยาลัยแม่ฟ้าหลวง
ตำแหน่งและสถานที่ทำงานปัจจุบัน	นิติรปฏิบัติการ กรมส่งเสริมการปกครองท้องถิ่น