มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล : ศึกษากรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

กิจจา ทรงความเจริญ



วิทยานิพนธ์เสนอมหาวิทยาลัยพะเยา เพื่อเป็นส่วนหนึ่งของการศึกษา
หลักสูตรปริญญานิติศาสตรมหาบัณฑิต
มิถุนายน 2563
ลิขสิทธิ์เป็นของมหาวิทยาลัยพะเยา

มหาวิทยาลัยพะเยา
UNIVERSITY OF PHAYAO

มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล : ศึกษากรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

กิจจา ทรงความเจริญ

วิทยานิพนธ์เสนอมหาวิทยาลัยพะเยา เพื่อเป็นส่วนหนึ่งของการศึกษา
หลักสูตรปริญญานิติศาสตรมหาบัณฑิต
มิถุนายน 2563
ลิขสิทธิ์เป็นของมหาวิทยาลัยพะเยา

LEGAL MEASURES FOR PERSONAL DATA PROTECTION OF THE HOSPITAL SERVICE RECIPIENTS : A STUDY OF AN ELECTRONIC PERSONAL HEALTH RECORD APPLICATION

KIJJA SONGKWAMJAROEN

A Thesis Submitted to University of Phayao

in Partial Fulfillment of the Requirements

for the Master of Laws Degree

June 2020

Copyright 2020 by University of Phayao

วิทยานิพนธ์

เรื่อง

มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล : ศึกษากรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

ของ กิจจา ทรงความเจริญ

ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษา

หลักสูตรปริญญานิติศาสตรมหาบัณฑิต

ของมหาวิทยาลัยพะเยา

..... ประธานกรรมการสอบวิทยานิพนธ์

(รองศาสตราจารย์ดิเรก ควรสมาคม)

..... ประธานที่ปรึกษาวิทยานิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร. วิมลเรขา ศิริชัยราวรรณ)

..... กรรมการที่ปรึกษาวิทยานิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร.ไพรัช ธีระชัยมหิทธิ์)

..... อาจารย์บัณฑิตศึกษามหาวิทยาลัยพะเยา

(ผู้ช่วยศาสตราจารย์ ดร. ภัทราวรรณ รัตนเกษตร)

..... คณบดีคณะนิติศาสตร์

(รองศาสตราจารย์ ดร. พรรณรายรัตน์ ศรีไชยรัตน์)

เรื่อง: มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล : ศึกษากรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

ผู้วิจัย: กิจจา ทรงความเจริญ, วิทยานิพนธ์: น.ม., มหาวิทยาลัยพะเยา, 2562

อาจารย์ที่ปรึกษา: ผู้ช่วยศาสตราจารย์ ดร. วิมลเรขา ศิริชัยราวรรณ อาจารย์ที่ปรึกษาร่วม ผู้ช่วยศาสตราจารย์ ดร.ไพรัช ธีระชัยมหิทธิ์

คำสำคัญ ข้อมูลส่วนบุคคล, ระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล, ข้อมูลสุขภาพส่วนบุคคล, การละเมิดข้อมูลส่วนบุคคล

บทคัดย่อ

ภาครัฐได้เตรียมการบูรณาการในหลายด้านเพื่อการพัฒนาประเทศและยกระดับความมั่นคงในการดำรงชีวิตของประชาชนผ่านการขับเคลื่อนด้วยเทคโนโลยีสารสนเทศซึ่งหนึ่งในนั้นคือการบูรณาระบบสุขภาพของประเทศไทยโดยการนำระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลมาเป็นตัวช่วยในการเก็บและรวบรวมข้อมูลของผู้มารับบริการในโรงพยาบาล ในอดีตการจัดเก็บระเบียนสุขภาพเป็นการเก็บรวบรวมข้อมูลในรูปแบบของเอกสารกระดาษแต่ปัจจุบันระเบียนสุขภาพของผู้มารับบริการในโรงพยาบาลจัดเก็บในรูปแบบเอกสารอิเล็กทรอนิกส์ทำให้เข้าถึงข้อมูลได้ง่ายจนบางครั้งเกิดการเผยแพร่ข้อมูลของผู้มารับบริการในโรงพยาบาลสู่สาธารณะโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล และละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูล

งานวิจัยนี้ศึกษาแนวคิดทฤษฎีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายไทยที่มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลสุขภาพส่วนบุคคลได้แก่ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและสหรัฐอเมริกาในประเด็นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์เพื่อเสนอมาตรการทางกฎหมายที่เหมาะสม ดังนี้ ประการแรก ควรแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 เพื่อให้ครอบคลุมทั้งข้อมูลส่วนบุคคลและข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์โดยให้เพิ่มนิยาม“ข้อมูลสุขภาพส่วนบุคคล” เพิ่มสิทธิเจ้าของข้อมูลส่วนบุคคลด้านสุขภาพในพระราชบัญญัติฉบับนี้ ประการที่สอง ควรแก้ไขเพิ่มเติมระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคลพ.ศ. 2561 โดยเพิ่มนิยาม“ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล”

Title: LEGAL MEASURES FOR PERSONAL DATA PROTECTION OF THE HOSPITAL SERVICE RECIPIENTS : A STUDY OF AN ELECTRONIC PERSONAL HEALTH RECORD APPLICATION

Author: Kijja Songkwamjaroen, Thesis: LL.M., University of Phayao, 2019

Advisor: Assistant Professor Wimonrekha Sirichairawan , Ph.D. Co-advisor Assistant ProfessorPairush Teerachaimahit , Ph.D.

Keyword Personal Data, Personal Information, Personal Health Record, Personal Health Record Application

ABSTRACT

Thai government have prepared to integrate many aspects for developing country and raising the living standards of people through Information Technology. One of them is the integration of Thai health system by personal health record application to collect and gather the data of service recipients in a hospital. In the past, health records of service recipients were collected in the form of paper documents, but nowadays, health records of service recipients are stored in electronic documents. This make it easier to access information that results in such information being disseminated to the public without the consent of the personal data owner and violate the right to privacy of the data owner.

This research studies the concept and theory regarding personal data protection and the provisions in Thai law regarding personal health data protection, such as the Ministerial Regulation on the Protection and Management of Personal Health Information B.E. 2561 and the Personal Data Protection Act B.E. 2562 in comparison with the personal data protection laws of the European Union and the United States of America. It focuses on issue of the protection of personal data stored in electronic systems in order to propose the appropriate legal measures as follows. First, the amendment should be made to the Personal Data Protection Act B.E. 2562 in order to cover both personal data and personal health data stored in the electronic system by adding the definition of “personal health data” and adding the rights of personal health data owners into this Act. Second, amendments should be made to the Ministerial Regulation on the Protection and Management of Personal Health Information B.E. 2561 by adding the definition of “Electronic Personal Health Information”.

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จลุล่วงอย่างสมบูรณ์ด้วยความกรุณาและความช่วยเหลือเป็นอย่างยิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.วิมลเรขา ศิริชัยราวรรณ และผู้ช่วยศาสตราจารย์ ดร.ไพรัช ธีระชัยมหิทธิ์ อาจารย์ที่ปรึกษา ขอขอบคุณ พ.ต.ท.เทิดสยาม บุญยะเสนา กรุณาชี้แนะแนวทางในด้านกฎหมาย

ขอบกราบขอบพระคุณรองศาสตราจารย์ดิเรก ควรสมาคม ที่กรุณาเป็นประธานกรรมการสอบ ผู้ช่วยศาสตราจารย์ ดร.ภัทราวรรณ รัตนเกษตร ผู้ช่วยศาสตราจารย์ ดร.นภนันต์ ศุภศิริพงษ์ และผู้ช่วยศาสตราจารย์ ดร.ธิติ ไวกวี เป็นอย่างสูงที่รับเป็นกรรมการตรวจโครงร่างวิทยานิพนธ์ พร้อมทั้งให้คำแนะนำ ข้อเสนอแนะในการเขียนวิทยานิพนธ์อย่างละเอียด ทำให้วิทยานิพนธ์เล่มนี้มีความสมบูรณ์ยิ่งขึ้น ขอกราบขอบพระคุณคณบดีคณะนิติศาสตร์ มหาวิทยาลัยพะเยา รองศาสตราจารย์ ดร.พรรณรายรัตน์ ศรีไชยรัตน์ ที่สนับสนุนให้การทำวิจัยตลอดจนการสอบวิทยานิพนธ์ผ่านไปได้ด้วยดี ขอบคุณอาจารย์ทุก ๆ ท่านที่ประสิทธิประสาทวิชาและสนับสนุนงานวิจัยในครั้งนี้

ขอบคุณกำลังใจและแรงสนับสนุนจากครอบครัวโดยเฉพาะคุณแม่สุชาดา ทรงความเจริญ คุณสุนารีย์ ทรงความเจริญและครอบครัวตันแรง ขอบคุณเจ้าหน้าที่สำนักงานพื้นที่พิเศษ 6 และเจ้าหน้าที่องค์การบริหารการพัฒนาพื้นที่พิเศษเพื่อการท่องเที่ยวอย่างยั่งยืน (องค์การมหาชน) ทุกท่าน ที่สนับสนุนเรื่องเวลาในการทำวิจัย ขอบคุณท่านปองศักดิ์ นันทเสน ที่ให้กำลังใจและข้อแนะนำทั้งในเรื่องการดำเนินชีวิตและการทำงานวิจัย ท้ายที่สุดความสำเร็จจากการศึกษาและประโยชน์ที่เกิดจากงานวิจัยชิ้นนี้ ขอมอบแด่ พ.ต.อ.ประกิจ ทรงความเจริญ คุณพ่อผู้ซึ่งเป็นแรงบันดาลใจในการดำรงชีวิตของกระผมเสมอ

กิจจา ทรงความเจริญ

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง ..... ฌ

บทที่ 1 บทนำ 1

ความเป็นมา และความสำคัญของปัญหา 1

ปัญหาของการวิจัย 4

วัตถุประสงค์ของการวิจัย 4

สมมติฐานของการวิจัย 5

วิธีดำเนินการวิจัย 5

ขอบเขตของการวิจัย 5

นิยามศัพท์เฉพาะ 6

ประโยชน์ที่จะได้รับจากการวิจัย 7

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง 9

แนวคิดและทฤษฎีในการคุ้มครองสิทธิส่วนบุคคล 9

หลักการคุ้มครองข้อมูลส่วนบุคคล 13

นิยามของข้อมูลและข้อมูลส่วนบุคคล 15

กฎหมายเกี่ยวกับหลักการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพส่วนบุคคลในรูปแบบข้อมูลอิเล็กทรอนิกส์ 26

บทที่ 3 วิธีดำเนินการวิจัย 44

รูปแบบการวิจัย 44
วิธีการเก็บรวบรวมข้อมูล 44
การวิเคราะห์ข้อมูล 44
บทที่ 4 ผลการวิจัย 46
มาตรการคุ้มครองข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ 47
การศึกษามาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ของผู้มารับบริการในโรงพยาบาลกรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล. 71
บทที่ 5 สรุปและข้อเสนอแนะ 88
บทสรุป 88
ข้อเสนอแนะ 90
บรรณานุกรม 93
ภาคผนวก 98
ภาคผนวก ก ระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 99
ภาคผนวก ข หนังสือแสดงความยินยอม 108
ภาคผนวก ค มาตรฐานข้อมูลระบบประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์ 109
ภาคผนวก ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 114
ประวัติผู้วิจัย 122

สารบัญตาราง

หน้า

ตาราง 1 แสดงการเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 GDPR และ HIPAA.....48

ตาราง 2 ตารางการประเมินโอกาสที่จะเกิดความเสี่ยง 61

ตาราง 3 เกณฑ์การประเมินผลกระทบของความเสี่ยงด้านการดำเนินงาน..... 61

ตาราง 4 เกณฑ์การประเมินผลกระทบของความเสี่ยงด้านนโยบาย กฎหมายและระเบียบข้อบังคับ 62

ตาราง 5 แสดงการประเมินระดับความเสี่ยง.....63

ตาราง 6 แสดงเกณฑ์ระดับความเสี่ยง 63

ตาราง 7 เปรียบเทียบเวชระเบียนแบบเดิมและระเบียนสุขภาพอิเล็กทรอนิกส์ 74

บทที่ 1

บทนำ

ความเป็นมา และความสำคัญของปัญหา

สังคมยุคปัจจุบันสื่ออิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญในการดำรงชีวิตประจำวัน เป็นสื่อที่ได้รับความนิยมอย่างแพร่หลายในทุกกิจกรรมที่เกี่ยวข้อง วิวัฒนาการของสื่ออิเล็กทรอนิกส์ทำให้สามารถเข้าถึงข้อมูลหรือข่าวสารได้ง่าย ในทางกลับกันเมื่อข้อมูลสามารถเข้าถึงได้ง่ายจึงอาจมีการนำข้อมูลเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น โดยอาจก่อให้เกิดความเสียหายหรือสูญหายของข้อมูลหรืออาจถูกนำข้อมูลไปใช้ในทางที่ผิดไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตาม ความก้าวหน้าของสังคมยุคข้อมูลข่าวสารนำมาซึ่งบริการอิเล็กทรอนิกส์ในรูปแบบที่แตกต่างกันไปรวมถึงประเภทของเทคโนโลยีและอุปกรณ์ที่หลากหลายมากขึ้น บุคลากรทางการแพทย์นำเทคโนโลยีหลายด้านมาประยุกต์ใช้เพื่อให้เกิดประโยชน์สูงสุดแก่ผู้รับบริการในโรงพยาบาล เช่นการถ่ายรูปบาดแผลของผู้ป่วยและผลตรวจทางห้องปฏิบัติการให้กับสหสาขาวิชาชีพที่ร่วมดูแลผู้ป่วยผ่านทางสื่ออิเล็กทรอนิกส์ ซึ่งความสะดวก รวดเร็วจากการใช้เทคโนโลยี ทำให้บุคคลากรทางการแพทย์กระทำการละเมิดข้อมูลส่วนบุคคลของผู้รับบริการโดยไม่ตั้งใจทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลได้มากขึ้น กรณีที่เกิดขึ้นและเป็นข่าวทางสื่ออิเล็กทรอนิกส์ เช่นกรณีการเผยแพร่ภาพของดาราชายคนหนึ่งขณะที่ป่วยในระยะวิกฤติผ่านทางสื่อสังคมออนไลน์[1] ส่งผลให้โรงพยาบาลที่ทำการรักษาดาราชายคนนี้ออกประกาศเตือนไปยังบุคลากรของโรงพยาบาลห้ามโพสตร์ภาพหรือแชร์ข่าวที่เกี่ยวกับอาการป่วยของนักแสดงหนุ่มออกไปเพราะจะเป็นการละเมิดสิทธิ์ของอีกฝ่าย[2] และในระยะเวลาที่ใกล้เคียงกัน ได้มีการเผยแพร่ภาพและคลิปวิดีโอขณะที่ทำการรักษานักแสดงสาวคนหนึ่งที่ถูกหามส่งโรงพยาบาลเนื่องจากกินยานอนหลับเกินขนาด จึงเห็นได้ว่าเหตุการณ์ลักษณะนี้เกิดขึ้นได้ง่ายถือเป็นเรื่องปกติของสังคมออนไลน์ยุคปัจจุบัน หากบุคคลกรในโรงพยาบาลไม่ตระหนักถึงผลเสียที่เกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล โรงพยาบาลไม่มีบทลงโทษที่ชัดเจน ไม่

---

[1] ยกเคสแชร์ภาพป่วย “ปอ ทฤษฎี” ทำไกด์ไลน์หมอใช้โซเชียลชี้หารืออาการป่วยใน “กรุ๊ปไลน์” ได้แต่ห้ามแคปส่งต่อ, หนังสือพิมพ์ผู้จัดการออนไลน์, ค้นวันที่ 31 ธันวาคม 2562 จาก https://mgronline.com/qol/detail/9580000125416.

[2] โซเชียลช็อต"เดลินิวส์" ไร้จรรยาบรรณลงภาพ "ปอ" ป่วย "รามา" ยันชุดคนป่วยไม่ใช่ของ รพ., หนังสือพิมพ์ผู้จัดการออนไลน์, ค้นวันที่ 31 ธันวาคม 2562 จาก https://mgronline.com/onlinesection/detail/9580000125380.

มีมาตรการที่เด็ดขาดมาบังคับใช้ ส่งผลให้สิทธิส่วนบุคคลของผู้มารับบริการในโรงพยาบาลถูกละเมิดได้ง่ายขึ้นเช่นกัน

แม้ว่า “ความเป็นส่วนตัว” จะมีหลายประการ แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญอย่างมากคือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล”เนื่องจากพัฒนาการทางเทคโนโลยีสารสนเทศที่ก้าวหน้าไปอย่างรวดเร็ว พัฒนาการที่ล้ำยุคของโปรแกรมคอมพิวเตอร์ส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลต่าง ๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่อีกต่อไป ทำให้การประมวลผล จัดเก็บ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว ในทางกลับกันจึงอาจมีการนำประโยชน์ของเทคโนโลยีเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐาน โดยการคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) รัฐบาลไทยเองได้ให้ความสำคัญกับเรื่อง “ข้อมูลส่วนบุคคล” โดยมีแนวทางการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลส่วนบุคคลที่อยู่จัดเก็บในระบบของภาครัฐซึ่งก็คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และต่อมาในปี พ.ศ. 2553 ได้ออกประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลหน่วยงานภาครัฐ พ.ศ. 2553 ปัจจุบันประเทศไทยได้บัญญัติ “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” ขึ้นมาเพื่อใช้ในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน อย่างไรก็ตาม แม้ว่า “ความเป็นส่วนตัว” จะมีหลายประการ แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญ คือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล” ทั้งนี้ เพราะพัฒนาการล้ำยุคของคอมพิวเตอร์ส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลต่าง ๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่อีกต่อไป ทำให้การประมวลผล จัดเก็บ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว ในทางกลับกันจึงอาจมีการนำประโยชน์ของเทคโนโลยีเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐาน โดยการคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) ถึงแม้ว่าประเทศไทยจะมีกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ในภาพรวมอยู่บ้างแล้ว รวมถึงมีบทบัญญัติที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลด้านสุขภาพในกฎหมายด้านสุขภาพบางฉบับ เช่น พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 แต่ล้วนเป็นกฎหมายที่ประกาศใช้มานาน ส่งผลให้ไม่ครอบคลุมกับการคุ้มครองข้อมูลสุขภาพในปัจจุบัน รวมทั้งไม่มีความชัดเจนเกี่ยวกับหลักเกณฑ์และแนวทางการ

คุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพโดยเฉพาะข้อมูลส่วนบุคคลของผู้ที่มารับบริการในโรงพยาบาลเป็นข้อมูลซึ่งสามารถบ่งบอกเอกลักษณ์ ลักษณะ หรือความเป็นบุคคลคนนั้นได้ เช่น เลขรหัสประจำตัวประชาชน หมายเลขโทรศัพท์ ที่อยู่ หรือแม้แต่ข้อมูลการรักษาพยาบาล

อย่างไรก็ตามข้อมูลสุขภาพมีลักษณะพิเศษที่ต่างจากข้อมูลธุรกรรมทั่วไป โดยในบางครั้งจำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ของส่วนรวมเช่นในกรณีการเกิดโรคระบาดจำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคล เช่น โรคที่เป็น แหล่งที่อยู่อาศัย บุคคลที่อยู่ใกล้ชิด เพื่อทำการสอบสวนและกักกันโรค หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อความปลอดภัยของผู้ป่วย เช่นกรณีผู้ป่วยประสบอุบัติเหตุจำเป็นต้องส่งตัวไปรักษาที่โรงพยาบาลอื่น ในขณะที่ผู้ป่วยไม่รู้สึกตัวและไม่มีญาติมาด้วยทางโรงพยาบาลจำเป็นต้องส่งต่อข้อมูลส่วนบุคคลของผู้ป่วยเพื่อให้อีกโรงพยาบาลเตรียมรับช่วงในการรักษาพยาบาลผู้ป่วยรายนี้ต่อ ในส่วนของการเปิดเผยข้อมูลส่วนบุคคลเพื่อการพัฒนาคุณภาพของการให้บริการ (Patient Safety and Quality Improvement) ตัวอย่างเช่นการนำข้อมูลส่วนบุคคลเฉพาะด้าน คือ โรคประจำตัว อายุ ประวัติครอบครัวมาใช้ในการทำวิจัยเพื่อหาแนวทางการดูแลผู้ป่วยเฉพาะโรค นอกจากนี้ในด้านการรักษาพยาบาลบางครั้งจำเป็นจะต้องมีการแลกเปลี่ยนข้อมูลสุขภาพในกลุ่มผู้ให้การรักษาพยาบาล ซึ่งหากพิจารณาจากความหมายของข้อมูลส่วนบุคคลแล้วจะเห็นได้ว่าข้อมูลส่วนบุคคลมีความสำคัญต่อบุคคลเป็นอันมากฉะนั้น จึงมีความจำเป็นที่จะต้องบัญญัติกฎหมายเพื่อให้การรับรองและให้ความคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

ในส่วนภาครัฐของประเทศไทย ได้เตรียมการบูรณาการในหลายด้านเพื่อการพัฒนาประเทศและยกระดับความมั่นคงในการดำรงชีวิตของประชาชน ผ่านการขับเคลื่อนด้วยเทคโนโลยีสารสนเทศ ซึ่งหนึ่งในการขับเคลื่อนที่น่าสนใจนั้น เป็นการขับเคลื่อนด้านการบูรณาการระบบสุขภาพของไทยด้วย ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล หรือ Personal Health Records (PHR) ซึ่งระบบสาธารณสุขของไทยกว่าร้อยละ 7 ดำเนินการโดยภาครัฐผ่านโรงพยาบาลและสาธารณสุขชุมชนครอบคลุมพื้นที่ 77 จังหวัด มีหน่วยงานสาธารณสุขถึง 10,000 แห่ง มีบุคลากรที่เกี่ยวข้องประมาณ 330,000 คน ในอดีตนั้นการจัดเก็บระเบียนสุขภาพเป็นการเก็บรวบรวมข้อมูลในรูปแบบของเอกสารกระดาษ (Paper Document) แต่ PHR เป็นการจัดเก็บระเบียนสุขภาพส่วนบุคคลโดยใช้ระบบอิเล็กทรอนิกส์มาเป็นตัวช่วยในการเก็บและรวบรวมข้อมูลทำให้เกิดการเชื่อมโยงข้อมูลระหว่างสถานพยาบาล โรงพยาบาล และหน่วยงานที่เกี่ยวกับสาธารณสุขของประชาชนในแต่ละจังหวัด เช่น ข้อมูลพื้นฐานทั่วไป ประวัติการรักษา ประวัติการแพ้ยา รวมถึงนำเข้าข้อมูลการดูแลสุขภาพของแต่ละบุคคล การออก

กำลังกายและผลการตรวจร่างกาย เพื่อช่วยให้ประชาชนสามารถดูแลสุขภาพตนเองระหว่างรอการพบแพทย์ครั้งหน้า รวมถึงเปรียบเทียบและปฏิบัติตามคำแนะนำจากแพทย์ได้ด้วย ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลนี้ผู้ใช้บริการสามารถบริหารข้อมูลสุขภาพของตัวเองและครอบครัวอย่างเป็นระบบ สามารถติดตามและนัดพบแพทย์ผ่านทางระบบออนไลน์ได้ทันที

ด้วยเหตุนี้ผู้วิจัยจึงมุ่งทำการศึกษาว่ากฎหมายไทยมีมาตรการใดที่จะสามารถนำมาปรับใช้ในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาลที่มีการจัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลเพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับมาตรฐานที่เป็นสากล ปรับปรุงกฎหมายไทยให้เหมาะสมกับยุคที่เทคโนโลยีมีบทบาทสำคัญกับการดำเนินชีวิต

ปัญหาของการวิจัย

1. พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ยังไม่สามารถคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลตามมาตรฐานสากล

2. พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 ไม่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลเนื่องจากยังมีช่องว่างของกฎหมายให้ผู้อื่นกระทำการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลที่จัดเก็บไว้ในระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลได้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวคิดทฤษฎีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2. เพื่อศึกษาเปรียบเทียบมาตรการทางกฎหมายของไทยและต่างประเทศในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาลที่ถูกจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

3. เพื่อเสนอแนะมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

สมมติฐานของการวิจัย

การจัดเก็บข้อมูลส่วนบุคคลในระบบอิเล็กทรอนิกส์สุ่มเสี่ยงที่จะเกิดการละเมิดข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ได้ง่าย ปัจจุบันมาตรการทางกฎหมายที่บังคับใช้ในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาลที่มีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลยังไม่เพียงพอเนื่องจากยังมีช่องว่างของกฎหมายให้ผู้อื่นกระทำการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลที่จัดเก็บไว้ในระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลได้ งานวิจัยชิ้นนี้ผู้วิจัยจึงมุ่งศึกษาปัญหาดังกล่าวเพื่อเสนอแนวทางแก้ไขพัฒนากฎหมายไทยต่อไป

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีศึกษาข้อมูลจากเอกสาร (Documentary Research) เช่นตัวบทกฎหมาย ทฤษฎี บทความวิชาการ วิทยานิพนธ์ คดีที่เคยเกิดขึ้นทั้งของประเทศไทยและต่างประเทศ ตลอดจนข้อมูลที่ค้นคว้าได้จากเว็บไซต์บนอินเทอร์เน็ต ผู้วิจัยทำการศึกษาหลักเกณฑ์และมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยภายใต้พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ศึกษาเปรียบเทียบกับกรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD : The Organization for Economic Cooperation and Development) ในเรื่อง Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (Regulation (EU) 2016/679 General Data Protection Regulation –GDPR)และพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (The Health Insurance Portability and Accountability Act of 1996 – HIPAA) โดยนำมาวิเคราะห์ในประเด็นที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ เพื่อให้ทราบถึงหลักเกณฑ์ แนวทางปฏิบัติ และปัญหาเพื่อนำมาซึ่งการพัฒนากฎหมายของประเทศไทยต่อไป

ขอบเขตของการวิจัย

การวิจัยนี้เป็นการศึกษาถึงหลักเกณฑ์ แนวทางปฏิบัติ และปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยโดยเฉพาะการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาลที่มีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล (Personal Health Records –PHR) นำมาวิเคราะห์เปรียบเทียบกับ

กฎหมายต่างประเทศ ในประเด็นเกี่ยวกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคล การป้องปรามการละเมิดข้อมูลและระบบที่ใช้ในการป้องกันข้อมูลเพื่อสร้างความมั่นใจให้แก่ผู้มารับบริการในโรงพยาบาลที่มีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

นิยามศัพท์เฉพาะ

ข้อมูลส่วนบุคคล[3] หมายความว่า ข้อมูลซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าโดยทางตรงหรือทางอ้อม รวมถึงการกำหนดให้ข้อมูลส่วนบุคคลรวมถึงข้อมูลที่สามารถระบุตัวบุคคลนั้นได้แม้ว่าในเบื้องต้นจะไม่สามารถระบุตัวบุคคลได้ แต่หากในที่สุดแล้วสามารถระบุตัวบุคคลได้ก็อยู่ภายใต้บังคับของกฎหมายเช่นกัน

ผู้มารับบริการในโรงพยาบาล (ผู้ป่วย)[4] หมายความว่า ผู้ที่เข้ารับการรักษาหรือผู้รับบริการด้วยการพยาบาล จำแนกเป็น 2 ประเภทคือ

1. ผู้ป่วยใน หมายถึง ผู้ที่ต้องเข้ารับการรักษาในโรงพยาบาลหรือสถานพยาบาลอย่างน้อย 6–8 ชั่วโมง หรือผู้ที่ต้องเสียค่าห้องและค่าอาหารประจำวันในการเข้ารักษาในโรงพยาบาลและสถานพยาบาล
2. ผู้ป่วยนอก หมายถึง ผู้ที่รับการบริการหรือเวชภัณฑ์อันเนื่องมาจากการรักษาพยาบาลในแผนกผู้ป่วยนอกหรือในห้องรักษาฉุกเฉินของโรงพยาบาลและสถานพยาบาล หรือผู้ที่รับการศัลยกรรมผ่าตัดเล็ก (Minor Surgery) โดยไม่เป็นผู้ป่วยในตามนิยามผู้ป่วยใน

ระเบียนสุขภาพ[5] หมายความว่า การบันทึกข้อมูลเกี่ยวกับประวัติส่วนบุคคล ข้อมูลการรักษาพยาบาล ข้อมูลการตรวจสุขภาพ พฤติกรรมสุขภาพและผลการวิเคราะห์สุขภาพของสถานพยาบาล

ข้อมูลสุขภาพส่วนบุคคล[6] หมายความว่า เพศ อายุ น้ำหนัก ส่วนสูง รอบเอว ความดันโลหิตและผลตรวจทางห้องปฏิบัติการ เช่นผลตรวจเลือด ปัสสาวะ อุจจาระ เสมหะและน้ำไขสันหลัง รวมถึงภาพหรือเสียงที่บันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ อาทิเช่นภาพเอกซเรย์

---

[3] กลุ่มงานพัฒนากฎหมาย สำนักงานเลขาธิการวุฒิสภา, รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 (กรุงเทพฯ: ม.ป.ท., 2560).

[4] คำนิยาม, ค้นวันที่ 2 ธันวาคม 2561 จาก http://service.nso.go.th/nso/nso_center/project/table/files/S-hospital-p/2555/000/00_S-hospital-p_2555_000_000000_00002.pdf

[5] ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561, ราชกิจจานุเบกษา, ค้นวันที่ 31 ธันวาคม 2562 จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2561/E/124/1.PDF.

[6] เรื่องเดียวกัน.

หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้

ข้อมูลอิเล็กทรอนิกส์[7] หมายความว่า ข้อมูลของบุคคลที่จัดเก็บไว้ในรูปแบบอิเล็กทรอนิกส์

ระบบระเบียนสุขภาพส่วนบุคคล (Personal Health Records–PHRs)[8] หมายถึง ระบบการจัดเก็บข้อมูลสุขภาพของผู้ป่วยในรูปแบบอิเล็กทรอนิกส์ ผู้ป่วยสามารถเข้าถึง ควบคุมดูแล หรือจัดการข้อมูลของตนเองได้เอง รวมถึงแลกเปลี่ยนข้อมูลกับผู้อื่นได้ไม่ว่าข้อมูลนั้นจะมีแหล่งที่มาจากข้อมูลในระบบสารสนเทศของสถานพยาบาลโดยตรง ข้อมูลที่ได้มาจากการบันทึกของผู้ป่วยเอง หรือข้อมูลจากแหล่งอื่นก็ตาม ทั้งนี้ รวมถึงกรณีที่ผู้แทนโดยชอบธรรมเป็นผู้ใช้งานในระบบอิเล็กทรอนิกส์แทนผู้ป่วยด้วย

จากคำนิยามที่ได้กล่าวไปแล้ว คำที่เกี่ยวข้องกับการศึกษาวิจัยครั้งนี้และยังไม่มีนิยามศัพท์เฉพาะคือ ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล ในการศึกษาครั้งนี้ผู้วิจัยจึงให้คำนิยาม **ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล** หมายความว่า ข้อมูลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ โดยเป็นข้อมูลที่เกี่ยวข้องกับตัวบุคคลผู้เป็นเจ้าของข้อมูลโดยตรงหรือทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ง่าย เช่น ชื่อสกุล อายุ อาชีพ หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล์ ผลตรวจทางห้องปฏิบัติการ เช่นผลตรวจเลือด ปัสสาวะ อุจจาระ เสมหะและน้ำไขสันหลัง รวมถึงภาพหรือเสียงที่บันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้ แต่ไม่รวมถึงที่อยู่ สถานที่ทำงาน

ประโยชน์ที่จะได้รับจากการวิจัย

1. ทำให้ทราบถึงความเป็นมา แนวคิด ทฤษฎี เกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลในยุคอิเล็กทรอนิกส์ โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 เพื่อนำมาประยุกต์ใช้คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลตามมาตรฐานสากล

---

[7] เรื่องเดียวกัน.

[8] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC), **ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล–Phr**, ค้นวันที่ 2 ธันวาคม 2561 จาก https://www.nectec.or.th/innovation/innovation-software/phr.html

2. ทำให้ทราบมาตรการทางกฎหมายของไทยและต่างประเทศในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบอิเล็กทรอนิกส์ที่มีอยู่ในปัจจุบัน ในเรื่องการคุ้มครองสิทธิความเป็นส่วนตัวจากใช้ระบบอิเล็กทรอนิกส์เพื่อจัดเก็บระเบียนสุขภาพส่วนบุคคล ทั้งปัญหาในแง่เนื้อหา (Content) การปรับใช้ (Application)

3. เสนอแนะแนวทางการแก้ไข ปรับปรุง พัฒนากฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัวของผู้มารับบริการในโรงพยาบาลที่มีการลงทะเบียนในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล ให้มีความทันสมัย และ เหมาะสมกับสภาพการณ์ในสังคมปัจจุบันต่อไป

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นสิทธิมนุษยชนขั้นพื้นฐาน โดยการคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) ซึ่งเป็นบ่อเกิดและรากฐานของสิทธิมนุษยชน โดยใช้แนวคิดตามกฎหมายธรรมชาติเนื่องจากแนวคิดนี้เห็นว่าสิทธิเหล่านั้นมีอยู่แล้วตามธรรมชาติไม่ใช่เป็นสิ่งที่มนุษย์คิดสร้างขึ้นเพียงแต่มนุษย์เป็นผู้ค้นพบเท่านั้น อย่างไรก็ตามในยุคปัจจุบันเทคโนโลยีสารสนเทศถูกพัฒนาให้ก้าวหน้ามากขึ้น การเข้าถึงและการส่งต่อข้อมูลต่าง ๆ สามารถกระทำได้โดยง่าย รวดเร็วและแพร่หลาย ทำให้เกิดการล่วงละเมิดข้อมูลส่วนบุคคลเพื่อแสวงหาประโยชน์โดยมิชอบเป็นเหตุให้เจ้าข้อมูลส่วนบุคคลได้รับความเสียหาย จึงจะเห็นได้ว่ามาตรการในคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในปัจจุบันไม่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ ประเทศไทยยุคไทยแลนด์ 4.0 ให้ความสำคัญกับการบูรณาการเทคโนโลยีสารสนเทศให้เข้ามามีบทบาทในการดูแลสุขภาพของประชาชน เป็นการบูรณาการระบบสุขภาพของไทยด้วยการจัดทำระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลหรือ Personal Health Records (PHR) ด้วยเหตุนี้ผู้วิจัยจึงเกิดแนวความคิดเกี่ยวกับการหามาตรการทางกฎหมายเพื่อใช้คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลขึ้น

แนวคิดและทฤษฎีในการคุ้มครองสิทธิส่วนบุคคล

พัฒนาการทางเทคโนโลยีการสื่อสารเป็นเหตุให้บุคคลมีการติดต่อสื่อสารในช่องทางใหม่ ๆ สิทธิในความเป็นอยู่ส่วนตัวจึงมีการพัฒนาไปตามสภาพสังคม แนวคิดการเรียกร้องให้มีการคุ้มครองสิทธิส่วนตัวมีมานานกว่า 2,000 ปี โดยสิทธิดังกล่าวเป็นสิทธิตามธรรมชาติมิใช่สิทธิตามกฎหมาย ซึ่งมีผู้ให้คำอธิบายความหมายของสิทธิส่วนบุคคลไว้หลายความหมายดังนี้

Richard A. Spinello ให้ความหมายว่าสิทธิส่วนบุคคล[9] หมายถึง การจำกัดการเข้าถึงตัวปัจเจกชนโดยบุคคลอื่น ประกอบด้วยปัจจัยสำคัญ 3 ประการได้แก่

1. การเก็บรักษาความลับ หรือจำกัดมิให้ผู้อื่นรู้ข้อมูลของตนเอง
2. การปิดบังชื่อ การไม่เปิดเผยตัว หรือป้องกันมิให้ผู้อื่นทราบว่าตนเองเป็นใคร
3. การอยู่อย่างสันโดษ หรือมิให้บุคคลอื่นใกล้ชิดทางกายภาพ

ในที่ประชุมคณะกรรมการนักนิติศาสตร์สากล (International Commission of Jurists: ICJ) ในปี ค.ศ. 1967 ที่กรุงสต็อกโฮล์ม ประเทศสวีเดน ให้คำนิยามสิทธิส่วนบุคคล หมายถึง สิทธิในความเป็นส่วนตัว สิทธิที่จะอยู่โดยลำพัง มีการรบกวนหรือแทรกแซงจากบุคคลอื่นในระดับที่ต่ำที่สุด

จากที่กล่าวมาจึงสรุปได้ว่า สิทธิส่วนบุคคล หมายถึง สิทธิของปัจเจกชนที่จะดำรงชีวิตอย่างเป็นอิสระตามลำพัง ปราศจากการรุกล้ำจากบุคคลอื่นทางกายภาพ และการสิทธิส่วนบุคคลต้องไม่ขัดต่อกฎหมาย

ในประเทศอังกฤษ สมัยพระเจ้าวิลเลี่ยม[10] มีการทำบัญญัติสิทธิ์ (Bill of Rights) เพื่อเป็นหลักประกันขั้นพื้นฐานในสิทธิเสรีภาพของประชาชน 3 ด้าน คือ สิทธิในจิตสำนึก (Right of Conscience) สิทธิของบุคคลที่ถูกล่าวหาว่ากระทำความผิดทางอาญา และสิทธิในทรัพย์สิน ซึ่ง Bill of Rights ในเวลาต่อมาถูกนำไปใช้เป็นต้นแบบของกฎหมายเกี่ยวกับสิทธิส่วนบุคคลในประเทศที่เป็นอาณานิคมอังกฤษและประเทศสหรัฐอเมริกา

ส่วนการให้ความคุ้มครองสิทธิส่วนบุคคลของปวงชนชาวไทย พระมหากษัตริย์ของไทยมีประกาศ รับรู้ถึงสิทธิส่วนบุคคลของชาวไทยมาตั้งแต่สมัยสุโขทัย และพัฒนาการคุ้มครองสิทธิส่วนบุคคลอย่างค่อยเป็นค่อยไป กระทั่งวันที่ 24 มิถุนายน พ.ศ. 2475 ที่มีการเปลี่ยนแปลงการปกครองเป็นระบอบประชาธิปไตย จึงมีรัฐธรรมนูญที่รับรองถึงสิทธิสำคัญของพลเมือง สิทธิทางแพ่ง สิทธิทางเศรษฐกิจ สิทธิทางการเมืองและเริ่มมีการ รับรองสิทธิความเป็นส่วนตัวไว้อย่างชัดเจนในรัฐธรรมนูญ พ.ศ. 2540 เป็นฉบับแรก

บ่อเกิดและรากฐานของสิทธิความเป็นส่วนตัวหรือสิทธิส่วนบุคคล คือ หลักของสิทธิมนุษยชน ซึ่งหลังสงครามโลกครั้งที่สองมีการจัดตั้งสหประชาชาติและมีการยกร่างปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ตามแนวความคิดเรื่องสิทธิมนุษยชนสามารถย้อนกลับไปได้ในทุก

---

[9] ธาริณี มณีรอด, **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล** (นิติศาสตร์มหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธุรกิจบัณฑิตย์, 2559), หน้า 55.

[10] จรัญ โฆษณานันท์, **สิทธิมนุษยชนไร้พรมแดน ปรัชญา กฎหมายและความเป็นจริงทางสังคม** (กรุงเทพฯ: มหาวิทยาลัยรามคำแหง, 2545). หน้า 190.

หลักศาสนา วัฒนธรรม และปรัชญา ไม่ว่าในศาสนาฮินดู (Manu Smriti) ลัทธิขงจื๊อ อัลกุรอาน และบัญญัติสิบประการ ล้วนมีเค้าโครงเกี่ยวกับสิทธิต่าง ๆ บางประการซึ่งรวมกันเรียกว่า คำประกาศสิทธิมนุษยชนสากลสหประชาชาติ (United Nations Universal Declaration of Human Right –UDHR) ซึ่งประกอบด้วยแนวคิดเกี่ยวกับกฎธรรมชาติ การรับรองสิทธิธรรมชาติโดยไม่คำนึงถึงความแปรผันทางด้านกฎหมายและขนบจารีตของมนุษย์ ลักษณะของสิทธิมนุษยชน[11] ประกอบด้วยสิ่งต่อไปนี้ คือ 1.เป็นสิทธิพื้นฐานที่ติดตัวมาของมนุษย์ทุกคน (Primary Rights) แสดงให้เห็นว่ามนุษย์ที่เกิดมาในโลกนี้ก็มีสิทธิมนุษยชนติดตัวมาด้วยตั้งแต่เกิด 2. เป็นสิทธิที่เป็นสากล แสดงให้เห็นว่ามนุษย์ทุกคนควรมีความเท่าเทียมกันในศักดิ์ศรีของความเป็นมนุษย์ 3.เป็นสิทธิที่ไม่สามารถถ่านโอนให้กันได้ คือ 4.เป็นสิทธิที่ไม่อาจถูกแยกจากกัน คือ มนุษย์ทุกคนย่อมมีสิทธิดังกล่าวที่กล่าวมาทั้งหมดเพื่อที่จะดำรงชีวิตอยู่ต่อไปอย่างมีศักดิ์ศรี มีมาตรฐานในการดำรงชีวิตอย่างมีเสรีภาพและมีความมั่นคง เหมาะสมกับความเป็นมนุษย์ ซึ่งนอกจากลักษณะของสิทธิมนุษยชนตามคำประกาศของสิทธิมนุษยชนสากลสหประชาชาติแล้ว ยังได้แบ่งขอบเขตของสิทธิมนุษยชนออกมาได้อีก 5 ด้าน[12] คือ

1. สิทธิพลเมือง (Civil Rights) เป็นสิทธิในชีวิตและร่างกายของประชาชนในฐานะที่เป็นพลเมืองแห่งรัฐ เป็นสิทธิเกี่ยวข้องกับความเสมอภาคตามกฎหมาย เช่น ความเป็นส่วนตัว การติดต่อสื่อสาร ความเท่าเทียมทางเพศ สิทธิในการได้รับสัญชาติ สิทธิในการพิจารณาคดีอย่างอิสระของผู้พิพากษา ความเสมอภาคทางกฎหมายและไม่ถูกเลือกปฏิบัติ เป็นต้น

2. สิทธิทางการเมือง (Political Rights) เป็นสิทธิของประชาชนที่จะแสดงความคิดเห็นทางการเมืองเช่นการสมัครเป็นสมาชิกพรรคการเมือง การมีส่วนร่วมเคลื่อนไหวทางการเมือง และการลงคะแนนเสียงเลือกตั้ง เป็นต้น

3. สิทธิทางสังคม (Social Rights) เป็นสิทธิของประชาชนทางสังคมที่จะได้รับบริการจากสังคม ในฐานะที่เป็นสมาชิกของสังคม เช่น สิทธิการเข้าถึงการบริการสาธารณะ วิถีชีวิตทางสังคม การมีครอบครัว การได้รับการคุ้มครองจากรัฐเป็นต้น

4. สิทธิทางเศรษฐกิจ (Economic Rights) เป็นสิทธิของประชาชนในการทำงาน

---

[11] วไล ณ ป้อมเพชร, "สิทธิมนุษยชน/ลักษณะเฉพาะของสิทธิมนุษยชน," ใน **สารานุกรมไทยสำหรับเยาวชน** (กรุงเทพฯ: ม.ป.ท., 2551). หน้า 126.

[12] กรมคุ้มครองสิทธิและเสรีภาพ, "บทวิเคราะห์ข้อมูล สถานการณ์ และเชื่อมโยงเพื่อวางทิศทางแผนสิทธิมนุษยชนแห่งชาติ ฉบับที่ 3 (พ.ศ. 2557–2561)," คณะรัฐมนตรีและราชกิจจานุเบกษา (กรุงเทพฯ: 2556). หน้า 39.

ประกอบอาชีพเพื่อนำมาเป็นค่าใช้จ่ายในการดำรงชีวิตประจำวัน เช่นสิทธิที่จะได้รับการประกันสินค้าราคาสินค้าเกษตรอย่างเป็นธรรม สิทธิในการตั้งสหภาพหรือการนัดหยุดงาน สิทธิในการรับค่าแรงอย่างเป็นธรรมและถูกต้องตามกฎหมาย เป็นต้น

5. สิทธิทางวัฒนธรรม (Cultural Rights) เช่น สิทธิเข้าร่วมในพิธีกรรม ประเพณี สิทธิในการแต่งกายตามขนบธรรมเนียมท้องถิ่นและความเชื่อ เป็นต้น

การบัญญัติกฎหมายให้คุ้มครองตามหลักสิทธิมนุษยชนนั้นเพื่อให้เกิดความสงบสุขในสังคม เคารพในสิทธิเสรีภาพความเป็นส่วนตัวของแต่ละบุคคล แนวทางในการคุ้มครองสิทธิความเป็นส่วนตัวมี 4 แนวทาง[13]คือ

1. สิทธิความเป็นส่วนตัวที่เกี่ยวกับชื่อ เครื่องหมาย เครื่องหมายประจำตระกูล เครื่องหมาย ประจำสมาคม เครื่องแบบหรือสัญลักษณ์ เครื่องหมายการค้า ชื่อทางการค้า ตราของบริษัทและหีบห่อ สินค้า เป็นต้น

2. สิทธิความเป็นส่วนตัวที่เป็นการรบกวนทางกาย คือ สิทธิในชีวิต ร่างกาย สุขภาพอนามัย และสิทธิความเป็นส่วนตัวที่เป็นการรบกวนทางจิตใจ คือ การรบกวนความสันโดษการอยู่โดยลำพัง การมีเสรีภาพในการกระทำการงานตามใจสมัคร รวมถึงผลประโยชน์ต่าง ๆ ด้วย

3. สิทธิความเป็นส่วนตัวที่เกี่ยวกับความลับ เช่น ความลับในสุขภาพกาย สุขภาพจิต ชีวิตส่วนตัว ครอบครัว ความลับทางการค้าหรือวิชาชีพ ความเป็นอิสระในการดำรงชีวิตประจำวัน ภาพถ่าย สิทธิที่จะไม่เปิดเผยต่อสาธารณะในคำพูดสนทนาและเอกสาร เช่น สมุดบันทึกและจดหมาย เป็นต้น

4. สิทธิความเป็นส่วนตัวที่เกี่ยวกับเกียรติยศ ชื่อเสียง ศักดิ์ศรีของบุคคล หรือชื่อเสียงทาง วิชาชีพและทางการค้า

จากการศึกษาจึงสรุปได้ว่าสิทธิมนุษยชนเป็นสิทธิประจำตัวของมนุษย์ทุกคนไม่สามารถถ่ายโอนให้กันได้และต้องใช้สิทธิภายใต้ข้อบังคับของกฎหมาย แต่จากความเจริญของวิทยาศาสตร์และเทคโนโลยีส่งผลให้เกิดการละเมิดสิทธิมนุษยชนมากขึ้น จึงควรวางหลักกฎหมายในการคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลที่ชัดเจน

---

[13] อธิพร สิทธิธีรรัตน์, **ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์** (วิทยานิพนธ์มหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ: 2555), หน้า 35.

หลักการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายของแต่ละประเทศจะมีบทบัญญัติในการคุ้มครองความเป็นส่วนตัวที่แตกต่างกันไปทั้งนี้ต้องยึดหลักการเห็นประโยชน์ของสาธารณะมากกว่าเพื่อประโยชน์ส่วนบุคคล สิทธิความเป็นส่วนตัวเกี่ยวกับความลับหรือจะเรียกว่าสิทธิด้านข้อมูลส่วนบุคคลตามหลักของสิทธิมนุษยชนซึ่งอยู่ในหลักการพื้นฐานของกฎหมายที่ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลได้แก่ กรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development– OECD) ในเรื่อง Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ซึ่งให้ความสำคัญกับ “หลักการยินยอม” และ “หลักการปกปิด” เป็นหลักการทั่วไป “การเปิดเผย”[14] เป็นข้อยกเว้น โดยมีหลักการสำคัญอยู่ 9 ประการ ได้แก่[15]

1. หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle) หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดเท่าที่จำเป็นเท่านั้น และการเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย นอกจากนี้ต้องกระทำภายใต้ความรับรู้และความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลด้วย

2. หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน (Data Quality and Proportional Principle) หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลที่จะทำการประมวลผลนั้นต้องมีความเกี่ยวข้อง ได้สัดส่วนหรือเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ข้อมูลส่วนบุคคลนั้นต้องถูกต้องสมบูรณ์และปรับปรุงให้ทันสมัยอยู่ตลอดเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลจะประมวลผลและใช้ข้อมูลส่วนบุคคลนั้น อย่างไรก็ดีหลักการนี้ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจัดเก็บและประมวลผลข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) เช่น ข้อมูลเกี่ยวกับชาติกำเนิด ศาสนา หรือความเชื่อทางปรัชญา เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน

3. หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล (Purpose Specification Principle) กำหนดให้ต้องมีการระบุวัตถุประสงค์ในการประมวลผล ข้อมูลส่วนบุคคลก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคล

---

[14] คณาธิป ทองรวีวงศ์, "The Oecd Privacy Framework " ใน **รายงานวิจัยฉบับสมบูรณ์ เรื่อง การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน** (กรุงเทพฯ: ม.ป.ท.). หน้า 43-44.

[15] จันทจิรา เอี่ยมมยุรา, "แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย," **วารสารนิติศาสตร์** มหาวิทยาลัยธรรมศาสตร์ ปีที่34, ฉบับที่4 (2547). หน้า 653-657.

ภายหลังสามารถกระทำได้หากเป็นเพียงเพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ อย่างไรก็ตามหากมีการเปลี่ยนแปลงวัตถุประสงค์ผู้ควบคุมข้อมูล ส่วนบุคคลต้องระบุวัตถุประสงค์ที่เปลี่ยนแปลงไปนั้นทุกครั้ง นอกจากนี้การเก็บและใช้ข้อมูลส่วนบุคคลนั้นต้องไม่เกินกว่าระยะเวลาที่จำเป็นเพื่อให้วัตถุประสงค์ที่ได้แจ้งไว้สำเร็จลุล่วง

4. หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle) หลักการนี้ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยหรือทำให้สามารถเข้าถึงได้หรือนำข้อมูลส่วนบุคคลไปใช้เพื่อการอย่างอื่นนอกจากจากวัตถุประสงค์อื่นซึ่งไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้อำนาจตามบทบัญญัติของกฎหมายเพื่อความมั่นคงของประเทศ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อการปฏิบัติตามกฎหมาย หรือเพื่อประโยชน์มหาชนอื่น ๆ นอกจากนี้ยังกำหนดให้บุคคลใดซึ่งมิใช่ผู้จัดเก็บข้อมูลส่วนบุคคลจะนำข้อมูลส่วนบุคคลนั้นไปเปิดเผยโดยเจ้าของมิได้ยินยอมมิได้ แม้ทั้งการเปิดเผยนั้นจะมิได้ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลเลยก็ตาม นอกจากนี้เมื่อเจ้าของข้อมูลส่วนบุคคลอนุญาตให้มีการเปิดเผยข้อมูลแล้ว เจ้าของข้อมูลส่วนบุคคลนั้นยังมีสิทธิในการเพิกถอนความยินยอมเพื่อยุติการเผยแพร่ข้อมูลส่วนบุคคลนั้นได้ตลอดเวลา

5. หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguard Principle) หลักการนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการป้องกันรักษาความปลอดภัยของข้อมูลเพื่อมิให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ถูกทำลาย มีการใช้หรือเปลี่ยนแปลงแก้ไขหรือมีการเปิดเผยข้อมูลโดยบุคคลซึ่งปราศจากอำนาจ

6. หลักเปิดเผยโปร่งใส (Openness Principle) หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงวัตถุประสงค์การจัดเก็บหรือการรวบรวมข้อมูลส่วนบุคคล หรือการนำข้อมูลส่วนบุคคลนั้นไปใช้ ในการประมวลผลข้อมูลส่วนบุคคลต้องสามารถแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ ข้อมูลส่วนบุคคล รวมทั้งชื่อและสถานที่ตั้งของนายทะเบียนผู้ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle) หลักการดังกล่าวกำหนดสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคล ดังต่อไปนี้

7.1 ได้รับแจ้งหรือยืนยันจากนายทะเบียนว่าได้ทำการประมวลผล ใช้ หรือโอนข้อมูลส่วนบุคคลของตนหรือไม่

7.2 ได้รับการติดต่อจากนายทะเบียนเกี่ยวกับข้อมูลส่วนบุคคลของตน

7.2.1 ภายในเวลาอันสมควร

7.2.2 อาจมีค่าใช้จ่ายได้แต่ต้องไม่เกินสมควร

7.2.3 โดยวิธีที่เหมาะสม

7.2.4 โดยรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจได้

7.3 ได้รับเหตุผลเมื่อคำร้องตามข้อ 7.1 และ 7.2 ถูกปฏิเสธและมีสิทธิในการอุทธรณ์การปฏิเสธนั้น

7.4 คัดค้านการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับตน และ หากการโต้แย้งนั้นรับฟังได้มีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล ปรับปรุง แก้ไขเพิ่มเติมเพื่อให้ข้อมูลส่วนบุคคลนั้นถูกต้องและสมบูรณ์

8. หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน (Restriction on Onward Opposition) หลักการดังกล่าวมีวัตถุประสงค์เพื่อป้องกันมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับที่อยู่ในประเทศซึ่งปราศจากกฎหมายและวิธีปฏิบัติที่สามารถเป็นหลักประกันการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมี สัญญาส่งโอนข้อมูลส่วนบุคคลระหว่างกันที่ให้หลักประกันอย่างเพียงพอ

9. หลักความรับผิดชอบของนายทะเบียน (Accountability Principle) ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการที่ (1) ถึง (8) อย่างเคร่งครัด หากฝ่าฝืนหลักการดังกล่าวและก่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ควบคุม ข้อมูลส่วนบุคคลต้องรับผิดทั้งในทางแพ่งและทางอาญา และรับผิดในค่าใช้จ่ายเพื่อแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง รวมไปถึงต้องลบหรือทำลายข้อมูลส่วนบุคคลอีกด้วย

หลักการดังกล่าวคือหลักการเบื้องต้นของการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลขยายความคำนิยามออกได้เป็น ข้อมูลและข้อมูลส่วนบุคคล

นิยามของข้อมูลและข้อมูลส่วนบุคคล

ข้อมูล เป็นกลุ่มอักขระไม่ว่าตัวเลข ตัวอักษร รูปภาพ เสียงหรือสัญลักษณ์ใด ๆ ที่นำมา รวมกันแล้วก่อให้เกิดความหมายอย่างใดอย่างหนึ่งอันเป็นข้อเท็จจริง[16]หรือเรื่องราวที่

[16] พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554, ค้นวันที่ 3 ธันวาคม 2561 จาก http://www.royin.go.th/dictionary/.

เกี่ยวข้องกับสิ่งต่าง ๆ เช่น คน สิ่งของ สัตว์ ข้อมูลเป็นรูปแบบที่ใช้สำหรับการสื่อสาร[17] การแปลความหมายและการ ประมวลผลข้อมูล โดยการประมวลผลนั้นอาจทำได้จากการสังเกต การรวบรวม การวัด หรือการ ประมวลผลโดยคอมพิวเตอร์ เป็นต้น หากแบ่งตามสภาพของข้อมูลที่เกี่ยวข้องกับกลุ่มตัวอย่าง สามารถแบ่งออกได้เป็น 3 ประเภท[18] คือ ข้อมูลส่วนบุคคล (Personal Data) ข้อมูลสิ่งแวดล้อม (Environmental Data) และข้อมูลพฤติกรรม (Behavioral Data) ซึ่งในงานวิจัยนี้ขอกล่าวถึงเฉพาะข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Information / Personal Data) เป็นคำที่มีความหมายกว้างและหลากหลาย กฎหมายของแต่ละประเทศต่างให้คำนิยามที่แตกต่างกันออกไป ผู้วิจัยจึงขอยกตัวอย่างคำนิยามที่ปรากฏในกฎหมายที่ทำการศึกษา ดังนี้

ความหมายตามกรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ ให้นิยามว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องเฉพาะตัวบุคคลหรือสามารถชี้ถึงลักษณะเฉพาะส่วนบุคคลของเจ้าของข้อมูลได้ (Individual)[19]

ความหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ให้นิยามว่า ข้อมูลส่วนบุคคล (Personal Information) หมายถึง ข้อความ (Information) ใด ๆ ที่เกี่ยวกับบุคคลธรรมดา (Natural Person) อันระบุตัว (Identified) หรือ อาจระบุตัว (Identifiable) บุคคลนั้นได้ บุคคลที่อาจถูกระบุตัวโดยทางตรงหรือทางอ้อมนี้อาจจะทำได้โดยการอ้างอิงจากหมายเลขประจำตัวเฉพาะบุคคล (Identification Number) หรือจากปัจจัยอื่น ๆ ที่มีลักษณะเฉพาะทั้งในทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจรวมถึงเอกลักษณทางวัฒนธรรมและสังคมของบุคคลนั้น[20] ดังนั้น ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ข้อมูลส่วนบุคคลที่ถูกทำให่ม่ (De-identified) ข้อมูลที่ถูกเข้ารหัส (Encrypted) หรือการใช้นามแฝง (Pseudonym zed) แต่สามารถประมวลผลและระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ ก็ยังอยู่ในบทนิยามของคำว่าข้อมูลส่วนบุคคล[21]

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้นิยามว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายถึง ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัว เช่น การศึกษา ฐานะการเงิน ประวัติ

---

[17] พลพร ปิยวรรณ และสุภาพร เชิงเอี่ยม, "**ระบบสารสนเทศเพื่อการจัดการ**," (กรุงเทพฯ: ออฟเซ็ทพลัส, 2555). หน้า 13.

[18] ณาตยา ฉาบนาค, **ระบบสารสนเทศเพื่อการสื่อสาร**, (กรุงเทพฯ: เอส.พี.ซี.บุ๊คส, 2548), หน้า 118.

[19] GENERAL DEFINITIONS PART ONE (b) Organization for Economic Co-operation and Development.

[20] Article 4 General Data Protection Regulation.

[21] **The Eu General Data Protection Regulation (Gdpr) Is the Most Important Change in Data Privacy Regulation in 20 Years.**, Date cited 2 july 2018 Available from: https://eugdpr.org/the-regulation/.

สุขภาพ ประวัติ อาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะ อื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่นลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้ว[22]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ความหมาย “ข้อมูลส่วนบุคคล” ว่าเป็นข้อมูลเกี่ยวกับตัวบุคคลซึ่งจะทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น การศึกษา ฐานะการเงินประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงานหรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่น ที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[23]

จากการศึกษาพบว่าคำนิยามของ “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความคล้ายกันคือประกอบด้วย 2 องค์ประกอบด้วยกัน ได้แก่ข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัว และข้อมูลที่สามารถทำให้ระบุตัวบุคคลได้ แต่ก็มีข้อแตกต่างให้เห็นอยู่ 2 ประการคือ ประการแรกการใช้ชื่อเรียกต่างกันคือ “ข้อมูลข่าวสารสวนบุคคล” ในพระราชบัญญัติข้อมูลข่าวสารของราชการ กับ “ข้อมูลสวนบุคคล” ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประการที่สองการยกตัวอย่างของข้อมูลสวนบุคคล ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพิ่มตัวอย่างของประวัติกิจกรรมในขณะที่พระราชบัญญัติข้อมูลข่าวสารของราชการไม่ได้ระบุเรื่องนี้ จากการศึกษาจะเห็นได้ว่าขอบเขตของข้อมูลส่วนบุคคลตามกฎหมายไทยให้นิยามค่อนข้างแคบโดยเน้นเฉพาะข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัวบุคคลเท่านั้นซึ่งจะแตกต่างจากคำนิยาม “ข้อมูลส่วนบุคคล” ในกฎหมายต่างประเทศที่กำหนดให้ “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าโดยทางตรงหรือทางอ้อม รวมถึงการกำหนดให้ข้อมูลส่วนบุคคลรวมถึงข้อมูลที่สามารถระบุตัวบุคคลนั้นได้แม้ว่าในเบื้องต้นจะไม่สามารถระบุตัวบุคคลได้ แต่หากในที่สุดแล้วสามารถระบุตัวบุคคลได้ก็อยู่ภายใต้บังคับของกฎหมายเหมือนกัน แต่ในการศึกษาครั้งนี้ผู้วิจัยสนใจศึกษา ข้อมูลส่วนบุคคลของผู้ที่มารับบริการในโรงพยาบาลและได้จัดเก็บข้อมูลทั้งหมดไว้ในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลซึ่งในบางครั้งจะถูกเรียกว่าข้อมูลส่วนบุคคลด้านสุขภาพ

---

[22] **พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540**, ค้นวันที่ 2 เมษายน 2562 จาก http://www.dla.go.th/upload/service/2554/6/21.pdf.

[23] มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

ข้อมูลส่วนบุคคลด้านสุขภาพ (Personal Health Information) หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงรวมถึงการบันทึกข้อมูลโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด[24]

ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อมูลด้านสุขภาพของบุคคลที่เป็นเอกสารหรือข้อความในรูปแบบอิเล็กทรอนิกส์[25]

ดังนั้นจากการศึกษาผู้วิจัยจึงให้นิยาม **ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล** โดยยึดตามความหมายของคำว่า"ข้อมูลส่วนบุคคลด้านสุขภาพ"และ"ข้อมูลอิเล็กทรอนิกส์" ตามระเบียบระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 หมายถึง ข้อมูลของผู้มารับบริการในโรงพยาบาลและถูกจัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล โดยเป็นข้อมูลที่เกี่ยวข้องกับตัวบุคคลผู้เป็นเจ้าของข้อมูลโดยตรงหรือทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ง่าย เช่น ชื่อสกุล อายุ อาชีพ หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล์ ผลตรวจทางห้องปฏิบัติการ เช่น ผลตรวจเลือด ปัสสาวะ อุจจาระ เสมหะและน้ำไขสันหลัง รวมถึงภาพหรือเสียงที่บันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้ แต่ไม่รวมถึงที่อยู่ สถานที่ทำงาน ตัวอย่างของข้อมูลส่วนบุคคลด้านสุขภาพในโรงพยาบาล คือ เวชระเบียนหรือบันทึกการรักษาพยาบาล

การให้นิยามความหมายของข้อมูลส่วนบุคคล ความสำคัญของการใช้หรือเปิดเผยข้อมูลส่วนบุคคลแต่ละคนก็ส่งผลกระทบต่อเจ้าของข้อมูลที่ต่างกันออกไปตามประเภทของข้อมูลโดยแบ่งข้อมูลส่วนบุคคลออกเป็น 2 ประเภท[26]คือ ข้อมูลทั่วไป (Non-sensitive Data)และข้อมูลที่มีความอ่อนไหว (Sensitive Data) โดยข้อมูลทั้ง 2 ประเภทแตกต่างกันดังนี้ ข้อมูลทั่วไป ได้แก่ ชื่อสกุล อายุ การศึกษา สถานที่ทำงานหรือลักษณะทางกายภาพของข้อมูลที่บ่งบอกถึงลักษณะเฉพาะของเจ้าของข้อมูล ซึ่งข้อมูลเหล่านี้สามารถเปิดเผยต่อสาธารณชนได้ ต่างจากข้อมูลที่มีความอ่อนไหว ข้อมูลประเภทนี้หากเปิดเผยอาจกระทบต่อความรู้สึกของเจ้าของ

---

[24] ข้อ 4 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[25] เรื่องเดียวกัน.

[26] ศิริกุล ภู่พันธ์, **ข้อความคิดว่าด้วยข้อมูลส่วนบุคคล**, (กรุงเทพฯ: พีเพรส, 2548). หน้า 83.

ข้อมูล หรือต่อประชาชนทั่วไปและอาจก่อให้เกิดอันตรายต่อบุคคลได้ เช่นเชื้อชาติ ความคิดเห็นทางการเมืองและข้อมูลสุขภาพ

จากการทบทวนวรรณกรรมมีผู้ที่ทำการศึกษาและแบ่งประเภทของข้อมูลในประเด็นที่อ่อนไหวและส่งผลกระทบต่อเจ้าของข้อมูลหากมีการเปิดเผยข้อมูลส่วนบุคคลเป็น 3 ระดับ ดังนี้[27]

1. ข้อมูลที่มีความอ่อนไหวระดับต่ำ (Low Sensitivity) เป็นข้อมูลเกี่ยวกับตัวบุคคล เช่นประวัติการทำงาน การออกจากงาน ซึ่งข้อมูลนี้ทำให้นายจ้างใหม่เข้าถึงข้อมูลที่มีความอ่อนไหวระดับสูงกว่านี้ได้

2. ข้อมูลที่มีความอ่อนไหวระดับกลาง (Moderate Sensitivity) เป็นข้อมูลเกี่ยวกับการแสดงความคิดเห็นของบุคคล อาจก่อให้เกิดความเสียหายได้เมื่อข้อมูลถูกนำไปใช้ในทางมิควร ข้อมูลประเภทนี้จึงไม่ควรเก็บรวบรวมหรือบันทึกไว้

3. ข้อมูลที่มีความอ่อนไหวระดับสูง (High Sensitivity) เป็นข้อมูลเกี่ยวกับรายละเอียดส่วนตัวทั้งหมด เช่น พฤติกรรมทางเพศ ประวัติการรักษาพยาบาล หรือข้อมูลที่เจ้าของข้อมูลจัดให้เป็นเรื่องส่วนตัว ข้อมูลที่มีความอ่อนไหวระดับสูงจึงเป็นข้อมูลที่ไม่ควรมีการเก็บรวบรวมหรือบันทึก เช่นกัน

จากการแบ่งระดับของข้อมูลอ่อนไหวดังกล่าว พบว่าประวัติการรักษาหรือเวชระเบียนเป็นข้อมูลที่มีความอ่อนไหวระดับสูง ดังนั้นข้อมูลสุขภาพที่จัดเก็บบันทึกในเวชระเบียนหรือบันทึกทางการรักษาพยาบาล ไม่ว่าจะบันทึกเป็นรูปแบบเอกสารหรือจัดเก็บในระบบอิเล็กทรอนิกส์จึงเป็นข้อมูลที่มีความอ่อนไหวระดับสูง ต้องได้รับความคุ้มครองในระดับสูงเช่นกัน หลักการคุ้มครองข้อมูลส่วนบุคคลทั้งหมดที่กล่าวมาเมื่อจะนำมาบังคับใช้เป็นกฎหมายต้องยึดหลักความยินยอมประกอบด้วย

หลักความยินยอม

ความยินยอมคือ การแสดงเจตนาของผู้เสียหายหรือผู้มีอำนาจกระทำการแทนผู้เสียหายที่จะเป็นการยินยอมให้ผู้อื่นมาก่อให้ เกิดความเสียหายแก่ชีวิต ร่างกาย อนามัย เสรีภาพ ทรัพย์สินหรือสิทธิอื่นใดของผู้เสียหาย ในต่างประเทศที่เป็นต้นแบบของระบบกฎหมาย Civil Law และ Common Law อย่างประเทศสหพันธรัฐเยอรมนี และอังกฤษได้นำหลัก “Volenti non

---

[27] ธาริณี มณีรอด, **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล**, หน้า 55.

Fit Injuria (หลักความยินยอมไม่เป็นละเมิด)"[28] มาใช้เป็นหลักเกณฑ์ในการรับผิดทางละเมิด โดยประเทศสหพันธรัฐเยอรมนี นำหลักความยินยอมไม่เป็นละเมิด ไปใช้เป็น 3 แนวทาง[29] คือ

1. เมื่อผู้เสียหายให้ความยินยอมในการทำละเมิดซึ่งเป็นการกระทำที่ผิดกฎหมายแล้ว การกระทำที่เกิดจากความยินยอมจึงเป็นการกระทำที่ไม่ผิดกฎหมายแต่ต้องคำนึงถึงความสงบเรียบร้อยและศีลธรรม อันดีของประชาชนด้วย

2. เมื่อผู้เสียหายให้ความยินยอมในการทำละเมิดแล้วถือได้ว่าผู้เสียหายประสงค์ให้ความเสียหาย เกิดขึ้นแก่ตน และเมื่อผู้เสียหายต้องการเช่นนั้นจะถือว่ามีความเสียหายเกิดขึ้นมิได้ซึ่งผู้ที่จะได้รับความ เสียหายอันจะใช้สิทธิเรียกร้องค่าสินไหมทดแทนมีแต่เฉพาะตัวผู้ให้ความยินยอมเท่านั้นประชาชนหรือสังคม ไม่อาจใช้สิทธิดังกล่าวได้จึงไม่ต้องนำเรื่องความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนมาพิจารณา

3. ถ้าผู้เสียหายได้ให้ความยินยอมในทางแพ่งแล้วจำเลยสามารถอ้างความยินยอมของผู้เสียหายขึ้นและปฏิเสธความรับผิดของตนได้โดยไม่ต้องคำนึงถึงความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนถือว่าเป็นความต้องการของผู้เสียหายเอง ลักษณะทางกฎหมายของหลักความยินยอมประกอบด้วย[30]

3.1 ผู้ให้ความยินยอมซึ่งเป็นผู้ได้รับความเสียหายต้องเป็นผู้มีความสามารถในการให้ความยินยอม คือเข้าใจหยั่งรู้ถึงการกระทำนั้น (Raise able) และรู้คุณค่าของการกระทำว่าดีหรือไม่ เข้าใจถึงธรรมชาติของการกระทำและผลที่อาจเกิดขึ้นจากการกระทำนั้นได้และต้องรู้ถึงคุณค่าของการกระทำนั้นจากประสบการณ์ ของตนเอง ซึ่งจะต้องเป็นผู้ใหญ่พอสมควร (Maturity)

3.2 วิธีการให้ความยินยอม กฎหมายมิได้กำหนดแบบไว้จึงอาจให้โดยแจ้งชัดหรือโดยปริยาย และการนิ่งถือว่าเป็นการให้ความยินยอมได้ถ้าตามพฤติการณ์ทำให้บุคคลทั่วไปเข้าใจว่าเป็นการให้ความยินยอม

3.3 เงื่อนไขความสมบูรณ์ของความยินยอม พิจารณาจาก

3.3.1 ระยะเวลาการให้ความยินยอมจะต้องมีอยู่ก่อนหรืออย่างน้อยต้องมีในขณะกระทำและมีอยู่ตลอดการกระทำ

---

[28] **สุพัชรินทร์ อัศวธิตานนท์, พัฒนาการของหลักกฎหมาย Volenti Non Fit Injuria: ศึกษาการปรับใช้กับประเทศไทย** (นิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2551), หน้า 62.

[29] เรื่องเดียวกัน หน้า 68.

[30] กมลชัย รัตนสกาววงศ์, **ความยินยอมในกฎหมายอาญา** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2523), หน้า 22-46.

3.3.2 ความยินยอมต้องให้แก่ผู้กระทำโดยตรง

3.3.3 การให้ความยินยอมต้องเป็นไปโดยชอบด้วยกฎหมาย โดยความสมัครใจปราศจากการทำกลฉ้อฉล หลอกลวง ข่มขู่ หรือสำคัญผิด

3.3.4 การให้ความยินยอมต่อสิ่งหนึ่งไม่หมายความรวมถึงสิ่งอื่นที่เพิ่มหรือแตกต่างไปจากที่ผู้เสียหายให้ความยินยอมหรือโดยผู้เสียหายไม่ทราบถึง

3.3.5 ความยินยอมต้องไม่มีเงื่อนไข

3.3.6 ผู้กระทำต้องทราบถึงความยินยอมและได้กระทำด้วยความยินยอมในความผิดที่อ้างความยินยอมได้ในกรณีที่ผู้กระทำไม่ทราบความยินยอมของผู้เสียหายและได้กระทำความผิดตามที่กฎหมายบัญญัติ ผู้กระทำไม่อาจอ้างความยินยอมที่ตนไม่ทราบเป็นข้ออ้างได้

3.4 ผลของความยินยอม เมื่อการให้ความยินยอมได้กระทำโดยผู้ให้ความยินยอมที่ถูกต้องตาม กฎหมาย และใช้วิธีการให้ความยินยอมตลอดจนเงื่อนไขความสมบูรณ์ของความยินยอมถูกต้องครบถ้วน ตามหลักความยินยอมที่ได้กล่าวในตอนต้นแล้ว ย่อมทำให้ผลของความยินยอมเป็นไปโดยสมบูรณ์ซึ่งผู้กระทำสามารถอ้างหลักความยินยอมไม่เป็นละเมิดได้

3.5 ข้อยกเว้นหลักความยินยอมไม่เป็นละเมิด อาจมีในกรณีที่เกิดการประทุษกรรมโดยไม่ได้รับ ความยินยอม แต่ผู้กระทำไม่ต้องรับผิด ได้แก่

3.5.1 กรณีมีเหตุฉุกเฉินเกิดขึ้นอย่างแท้จริงและแจ้งชัด จำเป็นต้องกระทำก่อนได้รับความ ยินยอม เช่น การจับคนที่จะฆ่าตัวตายด้วยการกระโดดจากที่สูง โดยมัดมือมัดเท้าขังไว้ในห้อง

3.5.2 ในกรณีเช่นนั้นวิญญูชนย่อมให้ความยินยอมเช่นมีคนโยนระเบิดเข้ามาและระเบิดกำลัง จะระเบิดจึงผลักผู้ซึ่งอยู่ข้างๆ ให้ล้มเพื่อหลบแรงระเบิด และการผลักทำให้ผู้นั้นได้รับบาดเจ็บ ไม่ต้องรับผิด

3.5.3 ผู้กระทำไม่รู้หรือไม่มีเหตุควรรู้ว่าผู้ถูกกระทำจะไม่ให้ความยินยอมถ้ามีโอกาสถามบุคคลนั้น เช่น แพทย์นำคนเจ็บซึ่งสลบจากอุบัติเหตุเข้าทำการผ่าตัดเพื่อช่วยชีวิต

จากการศึกษาครั้งนี้พบว่า วิธีการให้ความยินยอม กฎหมายมิได้กำหนดรูปแบบไว้โดยชัดแจ้ง ความยินยอมอาจแสดงออกโดยการขานรับ ลงลายมือชื่อเป็นลายลักษณ์อักษร พยักหน้า ยกมือหรือการนิ่งถือว่าเป็นการให้ความยินยอมได้ สอดคล้องกับการให้ความยินยอมทางการแพทย์ ด้วยเหตุจำเป็นเพื่อช่วยชีวิต ความยินยอมอาจเกิดจากการแจ้งความจำเป็นในการตรวจรักษาให้ผู้ป่วยรับทราบโดยไม่มีการตอบรับ

ความยินยอมทางการแพทย์นั้นอาศัยแนวความคิดแบบมนุษยนิยมซึ่งเชื่อว่ามนุษย์ทุกคนย่อมมีสิทธิที่จะตัดสินใจว่าจะอนุญาตหรือ ไม่อนุญาตให้ผู้อื่นมากระทำต่อร่างกายของตน ถึงแม้ว่าการกระทำนั้นจะเป็นประโยชน์ต่อตนเอง ทำให้ “**หลักความยินยอมที่ได้รับการบอกกล่าว (Informed Consent)** กลายเป็นหลักจริยศาสตร์ทางการแพทย์ที่ได้รับการยอมรับในหมู่แพทย์และนักวิจัย อย่างกว้างขวางตั้งแต่ต้นศตวรรษที่ 20 เป็นต้นมา[31] หลักการของการให้ความยินยอมทางการรักษาพยาบาลนั้น ผู้รักษาหรือแพทย์ก็ต้องขออนุญาตผู้ป่วยก่อนจะทำการตรวจและรักษาและต้องให้ผู้ป่วยยินยอมที่จะให้ทำการนั้น ๆ ทุกครั้งจึงเรียกว่า “ความยินยอมที่ได้รับการบอกกล่าว”

องค์ประกอบของความยินยอมที่ได้รับการบอกกล่าว ความยินยอมที่ได้รับตามหลักความยินยอมที่ได้รับการบอกกล่าวจะสมบูรณ์ได้ต้องประกอบด้วย 5 องค์ประกอบดังนี้[32]

1. การเปิดเผยข้อมูล (Disclosure) การแจ้งข้อมูล เพื่อขอความยินยอมนั้นควรประกอบไปด้วย ข้อมูลเกี่ยวกับการวินิจฉัย (Diagnosis) ข้อมูลเกี่ยวกับขั้นตอนการรักษา (Procedure) ข้อมูลเกี่ยวกับความเสี่ยงที่อาจเกิดจากการ รักษาเมื่อเทียบกับประโยชน์ที่จะได้รับ (Risk and benefit) ข้อมูลเกี่ยวกับทางเลือกการรักษาอื่น (Alternative Treatment)

2. ความเข้าใจข้อมูล (Understanding) เพื่อให้ผู้ป่วยสามารถใช้สิทธิของตนได้เต็มที่ แพทย์หรือผู้ให้ข้อมูล ควรมั่นใจว่าผู้ป่วยมีความเข้าใจในข้อมูลที่ตนได้ให้ไป โดยการสร้างบรรยากาศที่เหมาะสมแก่การให้ข้อมูลและข้อแนะนำ เช่น การจัดสภาพแวดล้อมให้ผู้ป่วยผ่อนคลายและสามารถซักถาม ข้อสงสัยที่เกี่ยวข้องกับการตรวจวินิจฉัยและการรักษา รวมทั้งกำจัดข้อบกพร่องที่อาจเกิดจากการสื่อสารออกไป เช่น การใช้ล่ามที่เข้าใจภาษาของทั้งแพทย์และผู้ป่วย

3. ความสมัครใจ (Voluntariness) ถึงแม้ผู้ป่วย จะเข้าใจเนื้อหาสาระของการตรวจวินิจฉัยและการรักษาแล้ว ผู้ป่วยก็ต้องไม่อยู่ภายใต้การถูกบังคับหรือขู่เข็ญด้วยเงื่อนไขต่าง ๆ ที่จะทำให้การตัดสินใจไม่เป็นไปตามที่ตนต้องการไม่ว่าจะเป็นจากแพทย์หรือจากบุคคลภายนอก เช่น ญาติ นายจ้าง หรือผู้ออกค่ารักษาพยาบาล ในกรณีที่มีความขัดแย้งเกิดขึ้น แพทย์ควรเปิดโอกาสให้ผู้ป่วยได้ ตัดสินใจในขณะบุคคลภายนอกไม่อยู่ในห้องตรวจ

4. การพิจารณาถึงความสามารถในการตัดสินใจของผู้ป่วย ต้องพิจารณาเป็นเรื่อง ๆ หรือเรียกได้ว่าการพิจารณาความสามารถในการตัดสินใจนั้นมีลักษณะจำเพาะต่อเนื้อหาเฉพาะอย่าง หรือ เนื้อหาที่เฉพาะเจาะจง กลุ่มผู้ป่วยที่ไม่สามารถแสดงเจตนาให้ความยินยอม

---

[31] ศักดา สถิรเรืองชัย, "การรักษาความลับของผู้ป่วย," เวชบันทึกศิริราช ปีที่6 ฉบับที่2 (2556). หน้า 76-81.

[32] เรื่องเดียวกัน. หน้า 73.

ได้แก่ กลุ่มผู้ป่วยที่เป็นคนไร้ความสามารถ (incompetent person) ผู้เสมือนไร้ความสามารถ และผู้เยาว์(minor) ซึ่งจะกล่าวถึงรายละเอียดในส่วนของข้อยกเว้นของหลักความยินยอม

5. การให้ความยินยอม (Consent) หลังจากผู้ป่วยได้รับทราบข้อมูลทางการแพทย์และได้ตัดสินใจแล้ว การให้ความยินยอมจะมีผลเมื่อมีการแสดงออกซึ่งความยินยอมนั้น โดยอาจจะออกมาในรูปแบบที่ชัดแจ้ง (explicit) ไม่ว่าจะเป็นการบอกด้วยปากเปล่าหรือการเขียน หรือโดยปริยาย (implied) เช่น การยอมให้แพทย์ ตรวจโดยการนอนบนเตียง การยื่นแขนให้ทำการเจาะเลือด พึงสังเกตว่าขั้นตอนการให้ความยินยอมนั้นเป็นเพียงส่วนหนึ่งของความยินยอมที่ได้รับการบอกกล่าว ไม่ได้เป็นสาระสำคัญถึงแม้ผู้ป่วยจะได้ลงลายมือชื่อในเอกสารให้ความยินยอมในการตรวจหรือรักษา แต่ผู้ป่วยไม่ได้รับทราบข้อมูลเกี่ยวการให้บริการเสมือนว่าความยินยอมที่ได้มานั้นบกพร่องไม่ครบองค์ประกอบของความยินยอมที่ได้รับการบอกกล่าว

ข้อยกเว้นของหลักความยินยอมที่ได้รับการบอกกล่าว มีบางกรณีที่แพทย์สามารถทำ การรักษาพยาบาลผู้ป่วยได้โดยไม่ต้องขอความยินยอมและไม่ เป็นการผิดจริยธรรมในการประกอบวิชาชีพเวชกรรม ซึ่งเหตุที่จะทำให้แพทย์ไม่ต้องปฏิบัติตามหลักความยินยอม ที่ได้รับการบอกกล่าวมักเป็นเรื่องประโยชน์ที่เหนือกว่าการรับรู้ของแต่ละบุคคลเช่น ประโยชน์ที่จะเกิดกับสาธารณชนในกรณีของผู้ป่วยจิตเวชที่มีภาวะอันตรายหรือ ในกรณีที่แพทย์ไม่สามารถดำเนินการขอความยินยอมได้เนื่องจากผู้ป่วยไม่มีความสามารถในการให้ความยินยอม เช่น ผู้ป่วยอยู่ในภาวะฉุกเฉินหรือเร่งด่วนและไม่รู้สึกตัวในกรณีเหล่านี้แพทย์จำต้องให้การรักษาพยาบาลผู้ป่วยก่อนตามหลักการเกื้อกูลหรือยึดประโยชน์สูงสุดของผู้ป่วยเป็นหลัก (Beneficence)[33]

ในกรณีที่ไม่เร่งด่วนและผู้ป่วยยังไม่มีความสามารถในการให้ความยินยอมได้แก่ ผู้เยาว์ (Minor) ผู้ที่อาจให้ความยินยอมแทนผู้เยาว์ได้คือ ผู้ปกครองของผู้เยาว์ หรืออาจเป็นผู้ที่ดูแลผู้เยาว์โดยได้รับมอบหมายจากผู้ปกครอง[34] เช่น ญาติที่ผู้เยาว์มาพักอาศัยอยู่ด้วย หรือครูอาจารย์ที่โรงเรียน เนื่องจากหลักจริยศาสตร์การแพทย์ สันนิษฐานว่าผู้ปกครองจะตัดสินใจเพื่อประโยชน์สูงสุดของผู้เยาว์เสมอ ในกรณีผู้ป่วยที่ขาดความสามารถโดยสภาพเช่น ผู้ป่วยโรคหลอดเลือดสมองที่อยู่ในสภาพนอนติดเตียง เมื่อผู้ป่วยมีการเจ็บป่วยครั้งใหม่เกิดขึ้น การที่แพทย์ปรึกษาญาติถึงแนวทางการรักษานั้น ญาติของผู้ป่วยเป็นเพียงผู้ให้ความคิดเห็น ถ้าแนวทางการตัดสินใจของญาติเป็น ไปในทางที่เป็นผลเสียกับตัวผู้ป่วย เช่น ญาติขอนำผู้ป่วย

---

[33] นิธิพัฒน์ เจียรกุล, **จริยธรรมทางการแพทย์ยุคปัจจุบัน**, ค้นวันที่ 30 กรกฎาคม 2561 จาก file:///C:/Users/User/Downloads/file%204.pdf.

[34] ศักดา สถิรเรืองชัย, เรื่องเดียวกัน, หน้า 78.

กลับบ้านในขณะที่ผู้ป่วยยังต้องอาศัยเครื่องช่วยหายใจ หรือผู้ป่วยยังต้องได้รับยาทางหลอดเลือดดำ แพทย์สามารถให้การรักษาต่อโดยยึดหลักประโยชน์ของตัวผู้ป่วยเป็นหลักในการพิจารณาการรักษาพยาบาล

ดังนั้นผู้ให้บริการทางการรักษาพยาบาลจึงจำเป็นต้องทำความเข้าใจหลักการของหลักความยินยอมที่ได้รับการบอกกล่าวรวมทั้งข้อยกเว้นต่าง ๆ เพื่อให้สามารถประกอบวิชาชีพเวชกรรมได้ถูกต้องตามหลักจริยศาสตร์ทางการแพทย์ นำแนวคิดที่ได้มาพิจารณาปัญหาทางจริยศาสตร์ที่เกิดขึ้นระหว่างแพทย์และผู้ป่วย หาทางออกของปัญหาโดยมีเหตุผลทางจริยธรรมรองรับ รวมถึงในกรณีผู้รับบริการยินยอมให้ทำการรักษาพยาบาลแต่ไม่ยินยอมให้บันทึกข้อมูลส่วนบุคคลสถานพยาบาลต้องเคารพในสิทธิที่ผู้มารับบริการผู้นั้นร้องขอ

ปัจจุบันภาครัฐนำเทคโนโลยีสารสนเทศมาสนับสนุนด้านการบริการระบบสุขภาพในระดับจังหวัดให้เกิดประสิทธิภาพและจัดการปัญหาด้านสุขภาวะของโรคที่เกิดกับประชากรในพื้นที่ ช่วยบริหารและจัดการสนับสนุนการเชื่อมโยงข้อมูลด้านสุขภาพด้วยมาตรฐานที่แลกเปลี่ยนกันได้แบบทันที มีความถูกต้อง รวดเร็ว ประชาชนสามารถเข้าถึงได้ทุกที่ทุกเวลาโดยการใช้เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรือ อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตได้ หนึ่งในการขับเคลื่อนที่น่าสนใจนั้นเป็นการขับเคลื่อนด้านการบูรณาการระบบสุขภาพของไทยด้วย ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล หรือ Electronic Personal Health Records วัตถุประสงค์ของการจัดทำระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลคือให้เจ้าของข้อมูลสุขภาพและบุคลากรทางการแพทย์เข้าถึงและใช้ข้อมูลสุขภาพส่วนบุคคลได้อย่างมีประสิทธิภาพ[35] เพื่อก่อประโยชน์สูงสุดแก่เจ้าของข้อมูล การจัดการข้อมูลสุขภาพส่วนบุคคลแบ่งเป็น 3 รูปแบบคือ[36]

1. ข้อมูลที่เจ้าของข้อมูลสุขภาพส่วนบุคคลบันทึกเอง

2. ข้อมูลที่เชื่อมต่อข้อมูลสุขภาพทั่วไปบางส่วนที่บันทึกไว้ในเวชระเบียนอิเล็กทรอนิกส์ ทำให้เจ้าของข้อมูลทราบภาวะสุขภาพของตน

3. การจัดการข้อมูลสุขภาพร่วมกันระหว่าง เจ้าของข้อมูลสุขภาพ และระบบบริการสาธารณสุข เจ้าของข้อมูลสุขภาพสามารถลงข้อมูลของตนเองและดึงข้อมูลสุขภาพ จาก

---

[35] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC), **ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล–Phr**. ค้นวันที่ 2 ธันวาคม 2562 จาก https://www.nectec.or.th/innovation/innovation–software/phr.html

[36] ผู้เข้าอบรมหลักสูตรการพัฒนาความเชี่ยวชาญด้านนโยบายและยุทธศาสตร์สุขภาพ, Flow Policy Adoption **เรื่อง เทคโนโลยีสารสนเทศ Digital Transformation กระทรวงสาธารณสุข**, ค้นวันที่ 2 ธันวาคม 2562 จาก http://164.115.25.41/expertcenter/wp–content/uploads/2018/conference/HPT3/Report/G6.Paper–Digital–Transformation.pdf.

โรงพยาบาลที่รักษามาเก็บ รวบรวม ใช้และสามารถนำข้อมูลไปเชื่อมต่อกับสถานบริการทางการแพทย์ที่อื่นได้

แม้ว่าการจัดการข้อมูลสุขภาพร่วมกันระหว่างเจ้าของข้อมูลสุขภาพ และระบบบริการสาธารณสุขเป็นรูปแบบที่ทุกประเทศมุ่งหวังนำมาใช้เพื่อให้ระเบียนสุขภาพอิเล็กทรอนิกส์ก่อประโยชน์สูงสุดแก่ผู้ให้บริการและผู้รับบริการด้านสุขภาพ แต่ในส่วนของประเทศไทยระเบียนสุขภาพอิเล็กทรอนิกส์ยังอยู่ในระยะทดลองใช้ระบบ ส่วนประกอบของข้อมูลในระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล ประกอบด้วย[37]

1. เมนูข้อมูลประวัติส่วนบุคคล จะมีข้อมูลพื้นฐานทั่วไป ข้อมูลสุขภาพส่วนบุคคล ข้อมูลนักจัดการสุขภาพ ข้อมูลหลักประกันสุขภาพ ข้อมูลสถานบริการใกล้บ้าน และข้อมูลสุขศึกษา

2. ข้อมูลการรักษาพยาบาล ประกอบด้วย ข้อมูลประวัติการรักษาพยาบาล การรับวัคซีน และการนัดตรวจ

3. ข้อมูลการตรวจสุขภาพและพฤติกรรม ประกอบด้วย ข้อมูลการตรวจสุขภาพประจำปี ข้อมูลการคัดกรองโรคไม่ติดต่อเรื้อรัง การประเมินสุขภาพด้วยตัวเอง และสุดท้ายคือผลการวิเคราะห์สุขภาพ และสรุปสภาวะสุขภาพส่วนบุคคล

ข้อดีของการใช้ระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล คือ ประชาชนผู้เป็นเจ้าของข้อมูลสามารถเข้าไปค้นหาข้อมูลทั้งหมดของตนเองได้โดยง่าย สามารถบริหารข้อมูลสุขภาพของตัวเองและครอบครัวอย่างเป็นระบบ แต่ในขณะเดียวกันข้อมูลสุขภาพส่วนบุคคลอาจถูกเผยแพร่สู่สาธารณะโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลได้ เนื่องจากองค์ประกอบของระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลนอกจากจะประกอบด้วยเจ้าของข้อมูลแล้วยังมีผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งหากเกิดความผิดผลาดจากการเก็บ การใช้ การเปิดเผยหรือการประมวลข้อมูล ก็อาจส่งผลให้ข้อมูลถูกเผยแพร่ออกไปสู่สาธารณะจนส่งผลกระทบต่อเจ้าขอข้อมูลส่วนบุคคลได้ จึงควรมีมาตรการทางกฎหมายในการกำกับขอบเขตสิทธิและหน้าที่ของแต่ละบุคคลอย่างชัดเจน

---

[37] เรื่องเดียวกัน. หน้า14.

กฎหมายเกี่ยวกับหลักการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพส่วนบุคคลในรูปแบบข้อมูลอิเล็กทรอนิกส์

กรอบในการคุ้มครองข้อมูลส่วนบุคคลที่นิยมของสากลประเทศและประเทศไทยใช้นำมาใช้อ้างอิงเป็นแนวทางในการดำเนินการที่เกี่ยวกับข้อมูลส่วนบุคคลซึ่งอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ วางหลักว่าข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอนตั้งแต่การเก็บรวบรวม การเก็บรักษา และการเปิดเผย หลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพที่ผู้วิจัยศึกษา ค้นคว้า ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (Regulation (EU) 2016/679 General Data Protection Regulation –GDPR)และพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (The Health Insurance Portability and Accountability Act of 1996 – HIPAA)

เดิมกฎหมายที่บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีสาระสำคัญอยู่ 2 ประการ คือ การรับรองสิทธิของประชาชนในการเข้าถึงข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลของประชาชน ซึ่งหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลคือ หากหน่วยงานของรัฐจะเปิดเผยข้อมูลส่วนบุคคลที่หน่วยงานของตนเก็บรักษาอยู่ ไม่ว่าจะเป็นการเปิดเผยต่อหน่วยงานราชการอื่น ๆ หรือต่อบุคคลอื่น ๆ จะต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลเว้นแต่กรณีที่กฎหมายยกเว้นให้ อย่างไรก็ตามยังคงปรากฏให้เห็นอยู่ทั่วไปว่า ข้อมูลส่วนบุคคลของประชาชนที่หน่วยงานของรัฐมีหน้าที่ต้องควบคุมดูแลและคุ้มครองอย่างดีนั้น มักถูกเปิดเผยและนำไปใช้ประโยชน์กันอยู่บ่อยครั้งโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลแต่อย่างใด[38] ดังนั้นพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่ใช้อยู่ในปัจจุบันมีผลบังคับใช้ต่อหน่วยงานของรัฐเท่านั้นไม่อาจบังคับใช้กับหน่วยงานเอกชน จึงไม่สามารถคุ้มครองข้อมูลส่วนบุคคลที่เกิดจากการเก็บ รวบรวม หรือเปิดเผยจากเอกชนได้ ฝ่ายนิติบัญญัติจึงได้ตรากฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น โดยให้เหตุผลที่บันทึกในหลักการและเหตุผลประกอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความว่า

“เนื่องจากในปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูล

---

[38] นคร เสรีรักษ์, **ข้อมูลส่วนบุคคลสำคัญไฉน**, ค้นวันที่ 25 มีนาคม 2563 จาก http://www.fpps.or.th/news.php?detail=n1156791089.news.

ส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวสามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไกหรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ เป็นหลักการทั่วไปสมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น”[39]

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บันทึกหลักการและเหตุผลของร่างพระราชบัญญัติดังกล่าวแสดงให้เห็นว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องสำคัญ โดยเฉพาะข้อมูลที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์ สาระสำคัญโดยสรุปของพระราชบัญญัติฉบับนี้ คือ

คำนิยาม **“ข้อมูลส่วนบุคคล”** ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ความหมายของข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขประจำตัวของผู้มารับบริการในโรงพยาบาล อีเมล์ แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[40]

ผู้ควบคุมข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมายถึง ผู้ซึ่งมีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือผู้ที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งผู้ที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลต้องไม่ใช่บุคคลหรือนิติบุคคลคนเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้ให้คำนิยามไว้ แต่โดยหลักแล้วเจ้าของข้อมูลหมายถึง บุคคลที่ข้อมูลนั้นระบุไปถึง[41]

---

[39] "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,."

[40] มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[41] ผศ.ดร.โยฑศ์รัตต ธรรมบุษดี และ ไชยวัฒน์ จิรกิจไพบูลย์, **ผู้ช่วยวิจัยได้อะไรบ้างจากการเข้าร่วมงาน Pdpa-Privacy for All**, ค้นวันที่ 25 มีนาคม 2563 จาก https://medium.com/@mybooboy/%E0%B8%9C%E0% B8%B9%E0%B9%89%E0%B8%8A%E0%B9%88%E0%B8%A7%E0%B8%A2%E0%B8%A7%E0%B8%B4%E0%B8%88%E0%B8%B1%E0%B8%A2%E0%B9%84%E0%B8%94%E0%B9%89%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3%E0%B8%9A%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%88%E0%B8%B2%E0%B8%81%E0%B8%81%E0%

สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวกับตนเองจากผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงขอให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยที่มาของข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม[42]

2. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลนั้นมีรูปแบบที่อ่านหรือใช้งานได้ด้วยอุปกรณ์หรือเครื่องมืออัตโนมัติ[43]

3. เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้[44]

4. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลที่ได้จัดเก็บไว้[45]

5. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลที่จัดเก็บไว้ หรือทำให้ข้อมูลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้[46]

6. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขหรือดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[47]

หลักความยินยอม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติหลักความยินยอมไว้ว่า การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลจะกระทำโดยควบคุมข้อมูลส่วนบุคคลแต่การกระทำดังกล่าวทั้งหมดจะไม่สามารถกระทำได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือให้ความยินยอมในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้ ซึ่งการขอความยินยอมจะต้องทำเป็นรูปแบบลายลักษณ์

B8%B2%E0%B8%A3%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%B2%E0%B8%A3%E0%B9%88%E0%B8%A7%E0%B8%A1%E0%B8%87%E0%B8%B2%E0%B8%99-pdpa-privacy-for-all-7fbef5a83d82.

[42] มาตรา 30 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[43] มาตรา 31 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[44] มาตรา 32 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[45] มาตรา 34 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[46] มาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[47] มาตรา 34(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อักษรหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ว่าสภาพของเจ้าของข้อมูลส่วนบุคคลไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้[48]

ก่อนที่จะขอความยินยอมเพื่อเก็บข้อมูลจากเจ้าของข้อมูลส่วนบุคคล ผู้ที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลก่อนด้วยทุกครั้ง และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดตามวัตถุประสงค์ดังกล่าว

การถอนความยินยอม เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอม ในส่วนของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมนั้นโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่การถอนความยินยอมนั้นจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใดก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน ถึงผลกระทบที่จะเกิดขึ้นจากการถอนความยินยอมนั้น

ซึ่งผลของความผิดที่เกิดจากการเก็บรวบรวมข้อมูลส่วนบุคคล การนำข้อมูลส่วนบุคคลมาใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับนี้ ได้กำหนดโทษไว้ในฐานความผิดทางแพ่ง ทางอาญาและทางปกครอง ดังนี้

ความรับผิดทางแพ่ง

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะฟ้องร้องต่อศาลเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ทำตามบัญญัติแห่งพระราชบัญญัติจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลไม่ว่าผลการดำเนินการนั้นจะเกิดจากการจงใจหรือประมาทก็ตาม[49]ศาลมีอำนาจกำหนดค่าสินไหมทดแทนเพื่อเป็นการลงโทษเพิ่มจากค่าสินไหมที่แท้จริง แต่ไม่เกิน 2 เท่าของค่าสินไหมที่แท้จริง[50]

---

[48] มาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[49] มาตรา 77 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[50] มาตรา 78 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางอาญา

บทกำหนดโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีโทษทั้งจำทั้งปรับ ดังนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคล ใช้และเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จนทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย เสียชื่อเสียง โทษสูงสุดคือจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ[51]

2. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รู้มาจากการปฏิบัติหน้าที่แก่ผู้อื่น ต้องรับโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ[52]

3. ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล กรรมการหรือผู้จัดการต้องรับผิดในกรณีที่บุคคลดังกล่าวสั่งการ ละเว้นการสั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้[53]

โทษทางปกครอง

ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นเจ้าหน้าที่ของรัฐ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ส่วนราชการหรือหน่วยงานที่ได้รับมอบหมายอำนาจทางปกครองลงโทษทางปกครองแก่ผู้กระทำความผิดได้[54] ดังนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคลที่ไม่แจ้งวัตถุประสงค์ในการเก็บ รวบรวม ใช้ข้อมูลส่วนบุคคล ปฏิเสธคำขอให้เปิดเผยแหล่งที่มาของข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอมและไม่บันทึกข้อมูลส่วนบุคคลตามรายการที่กำหนด รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล[55]จนเป็นเหตุให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท[56]

2. ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เก็บ รวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลโดยไม่เป็นไปตามวัตถุประสงค์ที่แจ้งและไม่ขอความยินยอมจาก

---

[51] มาตรา 79 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[52] มาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[53] มาตรา 81 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[54] มาตรา 4 แห่งพระราชบัญญัติจัดตั้งศาลปกครองและวิธีพิจารณาคดีปกครอง พ.ศ. 2542

[55] มาตรา 85 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[56] มาตรา 82 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เจ้าของข้อมูลส่วนบุคคล[57]ไม่ปฏิบัติตามบัญญัติแห่งพระราชบัญญัตินี้[58]ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

3. ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เก็บ รวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ ศาสนา พฤติกรรมทางเพศ ความพิการตลอดจนข้อมูลสุขภาพ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[59]แล้วส่งต่อข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศหรือในเครือกิจการเดียวกัน[60] จนเป็นเหตุให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ต้องระวางโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

4. ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จนเป็นเหตุให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท[61]

5. ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจง หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ ต้องระวางโทษปรับทางปกครองไม่เกิน 5 แสนบาท[62]

6. คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองโดยใช้ดุลพินิจ[63]

จากการศึกษาพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายกลางที่มีบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไปของประเทศไทย ข้อมูลที่เกี่ยวข้องกับผู้ที่เสียชีวิตแล้วไม่อยู่ภายใต้การคุ้มครองของพระราชบัญญัติฉบับนี้ ฉะนั้นการเก็บ การใช้ และการเปิดเผยข้อมูลของผู้ที่เสียชีวิตแล้วสามารถทำได้โดยไม่ต้องขอความยินยอมจากบุคคลที่เกี่ยวข้องหรือทายาทแม้ว่าจะเป็นข้อมูลสุขภาพ ดังนั้นในส่วนของการคุ้มครองข้อมูลสุขภาพผู้วิจัยจึงศึกษาบทบัญญัติของ ระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

---

[57] มาตรา 83 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[58] มาตรา 86 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[59] มาตรา 84 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[60] มาตรา 87 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[61] มาตรา 88 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[62] มาตรา 89 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[63] มาตรา 90 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

ระเบียบฯอาศัยอำนาจตามมาตรา 20 แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2534 ระเบียบฯ นี้ออกมาเพื่อคุ้มครองข้อมูลด้านสุขภาพของประชาชน รวมถึงกำกับควบคุม การบริหารจัดการและการใช้ข้อมูลสุขภาพของประชาชน บัญญัตินิยามศัพท์เกี่ยวกับข้อมูลส่วนบุคคล เจ้าของข้อมูล ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ดังนี้[64]

"**ข้อมูลด้านสุขภาพของบุคคล**" หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด

"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อมูลของบุคคลที่บันทึกเป็นเอกสารแล้วถูกดัดแปลงให้เป็นรูปแบบอิเล็กทรอนิกส์หรือถูกบันทึกเป็นข้อความในรูปแบบอิเล็กทรอนิกส์

"ระเบียนสุขภาพ" หมายความว่า ทะเบียนหรือรายการ ข้อมูลด้านสุขภาพของบุคคล ที่กระทรวงสาธารณสุข หน่วยงานทั้งภาครัฐและเอกชน นำมาเก็บ จัดการ ใช้และเปิดเผยเพื่อประโยชน์ของเจ้าของข้อมูล

"เจ้าของข้อมูล" หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลด้านสุขภาพ

"ผู้ควบคุมข้อมูล" หมายถึง ส่วนราชการ หน่วยงาน โรงพยาบาล โรงพยาบาลส่งเสริมสุขภาพตำบล สถานีอนามัย ในสังกัดกระทรวงสาธารณสุข และหมายความรวมถึงสถานพยาบาล ตามพระราชบัญญัติสถานพยาบาล พ.ศ. 2541 และหน่วยงานของรัฐอื่นที่ประสงค์เข้าร่วมใช้ข้อมูลด้านสุขภาพร่วมกับกระทรวงสาธารณสุขซึ่งเป็นผู้จัดทำ เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลด้านสุขภาพของบุคคล

"ผู้บริหารจัดการข้อมูล" หมายความว่า กระทรวงสาธารณสุขรวมถึงบุคคลหรือหน่วยงานที่ได้รับมอบหมายจากกระทรวงสาธารณสุขให้ดำเนินการเก็บข้อมูล รวบรวมข้อมูล ใช้และเปิดเผยข้อมูล

---

[64] ข้อ 4 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

สิทธิของเจ้าของข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติสิทธิของเจ้าของข้อมูลสุขภาพส่วนบุคคล ดังนี้

1. เจ้าของข้อมูลสุขภาพส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลเปิดเผย[65] และสำเนาข้อมูลสุขภาพส่วนบุคคลของตน[66]

2. เจ้าของข้อมูลสุขภาพส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลสุขภาพของตนให้ถูกต้องตามหลักฐานแสดงข้อมูลที่แนบให้แก้ไข[67]

หลักความยินยอม

หลักความยินยอมตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ระบุเพียงว่า ข้อมูลสุขภาพส่วนบุคคลจัดว่าเป็นความลับส่วนบุคคล จะเปิดเผยได้เมื่อเจ้าของข้อมูลให้ความยินยอม ผู้ได้รับมอบอำนาจจากเจ้าของข้อมูลให้ความยินยอม ผู้แทนโดยชอบธรรมให้ความยินยอม หรือทายาทเป็นผู้ให้ความยินยอม[68] ซึ่งการเปิดเผยข้อมูลสุขภาพส่วนบุคคลนั้นต้องไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลและผู้ครอบครองข้อมูล[69]

ผู้ควบคุมข้อมูล อาจขอให้เจ้าของข้อมูลยินยอมให้เปิดเผยข้อมูลสุขภาพไว้ล่วงหน้าในกรณี เพื่อประโยชน์ของเจ้าของข้อมูล เพื่อการวิจัยโดยไม่ระบุชื่อ หรือเพื่อระงับเหตุที่ก่อให้เกิดอันตรายต่อชีวิตของเจ้าของข้อมูล[70]

การเปิดเผยข้อมูลสุขภาพส่วนบุคคลต่อ ศาล พนักงานสอบสวน ตำรวจและเจ้าหน้าที่ที่กฎหมายให้อำนาจ ผู้ควบคุมข้อมูลสามารถกระทำได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลสุขภาพ[71]

---

[65] ข้อ 14 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[66] ข้อ 19 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[67] ข้อ 23 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[68] ข้อ 14 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[69] ข้อ 13 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[70] ข้อ 21 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

บทลงโทษ

ตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 มิได้บัญญัติโทษไว้เป็นการเฉพาะ บัญญัติเพียงว่าหากมีบุคคลใดมิได้กระทำตามที่ระเบียบฯกำหนด การรับโทษให้ยึดตามกฎหมายที่เกี่ยวข้อง[72]

แม้ว่าระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 เป็นกฎหมายที่ออกมาเพื่อคุ้มครองข้อมูลสุขภาพส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่การคุ้มครองยังไม่ทัดเทียมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา

3. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (Regulation (EU) 2016/679 General Data Protection Regulation –GDPR)

GDPR ย่อมาจาก General Data Protection Regulation คือหลักคุ้มครองข้อมูลส่วนบุคคลแบบใหม่ของสหภาพยุโรป โดยสภาสหภาพยุโรปผ่านกฎหมายและมีผลบังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2561 ที่ผ่านมา[73] หลักสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป คือ ขยับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจน และให้ความคุ้มครองเป็นการทั่วไป (General) ใช้เหมือนกันในทุกประเทศสมาชิกของสหภาพยุโรป[74] รวมถึงการส่งข้อมูลระหว่างประเทศ กฎหมายฉบับนี้ระบุชัดเจนว่าผู้รับข้อมูล ซึ่งอาจจะเป็นบริษัทคลาวด์หรือบริษัทประมวลผลข้อมูล (Data Processer) ที่แม้จะอยู่ต่างประเทศนอกขอบเขตของประเทศสมาชิกสหภาพยุโรปก็ต้องทำตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

หลักการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดยสรุป

1. หน่วยงานควบคุมข้อมูลที่เจ้าของข้อมูลรับบริการ (Data Controller) ต้อง

---

[71] ข้อ 15 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[72] ข้อ 3 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[73] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, **กฎหมาย Gdpr ฉบับรวบรัด**, ค้นวันที่ 15 มีนาคม 2563 จาก: https://www.etda.or.th/content/gdpr-in-a-nutshell.

[74] Article 50 General Data Protection Regulation, “International cooperation for the protection of personal data”

ได้รับความยินยอมจากเจ้าของข้อมูล (Data Subject) ในการจัดเก็บข้อมูล รวมทั้งต้องกำหนดขอบเขตและวัตถุประสงค์ในการประมวลผลข้อมูลที่ชัดเจน

2. แต่ละประเทศต้องให้การคุ้มครองอย่างเคร่งครัดต่อข้อมูลที่อ่อนไหวเป็นพิเศษเช่น ความคิดทางการเมือง ศาสนาลัทธิ พฤติกรรมสุขภาพ พฤติกรรมทางเพศ การเป็นสมาชิกสหพันธ์ ประวัติอาชญากรรม เป็นต้น

3. การส่งข้อมูลไปต่างประเทศ หรือบริษัทที่อยู่ต่างประเทศ ผู้รับข้อมูลต้องมีการคุ้มครองข้อมูลมาตรฐานเดียวกับบริษัทในยุโรป

4. หน่วยงานควบคุมข้อมูลต้องกำหนดขอบเขต ระยะเวลาในการประมวลผลและมีมาตรการรักษาความปลอดภัยข้อมูลอย่างรัดกุม

5. เมื่อเกิดการละเมิดข้อมูลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง[75]

6. การขอความยินยอม ในกรณีที่บริษัทเอกชนทั่วไปที่ทำแอปพลิเคชันใช้งานผ่านโทรศัพท์มือถือจะมีวิธีขอความยินยอมแบบรวมในทุกรูปแบบเพื่อการนำข้อมูลไปใช้ GDPR บังคับให้การขอความยินยอมต้องอ่านง่าย ไม่กำกวม และไม่อนุญาตให้รวมการกดให้คำยินยอมของหลายวัตถุประสงค์ไว้ในหน้าเดียว[76]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ให้นิยามว่าข้อมูลส่วนบุคคลหมายถึง ข้อมูลของบุคคลธรรมดาที่ยังมีชีวิตอยู่และทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่นชื่อ หมายเลขประจำตัว ข้อมูลสถานที่อยู่ การระบุตัวตนทางออนไลน์ หรือปัจจัยหนึ่งหรือหลายอย่างที่กล่าวถึงอันทำให้สามารถระบุลักษณะทางกายภาพ ลักษณะทางพันธุกรรม สภาพทางจิต เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้นล้วนถือว่าเป็นข้อมูลส่วนบุคคลทั้งสิ้น ดังนั้น ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ข้อมูลส่วนบุคคลที่ถูกทำให่ม่ (De-identified) ข้อมูลที่ถูกเข้ารหัส (Encrypted) หรือการใช้นามแฝง (Pseudonym zed) แต่สามารถประมวลผลและระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ ก็ยังถือว่าอยู่ในบทนิยามของคำว่าข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ต้องอยู่ภายใต้บังคับของกฎหมาย [77]

---

[75] Article 33 General Data Protection Regulation, “Notification of a personal data breach to the supervisory authority”

[76] Article 7 General Data Protection Regulation, “Conditions for consent”

[77] **Gdpr ฉบับภาษาไทย**, ณรงค์ ใจหาญ นคร เสรีรักษ์, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร และ นิชานันท์ นันทศิริศรณ์, ผู้แปล, (กรุงเทพฯ: พี.เพรส, 2562), หน้า 41.

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ได้ให้คำจำกัดความและหน้าที่ของบทบาทของผู้เกี่ยวข้องกับข้อมูลส่วนบุคคลไว้ 3 บทบาท ดังนี้[78]

1. ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ บุคคลหรือนิติบุคคลผู้ซึ่ง ทำหน้าที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล[79] ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการของหน่วยงานต่าง ๆ

2. ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้[80] อนึ่ง “การประมวลผลข้อมูล” (Processing) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนั้น ไม่ใช่เพียงแค่การวิเคราะห์ หรือจัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย[81]

3. เจ้าของข้อมูลส่วนบุคคลหรือผู้ถูกประมวลผล (Data Subject) คือ บุคคลธรรมดาที่ข้อมูลนั้นระบุไปถึง ซึ่งข้อมูลนั้นถูกนำไปเก็บ รวบรวม ใช้ หรือเปิดเผย[82]

สิทธิของเจ้าของข้อมูล

GDPR ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล ดังนี้

1. เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลส่วนบุคคล รวมถึงมีสิทธิได้รับทราบวัตถุประสงค์การจัดเก็บข้อมูล ที่มาของข้อมูล ระยะเวลาที่คาดว่าจะใช้เก็บข้อมูล[83] เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอสำเนาข้อมูลของตนในรูปแบบอิเล็กทรอนิกส์หรือในรูปแบบอื่นจากผู้ควบคุมข้อมูลส่วนบุคคล

2. เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลของตนให้ถูกต้องและสมบูรณ์[84]

3. เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลที่จัดเก็บไว้[85] ในกรณีดังต่อไปนี้

3.1 ข้อมูลนั้นหมดความจำเป็น[86]

---

[78] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, เรื่องเดียวกัน, หน้า 23.

[79] Article 4 (7) General Data Protection Regulation

[80] Article 4 (1) General Data Protection Regulation

[81] Article 4 (2) General Data Protection Regulation

[82] Article 4 (8) General Data Protection Regulation

[83] Article 15 General Data Protection Regulation, “Right of access by the data subject”

[84] Article 16 General Data Protection Regulation, “Right to rectification”

[85] Article 17 General Data Protection Regulation, “Right to erasure”

3.2 เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม[87]

3.3 เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลของตน[88]

3.4 ข้อมูลนั้นถูกประมวลผลโดยมิชอบด้วยกฎหมาย[89]

4. เจ้าของข้อมูลส่วนบุคคลมีสิทธิจำกัดการประมวลผลข้อมูลส่วนบุคคลของตนจากผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลไม่ชอบด้วยกฎหมาย หรือในกรณีที่ข้อมูลหมดความจำเป็นต่อผู้ประมวลข้อมูลส่วนบุคคลแต่ข้อมูลดังกล่าวยังจำเป็นสำหรับเจ้าของข้อมูลส่วนบุคคล[90]

5. เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการแจ้งเตือนจากผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่ แก้ไข ลบ หรือจำกัดการประมวลผลข้อมูลส่วนบุคคลของตน[91]

6. เจ้าของข้อมูลส่วนบุคคลมีสิทธิใช้ และส่งต่อข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง[92]

7. เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้าน

8. เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่ปฏิเสธการวินิจฉัยหรือการประมวลผลจากกระบวนการประมวลผลอัตโนมัติ

หลักความยินยอม

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ภาษาที่เข้าใจง่าย ไม่ซับซ้อน เอกสารขอความยินยอมต้องแยกออกจากเอกสารอื่นอย่างชัดเจน เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมอย่างเสรีมิใช่ถูกบังคับ[93] การทำเครื่องหมายในช่องหน้าข้อความของแบบฟอร์มแล้ว การเงียบหรือการนิ่งเฉยไม่ถือว่าเป็นการยินยอม[94]

---

[86] Article 17 (a) General Data Protection Regulation

[87] Article 17 (b) General Data Protection Regulation

[88] Article 17 (c) General Data Protection Regulation

[89] Article 17 (d) General Data Protection Regulation

[90] Article 18 General Data Protection Regulation," Right to restriction of processing"

[91] Article 19 General Data Protection Regulation," Right to Notification obligation regarding rectification or erasure of personal data or restriction of processing"

[92] Article 20 General Data Protection Regulation," Right to data portability"

[93] Article 6 (1) (a) General Data Protection Regulation

[94] Section 32 Regulation (EU) 2016/679 of the European Parliament and of the Councilof27 April2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

การประมวลผลข้อมูลที่มีความอ่อนไหว เช่นข้อมูลสุขภาพส่วนบุคคลต้องได้รับความยินยอมโดยชัดเจน[95] เจ้าของข้อมูลส่วนบุคคลสิทธิเพิกถอนความยินยอมได้ทุกเมื่อ การเพิกถอนความยินยอมนั้นไม่ส่งผลกระทบต่อผลการประมวลผลข้อมูลส่วนบุคคลก่อนที่จะเพิกถอนความยินยอม

บทลงโทษ

GDPR เป็นกฎหมายกลางของสหภาพยุโรปเพื่อคุ้มครองข้อมูลส่วนบุคคล บทลงโทษที่บัญญัติไว้ใน GDPR มีแค่โทษปรับทางแพ่งและโทษปรับทางปกครอง แต่ไม่มีโทษอาญาหรือจำคุก โดยบัญญัติไว้ว่า

โทษปรับทางแพ่ง

การเก็บและประมวลผลข้อมูลส่วนบุคคลของประชาชนสหภาพยุโรป โดยไม่ปฏิบัติตามหลักของ GDPR จนทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเปิดเผยสู่สาธารณะโดยที่เจ้าของข้อมูลไม่ให้ความยินยอม เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการชดเชยความเสียหายจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[96]

โทษปรับทางปกครอง

หน่วยงานที่ดูกำกับแลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักของ GDPR จนทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเปิดเผยสู่สาธารณะโดยที่เจ้าของข้อมูลไม่ให้ความยินยอม จะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ ร้อยละ 2-4 ของรายได้ต่อปีทั่วโลก ขึ้นอยู่กับว่าวงเงินใดสูงกว่า[97]

จากการศึกษาพบว่า การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ให้ความคุ้มครองทุกส่วนที่อยู่ในระบบการคุ้มครองข้อมูลส่วนบุคคล พลเมืองของสหภาพยุโรปรวมถึงข้อมูลส่วนบุคคลของประชากรของสหภาพยุโรปจะได้รับความคุ้มครองทุกกรณีไม่ว่าการละเมิดข้อมูลส่วนบุคคลนั้นจะเกิดภายในสหภาพยุโรปหรือไม่ก็ตาม

แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะมีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลสุขภาพแต่กฎหมายฉบับนี้เป็นกฎหมายกลางที่คุ้มครองข้อมูลส่วนบุคคลในทุกภาคส่วน ผู้วิจัยจึงสนใจศึกษาพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูล

---

[95] Article 9 (2) (a) General Data Protection Regulation

[96] Article 82 General Data Protection Regulation," Right to compensation and liability"

[97] Article 83 General Data Protection Regulation," General conditions for imposing administrative fines"

ทางด้านการประกันสุขภาพของสหรัฐอเมริกา ซึ่งเป็นกฎหมายเฉพาะในการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพเพื่อนำมาประยุกต์ใช้กับการคุ้มครองข้อมูลสุขภาพที่จัดเก็บในระบบระเบียนอิเล็กทรอนิกส์ของประเทศไทย

4. พระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (The Health Insurance Portability and Accountability Act of 1996 – HIPAA)[98]

กฎหมายการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศสหรัฐอเมริกานั้นมีลักษณะการบัญญัติเป็นระบบกฎหมายเฉพาะเรื่อง (Sectoral law) ไม่มีกฎหมายแม่บทกลางในการวางหลักเกณฑ์เป็นการทั่วไป สภาครองเกรสจะตรากฎหมายก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนที่ถูกละเมิดขึ้น ดังนั้น การออกกฎหมายคุ้มครองส่วนบุคคลของสหรัฐอเมริกาจึงมีลักษณะเป็นการแก้ปัญหาที่เกิดขึ้นมากกว่าที่จะเป็นการวางหลักเกณฑ์เพื่อป้องกันปัญหา เป็นการตอบสนองหรือแก้ไขเป็นเรื่อง ๆ ไป กฎหมายคุ้มครองส่วนบุคคลจึงมีลักษณะเฉพาะเรื่องและยังมีการคุ้มครองตัวเองอีกรูปแบบหนึ่งซึ่งเรียกว่ากลไกกำกับดูแลตนเอง (Self–regulation) ผลจากความเติบโตในทางธุรกิจ การพัฒนาการทางเทคโนโลยีและการประกอบธุรกิจสมัยใหม่ กลไกกำกับดูแลตนเองสามารถมีได้หลายรูปแบบ เช่นการที่กลุ่มผู้ประกอบวิชาชีพหรือกลุ่มผู้ประกอบธุรกิจสาขาเดียวกันได้ร่วมกันจัดทำแนวปฏิบัติ (Code of Practice) เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยถือว่าแนวปฏิบัติดังกล่าวเป็นส่วนหนึ่งของนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของ ผู้ประกอบวิชาชีพหรือองค์กรที่ร่วมเป็นสมาชิกจำเป็นต้องปฏิบัติตาม หรืออีกวิธีการหนึ่งคือการออกนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของตนให้แก่สาธารณะชนได้รับทราบว่าองค์กรนั้น ๆ จะปฏิบัติต่อข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการเป็นไปในแนวทางใด ดังนั้นในการวิจัยนี้ผู้วิจัยจึงขอเสนอ เฉพาะหลักการสำคัญที่ปรากฏในพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา[99] (The Health Insurance Portability and Accountability Act of 1996–HIPAA)

นิยามของกฎหมาย HIPAA

HIPAA เป็นกฎหมายที่คุ้มครองข้อมูลที่เกี่ยวข้องกับข้อมูลสุขภาพและการรักษาพยาบาลของผู้ป่วยในทุกรูปแบบ ไม่ว่าจะเป็นโดยการพูด เขียน หรือการส่งข้อมูลทาง

---

[98] Hipaa Administrative Simplification Regulation Text (45 Cfr Parts 160, 162, and 164)

[99] Office for Civil Rights (OCR), **Summary of the Hipaa Privacy Rule**, Date cited 1 june 2018 Available from: https://www.hhs.gov/hipaa/for–professionals/privacy/laws–regulations/index.html.

อิเล็กทรอนิกส์ ข้อมูลดังกล่าวนี้ เรียกรวม ๆ ว่า Protected Health Information (PHI)[100] อันได้แก่ ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หมายเลขประกันสังคม หมายเลขประจำตัวผู้ป่วย ประวัติความเจ็บป่วย ผลการตรวจพิเศษ ผลการตรวจเลือดต่าง ๆ ข้อมูลบริษัทประกันสุขภาพ ข้อมูลค่ารักษาพยาบาล และอื่น ๆ ที่เกี่ยวข้อง

นิยามคำว่า “ข้อมูลสุขภาพ” ตามบทบัญญัติของ HIPAA หมายถึง ข้อมูลด้านสุขภาพด้านร่างกายและสุขภาพจิต[101]ที่ทำให้ระบุตัวบุคคลได้ ไม่ว่าข้อมูลสุขภาพนั้นจะถูกเก็บในรูปแบบของ เอกสาร รูปถ่าย การให้ข้อมูลด้วยวาจา และหมายรวมถึงข้อมูลที่ถูกสร้างขึ้นจากผู้ให้บริการด้านสุขภาพ หรือหน่วยงานที่ดูแลสุขภาพ โดยมีการบันทึกไว้เป็นเอกสารหรือจัดเก็บไว้ในระบบอิเล็กทรอนิกส์ แต่ความคุ้มครองข้อมูลสุขภาพจะครอบคลุมเฉพาะเจ้าของข้อมูลสุขภาพที่ยังมีชีวิตอยู่หรือเสียชีวิตไม่เกิน 50 ปี[102] ซึ่งผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้นจึงจะมีสิทธิใช้หรือส่งต่อข้อมูล การละเมิดกฎ(HIPAA Violation)[103]มีบทลงโทษที่รุนแรงคือ โทษปรับได้สูงสูดถึง1,500,000 ดอลล่าสหรัฐ

การบังคับใช้กฎหมาย HIPAA

สำหรับการบังคับใช้กฎหมายนี้ คณะกรรมาธิการการค้าแห่งสหพันธรัฐของสหรัฐอเมริกา (Federal Trade Commission– FTC) มีอำนาจดำเนินคดีกับ ผู้ฝ่าฝืนกฎหมาย โดยมีอำนาจกำหนดค่าปรับทางแพ่ง (15 U.S.C.A., section 6505 (a)) และมีบทลงโทษทางอาญา (42 U.S.C.1320d, section 1177)[104] ตัวอย่างคดีสำคัญที่แสดงถึงการบังคับใช้กฎหมาย HIPAA โดยคณะกรรมาธิการ FTC ยกตัวอย่างเช่น กรณีของบริทนีย์ สเปียร์ ในขณะที่เข้ารับการรักษาในโรงพยาบาลด้วยปัญหาทางจิต เกิดเหตุมีบุคคลที่ไม่มีส่วนเกี่ยวข้องในการดูแลรักษา แต่เป็นเจ้าหน้าที่ของโรงพยาบาลเข้าไปดูข้อมูลเกี่ยวกับการดูแลรักษาบริทนีย์ สเปียร์[105] เหตุการณ์ครั้งนั้นส่งผลให้แพทย์ พยาบาล จำนวนมากกว่าสิบคน ถูกไล่ออกจากงานและถูกลงโทษทาง

---

[100] **Protected Health Information**, Date cited Available from: https://www.truevault.com/protected-health-information.

[101] The Code of Federal Regulations Title 45 Section 160.524 (i)

[102] The Code of Federal Regulations Title 45 Section 160.103

[103] Laurie Zabel, **10 Common Hipaa Violations and Preventative Measures to Keep Your Practice in Compliance**, Date cited Available from: https://www.beckershospitalreview.com/healthcare-information-technology/10-common-hipaa-violations-and-preventative-measures-to-keep-your-practice-in-compliance.html.l

[104] Social Security, **Wrongful Disclosure of Individually Identifiable Health Information**, Date cited Available from: https://www.ssa.gov/OP_Home/ssact/title11/1177.htm.

[105] Reed Tinsley, **Hipaa and Britney Spears**, Date cited March 5, 2018 Available from: http://www.rtacpa.com/blog/hipaa-and-britn.

วินัย เนื่องจากตรวจสอบพบว่าบุคคลเหล่านั้นเข้าไปดูข้อมูลและประวัติการรักษาของผู้ป่วยที่ไม่ได้อยู่ในความดูแลของตน[106]

บทลงโทษทางแพ่ง เนื่องจากการละเมิดข้อมูลสุขภาพตามกฎหมาย HIPAA แบ่งออกเป็น 4 ระดับ[107] คือ

ระดับ 1 ละเมิดข้อมูลโดยไม่รู้ตัวและไม่สามารถหลีกเลี่ยงได้ในขณะที่พยายามปฏิบัติตามระเบียบของ HIPAA ปรับเป็นเงินตั้งแต่ 100 – 50,000 ดอลล่าต่อการละเมิด 1 ครั้ง

ระดับ 2 การละเมิดข้อมูลโดยปฏิบัติตามระเบียบของ HIPAA ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นแต่ไม่สามารถหลีกเลี่ยงได้ ปรับเป็นเงินตั้งแต่ 1,000 – 50,000 ดอลล่าต่อการละเมิด 1 ครั้ง

ระดับ 3 การละเมิดข้อมูลเนื่องจากละเลยการปฏิบัติตามระเบียบของ HIPAA ปรับเป็นเงินตั้งแต่ 10,000 – 50,000 ดอลล่าต่อการละเมิด 1 ครั้ง

ระดับ 4 การละเมิดข้อมูลเนื่องจากละเลยการปฏิบัติตามระเบียบของ HIPAAและไม่พยายามแก้ไขเมื่อรู้ถึงเหตุแห่งการละเมิด ปรับเป็นเงินตั้งแต่ 50,000 ดอลล่าขึ้นไป ต่อการละเมิด 1 ครั้ง

นอกจากบทลงโทษทางแพ่งตามกฎหมาย HIPAA และกฎความปลอดภัยแล้ว ผู้ให้บริการ ผู้ควบคุมข้อมูลหรือผู้อื่นที่กระทำการละเมิดข้อมูลสุขภาพของผู้อื่นตามกฎหมาย HIPAA ต้องเผชิญกับ**บทลงโทษทางอาญา** เมื่อกระทำการดังต่อไปนี้

1. ผู้ใดใช้ หรือเป็นเหตุที่ทำให้ใช้ลักษณะเฉพาะด้านสุขภาพของบุคคล
2. ผู้ใด ได้มาซึ่งข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้ ซึ่งอาจจะเกี่ยวกับปัจเจกบุคคล/ข้อมูลสุขภาพที่ระบุตัวบุคคลได้
3. ผู้ใดกระทำการเปิดเผยข้อมูลข้อมูลสุขภาพส่วนบุคคลที่สามารถระบุตัวบุคคลนั้น ผู้ที่กระทำดังที่กล่าวมา ต้องระวางโทษคือ

3.1 ปรับไม่เกิน 50,000 ดอลล่าสหรัฐ จำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ

3.2 ถ้ากระทำผิดเนื่องจากการอ้างสิทธิ์โดยมิชอบ โทษปรับไม่เกิน 100,000 ดอลล่าสหรัฐ จำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

---

[106] Charles Ornstein, **13 Hospital Workers Fired for Snooping in Britney Spears' Medical Records**, Los Angeles Times, Date cited May 1, 2018 Available from: https://www.latimes.com/archives/la-xpm-2008-mar-15-me-britney15-story.html.

[107] HIPAA Journal, **What Are the Penalties for Hipaa Violations?**, Date cited December 2, 2018 Available from: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.

3.3 ถ้ากระทำผิดโดยเจตนา เช่น ขายข้อมูล โอนย้ายข้อมูลหรือใช้ข้อมูลสุขภาพที่ระบุตัวบุคคล เพื่อประโยชน์ทางการค้า ประโยชน์ส่วนตัว หรือทำให้เกิดอันตรายต่อเจ้าของข้อมูลได้ โทษปรับไม่เกิน 250,000 ดอลล่าสหรัฐ จำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

จากการศึกษาพบว่า กฎหมาย HIPAA กำหนดหลักการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลหลายประการ โดยเฉพาะอย่างยิ่งสิทธิที่จะได้รับการรักษาความลับ และ สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลด้านสุขภาพ รวมถึงบทบัญญัติเกี่ยวกับการจัดการข้อมูลด้านสุขภาพของบุคคลที่มีความชัดเจน เช่น การเก็บรวบรวมข้อมูลส่วนบุคคลด้านสุขภาพ การใช้ข้อมูลส่วนบุคคลด้านสุขภาพ การเข้าถึงข้อมูลส่วนบุคคลด้านสุขภาพ และการแก้ไขข้อมูลส่วนบุคคลด้านสุขภาพ การดูข้อมูลส่วนบุคคลของผู้อื่นไม่ว่าโดยวิธีใด ก็ถือว่าผิดกฎหมาย แต่ตามกฎหมายไทยนั้นถ้าไม่ก่อความเสียหายแก่เจ้าของข้อมูล และไม่มีผู้ร้องทุกข์ จะไม่สามารถเอาผิดได้ ดังที่ปรากฏในคำพิพากษาศาลฎีกาที่ 5161/2547 ศาลฎีกาพิพากษาว่า ข้อมูลคอมพิวเตอร์ไม่เป็นวัตถุมีรูปร่าง ส่วนตัวอักษร ภาพแผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลดังกล่าวมิใช่รูปร่างของข้อมูลฉะนั้นข้อมูลมิใช่ทรัพย์[108] ดังนั้นเมื่อเกิดเหตุคัดลอกข้อมูลที่เราวางไว้บนโต๊ะหรือคัดลอกข้อมูลในระบบอิเล็กทรอนิกส์ที่ไม่ใส่รหัสป้องกันก็ไม่ใช่ความผิดฐานลักทรัพย์ ซึ่งขัดแย้งกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดบทลงโทษต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหากนำข้อมูลส่วนบุคคลที่เก็บ รวบรวมไว้ไปเปิดเผยสู่สาธารณะโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจนเป็นเหตุให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ต้องรับโทษทั้งทางอาญา[109] และโทษทางปกครอง[110]

จะเห็นได้ว่ากฎหมายในปัจจุบันได้ให้ความสำคัญกับสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล การนำข้อมูลส่วนบุคคลของผู้อื่นมาใช้จะต้องได้รับความยินยอม ผู้ควบคุมข้อมูลต้องมีระบบการขอใช้ข้อมูล การเก็บรวบรวม การเปิดเผยข้อมูลและวิธีการแก้ไขเมื่อพบปัญหาข้อมูลส่วนบุคคลถูกเผยแพร่สู่สาธารณโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดเจน มีบทลงโทษที่รุนแรงต่อผู้ที่ละเมิดข้อมูลส่วนบุคคลของผู้อื่น หลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพตามกฎหมายต่างประเทศกำหนดเหตุแห่งการยกเว้นหลักการคุ้มครองข้อมูลส่วน

---

[108] สอนชัย สิรารียกุล, **หมายเหตุท้ายฎีกา เรื่องความลับทางการค้า**, ค้นวันที่ 22 กุมภาพันธ์ 2561 จาก https://www.lawsiam.com/?name=lawyer-download&file=filedetail&max=2497.

[109] มาตรา 79 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[110] มาตรา 83 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บุคคลด้านสุขภาพซึ่งเป็นหลักสากลในทำนองเดียวกันคือ สามารถจำแนกเหตุแห่งการยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพตามหลักสากล ออกเป็น 3 ประการใหญ่ ๆ ได้แก่ 1)หลักความยินยอมของบุคคลซึ่งเป็นเจ้าของข้อมูล 2)ประโยชน์สาธารณะ และ3) ประโยชน์ของบุคคลซึ่งเป็นเจ้าของข้อมูล

จากการศึกษาพบว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ใช้เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลในภาพรวม และระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ที่ใช้คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระเบียนสุขภาพอิเล็กทรอนิกส์ของประเทศไทย มาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลยังไม่เทียบเท่ากับ GDPR และ HIPAA จึงไม่เพียงพอที่จะคุ้มครองข้อมูลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

บทที่ 3

วิธีดำเนินการวิจัย

วิทยานิพนธ์ฉบับนี้เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research)โดยมีขั้นตอนดำเนินการวิจัยดังต่อไปนี้

รูปแบบการวิจัย

ใช้รูปแบบวิจัยเอกสาร (Documentary Research) ศึกษาจากแนวคิด ทฤษฎีและจากกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยวิธีการทบทวนวรรณกรรม วิเคราะห์เนื้อหา (Content analysis) โดยมีขอบเขตศึกษาวิเคราะห์ตัวบทกฎหมาย บทความวิชาการ วิทยานิพนธ์ เอกสารอื่น ๆ ที่เกี่ยวข้อง โดยมีการศึกษาเชิงเปรียบเทียบ (Comparative analysis) ระหว่างกฎหมายต่างประเทศและกฎหมายไทยที่เกี่ยวข้อง โดยศึกษาถึงหลักการในการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะการคุ้มครองข้อมูลส่วนบุคคลในกรอบของยุโรปและสหรัฐอเมริกาที่สามารถใช้นำมาประยุกต์ใช้เป็นแนวทางในการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อนำมาใช้เป็นมาตรการในการคุ้มครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ของประเทศไทยต่อไป

วิธีการเก็บรวบรวมข้อมูล

ผู้วิจัยได้เก็บรวบรวมข้อมูลโดยรวบรวมจากแหล่งข้อมูลทั้งในส่วนภาษาไทย และภาษาต่างประเทศประกอบกับข้อมูลประเภทเอกสารและสิ่งพิมพ์อิเล็กทรอนิกส์ โดยศึกษาค้นคว้าข้อมูลกฎหมายจากหนังสือ ตำรา สิ่งพิมพ์อิเล็กทรอนิกส์ เอกสาร บทความ นิตยสาร วิทยานิพนธ์และงานวิจัยที่เกี่ยวข้อง รวมถึงการใช้ระบบสืบค้นในเว็บไซต์

การวิเคราะห์ข้อมูล

การศึกษาโดยรวมทั้งหมดตั้งแต่อดีตจนถึงปัจจุบัน ผู้วิจัยเห็นว่าสิทธิส่วนบุคคลเป็นเรื่องสำคัญ ประเทศไทยบัญญัติกฎหมายออกมาหลายฉบับเพื่อคุ้มครองสิทธิส่วนบุคคล อาทิ เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 บัญญัติเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวแต่ไม่มีหลักเกณฑ์ที่บังคับใช้ในการเก็บรวบรวมข้อมูล การนำข้อมูลส่วน

บุคคลมาใช้และการเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัติการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บไว้ในหน่วยงานของภาครัฐแต่ไม่คุ้มครองข้อมูลที่จัดเก็บโดยภาคเอกชน กฎหมายที่มีบทบัญญัติเกี่ยวกับการเปิดเผยข้อมูลด้านสุขภาพซึ่งยึดหลักเรื่องจรรยาบรรณของผู้ประกอบวิชาชีพด้านสุขภาพคือการรักษาความลับของผู้ป่วย บุคคลที่กระทำการละเมิดข้อมูลของผู้ป่วยมีบทลงโทษตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 แต่ด้วยความก้าวหน้าทางเทคโนโลยีทำให้ประเทศไทยบัญญัติกฎหมายออกมาเพื่อคุ้มครองข้อมูลด้านสุขภาพส่วนบุคคลที่จัดเก็บไว้ในระบบอิเล็กทรอนิกส์ อันได้แก่ ระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ซึ่งระเบียบฉบับนี้ออกมาโดยอ้างพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2534 และกฎหมายฉบับล่าสุดที่ประกาศใช้ คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งจะบังคับใช้เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลทุกภาคส่วน

หลักการวิเคราะห์ข้อมูลของการวิจัยมีกรอบการวิเคราะห์ดังนี้

1. การคุ้มครองข้อมูลส่วนบุคคลมีรากฐานจากแนวคิดทฤษฎีเกี่ยวกับสิทธิในความเป็นอยู่ส่วนตัว หรือสิทธิส่วนบุคคล (Right to privacy) ซึ่งอยู่ในกรอบของกฎหมายสิทธิมนุษยชน

2. กฎหมายไทยและกฎหมายต่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีระดับและรายละเอียดการคุ้มครองที่แตกต่างกัน โดยวิเคราะห์ในประเด็นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ของไทย ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 เปรียบเทียบกับกรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development–OECD) ใน เรื่ อ ง Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (Regulation (EU) 2016/679 General Data Protection Regulation –GDPR)และพระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (The Health Insurance Portability and Accountability Act of 1996 – HIPAA)

ผู้วิจัยจึงทำการศึกษาเปรียบเทียบมาตรการทางกฎหมายที่ได้กล่าวมาข้างต้น เพื่อเสนอแนะมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล ในบทต่อไป

บทที่ 4

ผลการวิจัย

เนื่องจากความก้าวหน้าด้านเทคโนโลยีสารสนเทศที่พัฒนาอย่างรวดเร็ว จึงทำให้เกิดปัญหาการล่วงละเมิดสิทธิความเป็นส่วนตัวและข้อมูลส่วนบุคคลของผู้อื่นได้ง่ายดาย จากการศึกษาพบว่าข้อมูลส่วนบุคคลเป็นเรื่องที่ละเอียดอ่อน กฎหมายของประเทศไทยในปัจจุบันที่มีบทบัญญัติในเรื่องของการดูแลคุ้มครองข้อมูลส่วนบุคคลนั้นมีกระจัดกระจายอยู่ในกฎหมายหลายฉบับ แต่ก็เป็นเพียงการคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง ยังไม่มีหลักเกณฑ์ กลไกหรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปซึ่งสามารถนำมาใช้เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลได้ ปัจจุบันจึงได้มีการตรา “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” ขึ้นมา ประกอบกับกระทรวงสาธารณสุขมีนโยบายจัดเก็บประวัติสุขภาพของผู้ที่มารับบริการในโรงพยาบาลหรือสถานพยาบาลที่อยู่ในการกำกับดูแลของภาครัฐให้อยู่ในระบบอิเล็กทรอนิกส์ทั้งหมด โดยเรียกว่า “ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล” ทดแทนการบันทึกเวชระเบียนแบบเดิมที่เป็นเอกสารเพื่อให้ทันกับยุคการติดต่อสื่อสารไร้พรมแดน การนำระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลมาใช้วัตถุประสงค์หลัก คือ เพื่อให้ประชาชนสามารถเข้าถึงและบริหารจัดการข้อมูลสุขภาพของตนเองได้เอง ผ่านการเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เช่น คอมพิวเตอร์ (Computer) คอมพิวเตอร์พกพา (Tablet) หรือ อุปกรณ์อิเล็กทรอนิกส์ที่สามารถเชื่อมต่อกับอุปกรณ์อื่น ๆ ผ่านทางเครือข่ายไร้สาย (Smart Devices) แต่การเข้าถึงข้อมูลได้ง่ายทำให้เกิดการละเมิดข้อมูลหรือข้อมูลส่วนบุคคลถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ยินยอมได้ง่ายเช่นกัน ข้อมูลที่ถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ยินยอม

จากการศึกษาแนวทางการคุ้มครองส่วนบุคคลด้านสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ตามกฎหมายไทยและกฎหมายต่างประเทศ ดังที่ได้กล่าวมาแล้วใน บทที่ 2 ในส่วนนี้ผู้วิจัยจะนำเสนอผลการวิเคราะห์ ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และ

พระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (HIPAA) เพื่อนำมาเสนอเป็นมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ของผู้มารับบริการในโรงพยาบาลกรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลของประเทศไทยต่อไป

มาตรการคุ้มครองข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์

ในอดีตโรงพยาบาลจะบันทึกข้อมูลส่วนบุคคลของผู้มารับบริการ ประวัติสุขภาพ และความเห็นของแพทย์ผู้รักษา บันทึกรวมกันในเอกสารที่เรียกว่าเวชระเบียน เวชระเบียนจึงเป็นเอกสารที่ต้องได้รับการคุ้มครองเนื่องจากเป็นข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล กฎหมายคุ้มครองข้อมูลสุขภาพส่วนบุคคลของประเทศไทยที่ผู้วิจัยทำการศึกษา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ซึ่งเป็นกฎหมายที่คุ้มครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล จากการศึกษาพบว่ากรอบในการคุ้มครองข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ยังไม่ชัดเจนและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลยังไม่ทัดเทียมกับกฎหมายต่างประเทศ เช่น GDPR และ HIPAA ผลการศึกษาแสดงการเปรียบเทียบกฎหมายในตาราง 1 ดังนี้

ตาราง 1 แสดงการเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 GDPR และ HIPAA

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
1. หลักการคุ้มครอง	- กฎหมายทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล ของประชาชนไทย	- กฎหมายเฉพาะ ในการคุ้มครองข้อมูลสุขภาพของประชาชนไทย	- กฎหมายทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลทั่วไปและข้อมูลสุขภาพ ของสหภาพยุโรป	- กฎหมายเฉพาะ ในการคุ้มครองข้อมูลสุขภาพของสหรัฐอเมริกา
2. นิยาม				
- ข้อมูลส่วนบุคคล	- ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ที่เสียชีวิต	-ข้อมูลด้านสุขภาพของบุคคล คือ ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสาร แฟ้ม รายงาน ภาพถ่าย ฟิล์ม การบันทึกภาพและเสียงหรือสิ่งที่บันทึกไว้ ปรากฏขึ้นในเรื่องสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้	- ข้อมูลของบุคคลธรรมดาที่ยังมีชีวิตอยู่และสามารถทำให้ระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม	- ข้อมูลสุขภาพ คือข้อมูลด้านสุขภาพร่างกายและสุขภาพจิตที่ทำให้ระบุตัวบุคคลได้ รวมถึงข้อมูลที่สร้างขึ้นจากผู้ให้บริการด้านสุขภาพ โดยเจ้าของข้อมูลสุขภาพยังมีชีวิตหรือเสียชีวิตแล้วไม่เกิน 50 ปี
- ผู้ควบคุมข้อมูลส่วนบุคคล	- ผู้ที่มีอำนาจ เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	- ส่วนราชการ หน่วยงานในสังกัดกระทรวงสาธารณสุขและสถานพยาบาล ตาม พรบ.	- บุคคลหรือนิติบุคคล ทำหน้าที่กำหนดวัตถุประสงค์ และวิธีการประมวลผลข้อมูล	- ไม่ได้นิยามไว้

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
		สถานพยาบาล พ.ศ. 2541 ซึ่งเป็นผู้จัดทำ เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล		
– ผู้ประมวลผลข้อมูลส่วนบุคคล	– ผู้ที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล แต่ไม่ใช่บุคคลหรือนิติบุคคลคนเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล	– มิได้นิยามไว้ แต่นิยามคำว่า “ผู้บริหารจัดการข้อมูล” คือ กระทรวงสาธารณสุขรวมถึงบุคคลหรือหน่วยงานที่ได้รับมอบหมายจากกระทรวงสาธารณสุขให้ดำเนินการเก็บข้อมูล รวบรวมข้อมูล ใช้และเปิดเผยข้อมูล	– ผู้ทำหน้าที่ บันทึก จัดการข้อมูล เก็บ รวบรวม ใช้ เปิดเผยข้อมูล หรือวิเคราะห์ข้อมูล อาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล	– ไม่ได้นิยามไว้
– เจ้าของข้อมูลส่วนบุคคล	– ไม่ได้นิยามไว้	– บุคคลผู้เป็นเจ้าของข้อมูลด้านสุขภาพ	– บุคคลธรรมดาที่ข้อมูลนั้นระบุถึง ซึ่งข้อมูลนั้นถูกนำไปเก็บรวบรวม ใช้ หรือเปิดเผย	– บุคคลผู้เป็นเจ้าของข้อมูลสุขภาพกายและสุขภาพจิต

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
3.สิทธิของเจ้าของข้อมูลส่วนบุคคล				
– การเข้าถึงข้อมูลส่วนบุคคล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลของตน รวมถึงให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยที่มาของข้อมูลที่ตนไม่ได้ให้ความยินยอม	– เจ้าของข้อมูล ผู้รับมอบอำนาจจากเจ้าของข้อมูล และผู้ที่ได้รับความยินยอมจากเจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลส่วนบุคคล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิรับทราบวัตถุประสงค์การจัดเก็บข้อมูล ที่มาของข้อมูล ระยะเวลาที่คาดว่าจะใช้ข้อมูล และมีสิทธิเข้าถึงข้อมูลของตน	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลของตนเพื่อตรวจสอบความถูกต้องของข้อมูล
– การขอสำเนาข้อมูลส่วนบุคคล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลสำเนาข้อมูลที่เกี่ยวกับตน	– เจ้าของข้อมูล ผู้รับมอบอำนาจจากเจ้าของข้อมูล และผู้ที่ได้รับความยินยอมจากเจ้าของข้อมูลมีสิทธิขอสำเนาข้อมูลส่วนบุคคล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลสำเนาข้อมูลที่เกี่ยวกับตนในรูปแบบอิเล็กทรอนิกส์หรือรูปแบบอื่น	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอสำเนาข้อมูลสุขภาพของตนได้ตลอดระยะเวลาที่ข้อมูลถูกบันทึกไว้
– การคัดค้านการใช้ข้อมูลส่วนบุคคล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านดำเนินการเก็บข้อมูล รวบรวมข้อมูล ใช้และเปิดเผยข้อมูลที่เกี่ยวกับตน	– ไม่ได้ระบุไว้	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน	–เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
– การลบข้อมูล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลที่จัดเก็บหรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้	– ไม่ได้ระบุไว้	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูล ในกรณี 1.ข้อมูลหมดความจำเป็น 2.ถอนความยินยอม 3.คัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน 4.การประมวลผลข้อมูลส่วนบุคคลมิชอบด้วยกฎหมาย	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ลบข้อมูลที่ไม่ต้องการให้จัดเก็บไว้
– การแก้ไข	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขหรือดำเนินการให้ข้อมูลที่เกี่ยวกับตนถูกต้องและเป็นปัจจุบัน	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลสุขภาพของตน ตามหลักฐานที่แสดง	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนแก้ไขข้อมูลให้ถูกต้องสมบูรณ์	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้หน่วยงานที่เก็บรวบรวมข้อมูล แก้ไขข้อมูลสุขภาพโดยหน่วยงานต้องดำเนินการภายใน 60 วัน นับจากวันที่รับคำร้อง
– จำกัดการประมวลผล	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องขอให้ผู้ควบคุมข้อมูล	– ไม่ได้ระบุไว้	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิจำกัดการประมวลผล ใน	– ไม่ได้ระบุไว้

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
	ส่วนบุคคลแก้ไขหรือดำเนินการให้ข้อมูลที่เกี่ยวกับตนถูกต้องและเป็นปัจจุบัน		กรณีข้อมูลหมดความจำเป็นหรือการประมวลผลข้อมูลส่วนบุคคลมิชอบด้วยกฎหมาย แต่ข้อมูลดังกล่าวจำเป็นต่อเจ้าของข้อมูลส่วนบุคคล	
- รับการแจ้งเตือนจากผู้ควบคุมข้อมูลส่วนบุคคล	- เมื่อเกิดการละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุให้เจ้าของข้อมูลทราบภายใน 72 ชั่วโมง	- ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ในกรณีแก้ไขข้อมูลสุขภาพ	- ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ในกรณี 1.แก้ไข ลบ หรือจำกัดการประมวลผล ภายใน 30 วัน 2. เกิดการละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับตั้งแต่เกิดการละเมิด	- เมื่อเกิดการละเมิดข้อมูลส่วนบุคคล หน่วยงานที่เกี่ยวข้องต้องแจ้งเหตุต่อ เจ้าของข้อมูลภายใน 60 วัน นับตั้งแต่เกิดการละเมิด
- ส่งต่อข้อมูลส่วนบุคคลของตน	- ส่งต่อข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง	- ไม่ได้ระบุไว้	- ส่งต่อข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง	- เจ้าของข้อมูลสุขภาพไม่มีสิทธิส่งต่อข้อมูลของตนไปยังบุคคลที่สามได้

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
–ปฏิเสธการวินิจฉัยหรือการประมวลผลจากการประมวลผลอัตโนมัติ	– ไม่ได้ระบุไว้	– ไม่ได้ระบุไว้	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ปฏิเสธการวินิจฉัยหรือการประมวลผลจากการประมวลผลอัตโนมัติ	– ไม่ได้ระบุไว้
– การให้ความยินยอม	– ผู้เยาว์อายุน้อยกว่า 10 ปีบริบูรณ์ ผู้ปกครองต้องให้ความยินยอม	– ผู้เยาว์อายุ 15 ปีบริบูรณ์ ต้องได้รับความยินยอมจากผู้เยาว์ก่อน	–เยาวชนที่อายุต่ำกว่า 16 ปี จะต้องมีผู้ปกครองเป็นผู้ให้ความยินยอมในการนำข้อมูลส่วนบุคคลของไปใช้ ในกรณีที่ประเทศสมาชิกมีข้อกำหนดอายุที่ต่ำกว่านั้นก็สามารถบังคับใช้ได้	– อายุของผู้เยาว์ในการให้ความยินยอม ขึ้นอยู่กับบทบัญญัติของกฎหมายแต่ละรัฐ
4. บทลงโทษ				
– ความรับผิดทางแพ่ง/การเยียวยาผู้เสียหาย	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ฟ้องร้องต่อศาล เรียกร้องให้ผู้ที่ละเมิดข้อมูลที่เกี่ยวกับตนชดใช้ค่าสินไหมทดแทน แต่ไม่เกิน 2 เท่าของค่าสินไหมที่	– ไม่ได้ระบุไว้ แต่ให้ยึดตามหลักกฎหมายอื่นที่เกี่ยวข้อง	– เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการชดเชยค่าเสียหายจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลข้อมูลส่วนบุคคล ในกรณีการเก็บและ	– แบ่งระดับการละเมิดข้อมูลสุขภาพเป็น 4 ระดับคือ 1. ไม่รู้ตัวและไม่สามารถหลีกเลี่ยงได้ ปรับตั้งแต่ 100 – 50,000ดอลล่าสหรัฐ ต่อการ

ประเด็น / กฎหมาย	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
	แท้จริง		ประมวลผลนั้นไม่ปฏิบัติตามหลักของ GDPR จนก่อความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล	ละเมิด 1 ครั้ง 2.ปฏิบัติตามระเบียบแต่ไม่สามารถหลีกเลี่ยงการละเมิดข้อมูล ได้ ปรับตั้งแต่ 1,000 – 50,000 ดอลล่าสหรัฐ ต่อการละเมิด 1 ครั้ง 3.ละเลยการปฏิบัติตามระเบียบ ปรับตั้งแต่ 10,000 – 50,000 ดอลล่าสหรัฐ ต่อการละเมิด 1 ครั้ง 4.ละเลยการปฏิบัติตามระเบียบและไม่พยายามแก้ไขเมื่อรู้เหตุแห่งการละเมิด ได้ ปรับตั้งแต่ 50,000 ดอลล่าสหรัฐขึ้นไป ต่อการละเมิด 1 ครั้ง
- โทษทางอาญา	- ใช้และเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม	- ไม่ได้ระบุไว้ แต่ให้ยึดตามหลักกฎหมายอื่นที่เกี่ยวข้อง	-ไม่มีบทลงโทษอาญา หรือจำคุก	- ใช้ หรือเป็นเหตุให้ใช้ลักษณะเฉพาะด้านสุขภาพ หรือ

ประเด็น / กฎหมาย	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
	จนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล โทษสูงสุด จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ - ใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รู้มาจากการปฏิบัติหน้าที่ ให้บุคคลอื่นรับทราบ โทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ - นิติบุคคลที่ละเว้นการสั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ต้องรับโทษตามที่บัญญัติ			เปิดเผยข้อมูลสุขภาพที่สามารถระบุตัวบุคคล ต้องระวางโทษปรับไม่เกิน 50,00 ดอลล่าสหรัฐ จำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ -กระทำผิดจากการอ้างสิทธิโดยมิชอบต้องระวางโทษปรับไม่เกิน 100,00 ดอลล่าสหรัฐ จำคุกไม่เกิน 5ปี หรือทั้งจำทั้งปรับ - ขายข้อมูล โอนย้ายข้อมูลหรือใช้ข้อมูลสุขภาพที่ระบุตัวบุคคลเพื่อประโยชน์ทางการค้าหรือประโยชน์ส่วนตนจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลสุขภาพ ต้องระวางโทษปรับไม่เกิน 250,00 ดอลล่าสหรัฐ

กฎหมาย / ประเด็น	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561	GDPR	HIPAA
– โทษทางปกครอง	– คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งปรับทางปกครองโดยใช้ดุลยพินิจ ระวางโทษปรับทางปกครองสูงสุดไม่เกิน 5 ล้านบาท	– ไม่ได้ระบุไว้ แต่ให้ยึดตามหลักกฎหมายอื่นที่เกี่ยวข้อง	– หน่วยงานที่กำกับดูแลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักของ GDPR จนก่อความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลหรือทำให้ข้อมูลถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ให้ความยินยอม โทษปรับสูงสุด 20 ล้านยูโร หรือ ร้อยละ 2– 4 ของรายได้ต่อปีทั่วโลกขึ้นอยู่กับวงเงินใดสูงกว่า	จำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ – ไม่มีบทบัญญัติลงโทษทางปกครอง

ที่มา: ผู้วิจัย

จากตารางเปรียบเทียบจึงควรกำหนดมาตรการในการคุ้มครองข้อมูลอย่างเป็นระบบดังนี้

1. จัดให้มีขั้นตอนในการกำหนดข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ ซึ่งประกอบด้วย 5 องค์ประกอบดังนี้

1.1 กำหนดให้มีนิยามความหมายของเจ้าของข้อมูลส่วนบุคคลและกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลผู้เป็นเจ้าของข้อมูลสุขภาพ[111] ซึ่งเป็นบุคคลธรรมดาที่ยังมีชีวิตอยู่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรมแล้วแต่ไม่เกิน 50 ปี[112]

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1) สิทธิในการได้รับแจ้งข้อมูล หมายถึง ผู้ควบคุมข้อมูลต้องแจ้งวัตถุประสงค์ของการเก็บข้อมูลให้เจ้าของข้อมูลส่วนบุคคลก่อนที่จะทำการบันทึกหรือขณะที่กำลังบันทึกข้อมูล[113] แจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลส่วนบุคคลจะถูกจัดเก็บเป็นระยะเวลานานเท่าใด[114] และใครคือผู้รับข้อมูล

2) สิทธิในการเข้าถึงข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลของตนเองได้ตลอดเวลาที่ข้อมูลถูกจัดเก็บไว้รวมถึงขอรับสำเนาที่เกี่ยวกับตนจากผู้ควบคุมข้อมูล[115] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลนั้นอยู่ในรูปแบบที่อ่านง่ายหรือใช้งานได้ด้วยเครื่องมืออัตโนมัติ[116]

3) สิทธิในการแก้ไขข้อมูล เมื่อพบว่าข้อมูลที่จัดเก็บไว้ผิดพลาดหรือมีความบกพร่อง เจ้าของข้อมูลส่วนบุคคลมีสิทธิแจ้งและร้องขอให้ผู้ควบคุมข้อมูลดำเนินการแก้ไขทันที[117]และข้อมูลต้องได้รับการแก้ไขภายในระยะเวลา 60วัน นับตั้งแต่ยื่นคำร้อง[118]

---

[111] ข้อ 4 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[112] The Code of Federal Regulations Title 45 Section 160.103

[113] มาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[114] Article 13(2)(a) General Data Protection Regulation

[115] Article 15 General Data Protection Regulation

[116] มาตรา 30 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[117] Article 16 General Data Protection Regulation

[118] The Code of Federal Regulations Title 45 Section 164.526

4) สิทธิในการลบข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลดำเนินการลบข้อมูลที่จัดเก็บไว้เมื่อเห็นว่าการใช้ข้อมูลไม่เป็นไปตามวัตถุประสงค์ที่แจ้งไว้[119]หรือเจ้าของข้อมูลถอนความยินยอมที่ให้ไว้[120]

5) สิทธิในการระงับการใช้ข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลระงับการใช้ข้อมูลแทนการลบข้อมูล[121] ในกรณีที่ข้อมูลหมดความจำเป็นตามวัตถุประสงค์การใช้ข้อมูลหรือครบกำหนดระยะเวลาในการเก็บข้อมูล แต่เจ้าของข้อมูลเห็นว่าข้อมูลนั้นยังมีความจำเป็น เช่นกรณีที่เป็นคดีความทางกฎหมาย[122]

6) สิทธิปฏิเสธการให้ใช้ข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านให้ผู้ควบคุมข้อมูลหรือผู้ใช้ข้อมูล นำข้อมูลของตนไปใช้แม้ข้อมูลจะถูกจัดเก็บไปแล้ว เช่นในกรณีบริษัทบัตรเครดิตและประกันภัย[123]

1.2 กำหนดขั้นตอนในการรักษาความปลอดภัยข้อมูลส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ ดังนี้

1.2.1 กำหนดและจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล ของตัวเจ้าของข้อมูล

1.2.2 กำหนดและจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้มารับบริการจากผู้ใช้ข้อมูลแต่ละระดับอย่างชัดเจน[124]

12.3 กำหนดให้บันทึกและสำรองข้อมูลไว้ในระบบฐานข้อมูลที่ปลอดภัยได้มาตรฐาน สำรองข้อมูลสม่ำเสมอและทดสอบการนำข้อมูลที่สำรองไว้มาใช้งาน ว่าสามารถใช้ได้หรือไม่

1.2.4 การรักษาความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล ควรมีระบบป้องกัน
การบุกรุกเครือข่ายและกำหนดรหัสผ่านของแต่ละบุคคลในการเข้าใช้งานในระบบ[125]

---

[119] Article 17 General Data Protection Regulation

[120] มาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[121] มาตรา 34 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[122] Article 18 General Data Protection Regulation

[123] Article 21 General Data Protection Regulation

[124] ข้อ 26 (3) แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

1.2.5 วางแผนซ้อมกู้และแก้ไขระบบจัดเก็บข้อมูลสม่ำเสมอ

1.2.6 วิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล

1.3 ระบุแหล่งที่มาของข้อมูล เส้นทางการส่งข้อมูลและความเชื่อมโยงของข้อมูลในระบบดังต่อไปนี้

1.3.1 เจ้าของข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูลเมื่อมีการลงทะเบียนเข้าใช้งานในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

1.3.2 ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้รับข้อมูล ที่เจ้าของข้อมูล ไปรับบริการ

1.3.3 ผู้รับข้อมูล นำข้อมูลไปใช้เพื่อประโยชน์แก่เจ้าของข้อมูล แล้วส่งข้อมูลกลับไปยังผู้ควบคุมข้อมูล

1.3.4 ผู้ควบคุมข้อมูล ส่งข้อมูลให้กับบุคคลภายนอกเมื่อเจ้าของข้อมูลหรือผู้แทนโดยชอบธรรมร้องขอ

1.4 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบที่จัดเก็บข้อมูล

1.4.1 การประเมินปัจจัยความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ ประกอบด้วย[126]

1) ปัจจัยภายนอกได้แก่[127]

1.1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของ เครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

1.2) การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

---

[125] ข้อ 26 (4) แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[126] สุรทศ ไตรติลานันท์ และสุรพล รวยสูงเนิน, "กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล," ใน **วารสารวิชาการพระจอมเกล้าพระนครเหนือ** (2559).

[127] สำนักงานปลัดกระทรวงเกษตรและสหกรณ์, **แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร**, ค้นวันที่ 2 ธันวาคม 2561 จาก https://wwwnno.moph.go.th/downloads/policy/570813ictriskplan.pdf.

1.3) การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

1.4) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

1.5) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

1.6) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2) ปัจจัยภายในได้แก่[128]

2.1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.2) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้ภายในองค์กร

2.3) เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

1.4.2 ประเมินโอกาสที่จะเกิดความเสี่ยง และผลกระทบของเหตุการณ์ที่อาจกระทบต่อข้อมูลที่จัดเก็บไว้ ประกอบด้วยปัจจัยดังนี้[129]

1) โอกาสที่จะเกิดความเสี่ยง หมายถึง เหตุการณมีโอกาสที่จะเกิดขึ้นมากน้อยเพียงใดและประเมินออกมาในลักษณะใด ซึ่งเกณฑ์ที่ใช้ในการประเมิน 5 ระดับ ดังที่แสดงใน ตาราง 2

---

[128] เรื่องเดียวกัน, หน้า 8.

[129] ศูย์เทคโนโลยีสารสนเทศและการสื่อสาร, **แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**, ค้นวันที่ 2 ธันวาคม 2561 จาก https://wwwnno.moph.go.th/downloads/policy/570813ictriskplan.pdf.

ตาราง 2 ตารางการประเมินโอกาสที่จะเกิดความเสี่ยง[130]

ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง	คำอธิบาย
1	สูงมาก	มีโอกาสเกิดขึ้นเป็นประจำทุกวัน
2	สูง	มีโอกาสเกิดขึ้นทุกสัปดาห์
3	ปานกลาง	มีโอกาสเกิดขึ้นทุกเดือน
4	น้อย	มีโอกาสเกิดขึ้นทุกปี
5	น้อยมาก	ไม่เกิดเลยหรือ ไม่มีโอกาสเกิด

2) ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่อาจจะเกิดขึ้น พิจารณาจากการนำปัจจัยต่าง ๆ มาวิเคราะห์ว่า หากเกิดขึ้นแล้วมีผลกระทบมากหรือน้อยแค่ไหน และเกณฑ์ที่ใช้ในการประเมินผลกระทบของความเสี่ยงมี 2 ด้าน คือ ด้านการดำเนินงานและด้านกฎหมาย

2.1) ผลกระทบดำเนินงาน หมายถึง ความเสี่ยงที่เกิดจากระบบภายในองค์กร เกิดจากตัวบุคลากร หรือเกิดจากข้อมูล จนส่งผลกระทบต่อการดำเนินงานของหน่วยงาน เกณฑ์การประเมิน ดังตาราง 3

ตาราง 3 เกณฑ์การประเมินผลกระทบของความเสี่ยงด้านการดำเนินงาน[131]

ผลกระทบ	ระดับคะแนน	คำอธิบาย
สูงมาก	5	กระทบต่อกระบวนการทำงานของทั้งองค์กร
สูง	4	กระทบต่อกระบวนการทำงานระหว่างส่วนงานมากกว่า 3 ส่วนงาน
ปานกลาง	3	กระทบต่อกระบวนการทำงานระหว่างส่วนงานมากกว่า 2 ส่วนงาน
น้อย	2	มีกระทบต่อกระบวนการทำงานภายในส่วนงาน
น้อยมาก	1	ไม่มีผลกระทบต่อกระบวนการทำงานในองค์กร

---

[130] สำนักงานปลัดกระทรวงเกษตรและสหกรณ์, **"แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร."** หน้า 55.

[131] เมธา สุวรรณสาร, **แนวทาง/กรอบการบริหารความเสี่ยงทั่วทั้งองค์กร**, ค้นวันที่ 2 เมษายน 2562 จาก http://www.itgthailand.com/tag/risk-assessment-matrix/.

2.2) ผลกระทบด้านนโยบาย กฎหมายและระเบียบข้อบังคับต่าง ๆ หมายถึง ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามนโยบาย กฎหมาย ข้อบังคับที่เกี่ยวข้อง หรือนโยบาย กฎหมาย ข้อบังคับที่มีอยู่ไม่เหมาะสมกับการนำมาใช้ เกณฑ์การประเมิน ดังตาราง 4

ตาราง 4 เกณฑ์การประเมินผลกระทบของความเสี่ยงด้านนโยบาย กฎหมายและระเบียบข้อบังคับ[132]

ผลกระทบ	ระดับคะแนน	คำอธิบาย
สูงมาก	5	เกิดการฟ้องร้องดำเนินคดี และเรียกค่าเสียหาย รวมถึงการฟ้องร้องที่เกิดจากการรวมตัวกันของผู้ที่ได้รับความเสียหาย
สูง	4	การละเมิดข้อกฎหมายที่สำคัญ
ปานกลาง	3	การฝ่าฝืนกฎหมายที่สำคัญ ที่มีการสอบสวนหรือรายงานไปยังหน่วยงานที่เกี่ยวข้อง รวมทั้งการดำเนินคดีและ/หรือเรียกร้องค่าเสียหาย
น้อย	2	การละเมิดข้อกฎหมายที่ไม่มีนัยสำคัญ
น้อยมาก	1	การไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับที่ไม่มีนัยสำคัญ

3) ประเมินระดับความเสี่ยง โดยใช้สูตร ดังนี้

ระดับความเสี่ยง = โอกาสที่จะเกิดความเสี่ยง x ผลกระทบของความเสี่ยง (ดังตาราง 5)

[132] เรื่องเดียวกัน.

ตาราง 5 แสดงการประเมินระดับความเสี่ยง[133]

ระดับความเสี่ยง			โอกาสที่จะเกิดความเสี่ยง				
			ต่ำมาก / น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก / บ่อยมาก
			1 คะแนน	2คะแนน	3คะแนน	4คะแนน	5คะแนน
ผลกระทบของความเสี่ยง	สูงมาก	5 คะแนน	5	10	15	20	25
	สูง	4 คะแนน	4	8	12	16	20
	ปานกลาง	3 คะแนน	3	6	9	12	15
	น้อย	2 คะแนน	2	4	6	8	10
	น้อยมาก	1 คะแนน	1	2	3	4	5
ระดับความเสี่ยง							

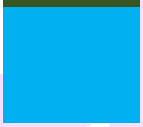
ซึ่งเมื่อประเมินระดับความเสี่ยงออกมาจะแบ่งเกณฑ์ในการประเมินระดับความเสี่ยงออกเป็น 5 ระดับ ดังตาราง 6

ตาราง 6 แสดงเกณฑ์ระดับความเสี่ยง[134]

ระดับความเสี่ยง	**ระดับคะแนน**	**แทนด้วยแถบสี**	**คำอธิบาย**
สูงมาก	15 – 25		ระดับความเสี่ยงสูงมาก คือมีโอกาสเกิดมากที่สุด และส่งผลกระทบต่อองค์กรระดับสูงไม่สามารถยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง
สูง	7 – 14		ระดับความเสี่ยงสูง คือมีโอกาสเกิดมากแม้เกิดแล้วไม่กระทบองค์กรก็ถือว่าเสี่ยงสูง หรือโอกาสเกิดน้อยแต่ผลกระทบสูง ไม่สามารถยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง

[133] ศูย์เทคโนโลยีสารสนเทศและการสื่อสาร, "**แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**." หน้า 28

[134] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC),**"ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล–Phr."**

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแถบสี	คำอธิบาย
ปานกลาง	3 – 6		ระดับความเสี่ยงปานกลาง คือมีโอกาสเกิดบ้าง หากเกิดแล้วกระทบกับองค์กรไม่มากนัก แต่ต้องมีแผนควบคุมความเสี่ยง
ต่ำ	1 – 2		ระดับความเสี่ยงต่ำ โอกาสเกิดน้อย หากเกิดแล้วโอกาสกระทบต่อองค์กรต่ำ

1.4.3 การจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ กรณีที่ระบบนำเสนอข้อมูลผิดพลาด หรือข้อมูลสุขภาพที่สำคัญหรือเป็นความลับ ถูกเปิดเผยหรือเผยแพร่ ทำได้โดย

1) จัดทำและประกาศใช้นโยบายป้องกันข้อมูลรั่วไหล

2) จัดอบรมให้ความรู้เกี่ยวกับการป้องกันความปลอดภัยของข้อมูลในองค์กร

3) จัดทำระบบการรักษาความปลอดภัยของข้อมูลที่มีระดับความลับสูง

1.5 กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในทุกขั้นตอน โดยกำหนดสิทธิและบทบาทของผู้เกี่ยวข้องกับข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ให้ชัดเจนเป็นลายลักษณ์อักษร ดังนี้

ผู้ควบคุมข้อมูล (Data Controller) หมายถึง ส่วนราชการหรือหน่วยงานในสังกัดกระทรวงสาธารณสุขและหน่วยงานของรัฐหน่วยอื่นที่ประสงค์เข้าร่วมใช้ข้อมูลสุขภาพ[135]

ผู้ประมวลผลข้อมูล (Data Processor) หรือผู้รับข้อมูล หมายถึงบุคคลหรือนิติบุคคล ที่ได้รับข้อมูลสุขภาพจากผู้ควบคุมข้อมูลและประมวลผลข้อมูลตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูล บันทึกและจัดเก็บข้อมูลแล้วนำข้อมูลสุขภาพนั้นไปใช้เพื่อประโยชน์แก่เจ้าของข้อมูล[136]

---

[135] ข้อ 4 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

1.5.1 ผู้ควบคุมข้อมูล มีหน้าที่ ดังนี้

1) จัดให้มีมาตรการเชิงเทคนิคที่ถูกต้องตามกฎหมาย ในการจัดเก็บและบริหารข้อมูลเพื่อประมวลผล[137]

2) จัดให้มีการขออนุญาต และอนุมัติคำร้อง ในการขอเข้าถึงระบบอิเล็กทรอนิกส์ที่จัดเก็บข้อมูลส่วนบุคคลไว้[138]

3) จัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจเพื่อรักษาความปลอดภัยของข้อมูล[139]

4) รายงานเหตุการณ์ความเสี่ยง เช่นข้อมูลถูกเผยแพร่สาสาธารณะโดยเจ้าของข้อมูลไม่ได้ให้ความยินยอมหรือมีการละเมิดข้อมูล ให้เจ้าของข้อมูลและผู้บริหารจัดการข้อมูลทราบ ภายใน 72 ชั่วโมง นับตั้งแต่เกิดเหตุการณ์[140]

5) เก็บและส่งต่อข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูล

6) ประเมินผลกระทบที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคลที่จัดเก็บ

7) เลือกประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการข้อมูลที่เหมาะสม

8) จัดให้มีระบบตรวจสอบข้อมูลส่วนบุคคลที่จัดเก็บไว้เพื่อลบหรือทำลายข้อมูลเมื่อครบกำหนดเวลาในการเก็บรักษาข้อมูล[141]

9) แต่งตั้งบุคคลทำหน้าที่ดูแลคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ[142]

10) มีหน้าที่โดยตรงต่อเจ้าของข้อมูลส่วนบุคคลในการที่ต้องปฏิบัติตามการใช้สิทธิของเจ้าของข้อมูล

1.5.2 ผู้ประมวลผลข้อมูล มีหน้าที่ ดังนี้

---

[136] เรื่องเดียวกัน.

[137] ข้อ 25 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[138] ข้อ 25(1) แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

[139] The Code of Federal Regulations Title 45 Section 164.404

[140] GDPR ฉบับภาษาไทย, เรื่องเดียวกัน, หน้า 152.

[141] GDPR ฉบับภาษาไทย, เรื่องเดียวกัน, หน้า 149.

[142] มาตรา 41 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1) จัดให้มีมาตรการเชิงเทคนิคเพื่อรักษาความมั่นคงปลอดภัยเพื่อการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง[143]

2) เก็บบันทึกข้อมูลส่วนบุคคลที่ได้ประมวลผลแล้ว[144]

3) ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล[145]

4) ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล[146]

5) กรณีข้อมูลส่วนบุคคลถูกเผยแพร่สู่สาธารณะโดยเจ้าของข้อมูลไม่ได้ให้ความยินยอมผู้ประมวลผลต้องแจ้งเหตุให้ผู้ควบคุมข้อมูลทราบโดยเร็ว

6) ผู้ประมวลผลข้อมูลต้องแจ้งให้ผู้ควบคุมทราบหากพบว่ามีทางเลือกในการประมวลผลที่มีความปลอดภัยสูงกว่า

1.6 กำหนดบทลงโทษเมื่อพบการละเมิดข้อมูลส่วนบุคคล

1.6.1 บทลงโทษทางแพ่ง แบ่งระดับการลงโทษ 4 ระดับ[147]

1) ผู้มีส่วนเกี่ยวข้องละเมิดข้อมูลส่วนบุคคลโดยไม่รู้ตัวและไม่สามารถหลีกเลี่ยงการละเมิดข้อมูลได้ ปรับตั้งแต่ 100 – 50,000 บาท ต่อการละเมิด 1 ครั้ง

2) ผู้มีส่วนเกี่ยวข้องปฏิบัติตามระเบียบแต่ไม่สามารถหลีกเลี่ยงการละเมิดข้อมูล ได้ ปรับตั้งแต่ 1,000 – 50,000 บาท ต่อการละเมิด 1 ครั้ง

3) ผู้มีส่วนเกี่ยวข้องละเลยการปฏิบัติตามระเบียบ ปรับตั้งแต่ 10,000 – 50,000 บาทต่อการละเมิด 1 ครั้ง

4) ผู้มีส่วนเกี่ยวข้องละเลยการปฏิบัติตามระเบียบและไม่พยายามแก้ไขเมื่อรู้เหตุแห่งการละเมิด ได้ ปรับตั้งแต่ 50,000 บาทขึ้นไป แต่ไม่เกิน 2 เท่าของความเสียหายที่เกิดขึ้นต่อการละเมิด 1 ครั้ง[148]

1.6.2 บทลงโทษทางอาญา

1) ผู้มีส่วนเกี่ยวข้องใช้และเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความ

---

[143] มาตรา 40(2) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[144] มาตรา 40(3) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[145] มาตรา 41 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[146] มาตรา 40(1) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[147] HIPAA Journal, Ibid.

[148] มาตรา 78 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ยินยอมจากเจ้าของข้อมูลส่วนบุคคล จนทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย เสียชื่อเสียง โทษสูงสุดคือจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ[149]

2) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รู้มาจากการปฏิบัติหน้าที่แก่ผู้อื่น ต้องรับโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ[150]

3) ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล กรรมการหรือผู้จัดการต้องรับผิดในกรณีที่บุคคลดังกล่าวสั่งการ ละเว้นการสั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้[151]

1.6.3 บทลงโทษทางปกครอง คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองโดยใช้ดุลพินิจ[152]

2. จัดให้มีมาตรฐานเกี่ยวกับความยินยอมในการจัดเก็บข้อมูลสุขภาพไว้ในระบบอิเล็กทรอนิกส์

2.1 เนื้อหาที่ขอความยินยอม

2.1.1 วัตถุประสงค์ของการเก็บ ใช้ และประมวลผลข้อมูล

2.1.2 ข้อมูลเบื้องต้นของผู้ควบคุมข้อมูล

2.1.3 ข้อมูลใดบ้างที่จะถูกเก็บ ใช้และประมวลผล

2.1.4 วิธีการที่ใช้ในการประมวลผล

2.1.5 การเปิดเผยข้อมูลต่อผู้ใช้ข้อมูลหรือบุคคลอื่น

2.1.6 ระยะเวลาในการเก็บ ใช้ข้อมูล

2.1.7 สิทธิต่าง ๆ ของเจ้าของข้อมูล

2.1.8 วิธีการถอนความยินยอม

2.2 หลักการขอความยินยอม

2.2.1 เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมอย่างเป็นอิสระโดยไม่มีเงื่อนไขหรือถูกบีบบังคับ[153]

---

[149] มาตรา 79 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[150] มาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[151] มาตรา 81 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[152] มาตรา 90 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[153] มาตรา 19 วรรคสี่ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.2.2 มีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอมแต่ละครั้งด้วยข้อความที่เข้าใจง่าย หากมีความจำเป็นต้องใช้ข้อมูลชุดเดียวกันในการประมวลผลข้อมูลหลายครั้ง เจ้าของข้อมูลส่วนบุคคลสามารถเลือกได้ว่าจะให้ความยินยอมสำหรับกรณีใดบ้าง

2.2.3 แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการประมวลผลตามวัตถุประสงค์ที่แจ้งไว้

2.2.4 เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ เว้นแต่สภาพของเจ้าของข้อมูลไม่อาจให้ความยินยอมโดยวิธีดังกล่าวได้จึงจะให้ผู้แทนโดยชอบธรรมให้ความยินยอมแทน และไม่ขอความยินยอมในแบบฟอร์มที่กำหนดให้โดยวิธีทำเครื่องหมายถูกในช่องที่กำหนดไว้[154]

2.2.5 กระบวนการถอนความยินยอมทำได้ง่ายไม่ยุ่งยากในระดับเดียวกันกับการให้ความยินยอม[155]

2.2.6 กรณีเจ้าของข้อมูลเป็นผู้เยาว์อายุน้อยกว่า 15 ปีบริบูรณ์ ต้องขอความยินยอมจากผู้แทนโดยชอบธรรม[156]

จากการศึกษาพบว่า ข้อมูลสุขภาพที่จัดเก็บในระบบอิเล็กทรอนิกส์ควรมีระดับความคุ้มครองสูงกว่าข้อมูลส่วนบุคคลทั่วไป เนื่องจากข้อมูลสุขภาพทางการแพทย์จัดว่าเป็นความลับของผู้ป่วย การเก็บรวบรวมและการใช้ข้อมูลสุขภาพมีประโยชน์หลายประการ เช่น เพื่อการรักษาพยาบาล เพื่อการพัฒนาและปรับปรุงการให้บริการด้านสาธารณสุข การควบคุมโรคและการป้องโรคติดต่อ เป็นต้น ด้วยเหตุนี้กฎหมายไทย กฎเกณฑ์ระหว่างประเทศ รวมถึงกฎหมายภายในของต่างประเทศหลายฉบับจึงได้กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพตามกฎหมายโดยคำนึงถึงความสมดุลระหว่างประโยชน์สาธารณะจากการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลด้านสุขภาพกับการคุ้มครองสิทธิของบุคคลซึ่งเป็นเจ้าของข้อมูลประกอบกัน ในส่วนของข้อมูลการรักษาซึ่งถือเป็นความลับของผู้ป่วย ได้แก่ ข้อมูลส่วนตัวของผู้ป่วยทุกอย่าง โดยส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับประวัติสุขภาพหรือการรักษาพยาบาล เช่น การตรวจวินิจฉัยโรค อาการของโรค ยาที่ใช้รักษา และถ้าหากเป็นการเจ็บป่วยที่ไม่เป็นไป

---

[154] มาตรา 19 วรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[155] มาตรา 19 วรรคห้า แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[156] ข้อ 14 แห่งระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

ตามปกติหรือมีผู้กระทำเมื่อข้อมูลถูกเปิดเผยไปแล้ว อาจทำให้ผู้ป่วยเกิดความอับอายหรือถูกคุกคามชีวิต เช่น กรณีผู้ป่วยถูกข่มขืนถูกทำร้ายร่างกาย หรือป่วยเป็นโรคที่สังคมรังเกียจ ยกตัวอย่างกรณี ผู้เป็นโรคเอดส์ได้เข้ารับการรักษาตัวในโรงพยาบาลหรือหน่วยงานหรือองค์กรที่จัดตั้งขึ้นเพื่อรักษาผู้ป่วย หากมีการนำข้อมูลประวัติการรักษามาเปิดเผยต่อสาธารณะ ถือเป็นการละเมิดข้อมูลส่วนบุคคลของผู้ป่วย

สิทธิทางด้านสุขภาพ เกิดจากสภาพยาบาลแห่งชาติของประเทศสหรัฐอเมริกา เล็งเห็นความสำคัญของการพิทักษ์สิทธิของผู้รับบริการในโรงพยาบาล โดยจัดการประชุมร่วมกันเพื่อประมวลสิทธิของผู้ป่วยที่พึงมีพึงได้จากการมารับบริการในโรงพยาบาล ซึ่งสาระสำคัญส่วนใหญ่เกี่ยวกับการเก็บความลับข้อมูลต่าง ๆ ของการวินิจฉัย การรักษาพยาบาล การยอมให้ผู้ป่วยตัดสินใจด้วยตนเองว่าจะทำอะไรบ้างในระหว่างที่เป็นผู้ป่วย หลังจากนั้นได้จัดทำเป็นคู่มือทางสิทธิและประกาศออกเป็นทางการในปี พ.ศ. 2516 เพื่อให้ผู้ป่วยเกิดความมั่นใจและรับรู้สิทธิของตนเอง แม้ว่าคำประกาศสิทธิไม่มีลักษณะเป็นกฎหมายที่จะบังคับให้ผู้ให้บริการด้านสุขภาพและโรงพยาบาลทุกแห่งต้องปฏิบัติตาม แต่เป็นสิ่งที่จำเป็นต้องมีเพื่อแสดงถึงความรับผิดชอบของโรงพยาบาลที่มีต่อผู้ป่วย สิทธิของผู้ป่วยในการที่จะได้รับการปกปิดข้อมูลไว้เป็นความลับ

หลักความรักษาลับของผู้ป่วย เป็นหลักการทางจริยศาสตร์ที่ได้รับการยอมรับและปฏิบัติกันมาอย่างเคร่งครัดต่อเนื่องตั้งแต่สมัยกรีซ และมีลักษณะเดียวกันในทุกประเทศทั่วโลก อาจจะ แตกต่างกันบ้างในส่วนของกฎหมายที่บัญญัติข้อยกเว้น ต่าง ๆ ซึ่งทำ ให้แพทย์สามารถเปิดเผยข้อมูลของผู้ป่วยได้ ปัจจุบันประเทศไทยได้บังคับใช้กฎหมายพระราชบัญญัติ สุขภาพแห่งชาติ พ.ศ. 2550 ซึ่งเป็นครั้งแรกที่มีการ กล่าวถึงข้อมูลด้านสุขภาพของบุคคลในกฎหมาย และในประกาศพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 นั้น ทุกสถานบริการทางการแพทย์และสาธารณสุขต้องมีการบริหารจัดการเวชระเบียน ซึ่งเป็นส่วนที่จะต้องมีการเก็บหลักฐานที่สมบูรณ์และสามารถใช้เป็นหลักฐานทางกฎหมายได้จริงตามที่ได้บัญญัติไว้ โดยมีมาตรการที่เกี่ยวข้องโดยตรงกับการบริหารจัดการเวชระเบียนและการรักษาความลับของผู้ป่วย คือ

1.กำหนดให้ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล ไม่สามารถนำไปเปิดเผยให้ผู้อื่นรู้ได้เพราะอาจก่อให้เกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูลสุขภาพได้ ยกเว้นแต่ว่าการเปิดเผยข้อมูลด้านสุขภาพนั้นเป็นไปตามความต้องการของเจ้าของข้อมูลหรือมีกฎหมายบัญญัติให้ต้องเปิดเผยไม่ว่ากรณี ใด ๆ หรืออ้างสิทธิตามกฎหมายว่าด้วยข้อมูล

ข่าวสารของทางราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่มิใช่ของตนมิได้

2.เจ้าของข้อมูลสุขภาพรวมถึงผู้แทนโดยชอบธรรมมีสิทธิที่จะได้รับทราบข้อมูลและเข้าถึงข้อมูลเกี่ยวกับการรักษาพยาบาลเฉพาะของตนที่ปรากฏในเวชระเบียนเมื่อร้องขอ ทั้งนี้ข้อมูลที่ร้องขอดังกล่าวต้องไม่เป็นการละเมิดสิทธิส่วนตัวของบุคคลอื่น และไม่ขัดต่อกฎหมาย

แต่ด้วยข้อจำกัดบางประการของการรักษาพยาบาลจำเป็นจะต้องมีการนำข้อมูลส่วนตัวของผู้ป่วยมาใช้ เจ้าหน้าที่ก็จะต้องปฏิบัติตามที่กำหนดไว้ การเปิดเผยความลับสามารถกระทำได้โดยไม่ขัดหลักต่อกฎหมาย เหตุแห่งการยกเว้นประกอบด้วยเหตุผลย่อย 2 ประการ คือ ความยินยอมของเจ้าของข้อมูลและอำนาจตามกฎหมาย ข้อยกเว้นที่เจ้าหน้าที่หรือผู้เกี่ยวข้องกับการรักษาสามารถเปิดเผยข้อมูลของผู้ป่วยได้ คือ

1. ในภาวะฉุกเฉินเร่งด่วน

2. ผู้ป่วยอยู่ในสภาวะไร้ความสามารถ

3. เพื่อปกป้องผู้อื่นจากอันตราย หรือเพื่อประโยชน์ต่อสังคมส่วนรวม

4. เพื่อประโยชน์ของผู้ป่วย เช่นการเปิดเผยให้บุคลากรอื่นในทีมสุขภาพที่มีส่วนเกี่ยวข้องกับการดูแลผู้ป่วย

5. เพื่อประโยชน์ของสาธารณะ เช่นการรายงานโรคติดต่อ โรคติดต่อทางเพศสัมพันธ์ การทารุณกรรมเด็ก

การเปิดเผยข้อมูลด้านสุขภาพของผู้ป่วยดังกล่าวต้องกระทำตามความจำเป็น ด้วยสัดส่วนการใช้ข้อมูลที่น้อยที่สุดอันจะสามารถบรรลุวัตถุประสงค์ของการเปิดเผยข้อมูลนั้นได้

ดังนั้นการเก็บข้อมูลของผู้มารับบริการในโรงพยาบาลไว้ในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล จำเป็นต้องมีมาตรการทางกฎหมายในการป้องปรามการกระทำผิดที่อาจจะเกิดขึ้น มีแนวปฏิบัติที่ชัดเจนเป็นรูปธรรมในเรื่องการเก็บรักษาข้อมูล การเปิดเผยข้อมูล การนำข้อมูลสุขภาพไปใช้ เพื่อสร้างความเชื่อมั่นแก่ผู้รับบริการว่าข้อมูลสุขภาพของตนได้รับการดูแลในระบบที่ปลอดภัย

การศึกษามาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ของผู้มารับบริการในโรงพยาบาลกรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

จากการศึกษาที่ได้กล่าวมาแล้วใน บทที่ 2 กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพที่ผู้วิจัยทำการศึกษาเปรียบเทียบกันระหว่างกฎหมายไทยกับกฎหมายต่างประเทศ ผู้วิจัยจึงวิเคราะห์ตามประเด็นดังนี้

1. นิยามข้อมูลสุขภาพส่วนบุคคล

เมื่อผู้รับบริการเข้ามาใช้บริการในโรงพยาบาล ข้อมูลพื้นฐานที่ใช้ประกอบการรักษาพยาบาล เพื่อใช้ระบุตัวของผู้มารับบริการในโรงพยาบาล ได้แก่ ชื่อ นามสกุล เพศ ศาสนา บ้านเลขที่ หมายเลขโทรศัพท์ เลขประจำตัวประชาชน หมายเลขโรงพยาบาล (Hospital Number–HN) ซึ่งข้อมูลดังกล่าวถือว่าเป็นข้อมูลพื้นฐานของผู้มารับบริการในโรงพยาบาล ข้อมูลสุขภาพส่วนบุคคล คือ ข้อมูลที่เกี่ยวกับสุขภาพ ประวัติการแพ้ยา ผลการตรวจทางห้องปฏิบัติการ เอกสารแสดงความยินยอมต่าง ๆ ของผู้รับบริการ บันทึกความเห็นของแพทย์ บันทึกทางการพยาบาล ข้อมูลดังกล่าวเป็นข้อมูลสุขภาพส่วนบุคคล ดังนั้นควรมีคำนิยาม “ข้อมูลสุขภาพส่วนบุคคล” อยู่ในกฎหมายที่บัญญัติมาเพื่อคุ้มครองข้อมูลส่วนบุคคล

ในส่วนของนิยาม ข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า ข้อมูลส่วนบุคคล ประกอบด้วย 2 องค์ประกอบ ได้แก่ ข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัว และข้อมูลที่สามารถทำให้ระบุตัวบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อม ยกตัวอย่างเช่น เพศ เชื้อชาติ ศาสนา หมายเลขบัตรประจำตัวประชาชน อัตลักษณ์ส่วนบุคคล อันได้แก่ ลายนิ้วมือ เสียง จอประสาทตา (Retinal) ส่วนสูง น้ำหนัก หมู่เลือด โรคประจำตัว เป็นต้น แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มีบทนิยามเกี่ยวกับข้อมูลสุขภาพ โดยเฉพาะมีเพียงบทบัญญัติว่า หน่วยงานใดที่ได้บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะแล้ว ให้ใช้บทบังคับตามกฎหมายนั้น ประเทศไทยจึงต้องยึดคำนิยาม ข้อมูลสุขภาพ ตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ซึ่งแตกต่างกับ GDPR ที่มีนิยามที่ชัดเจน ระหว่างข้อมูลส่วนบุคคลและ ข้อมูลสุขภาพ

GDPR บัญญัติว่าข้อมูลส่วนบุคคลคือ ข้อมูลของบุคคลธรรมดาที่ยังมีชีวิตอยู่และทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่นชื่อ หมายเลขประจำตัว ข้อมูลสถานที่อยู่ การระบุตัวตนทางออนไลน์หรือปัจจัยหนึ่งหรือหลายอย่างที่กล่าวถึงอันทำให้สามารถระบุลักษณะทางกายภาพ ลักษณะทางพันธุกรรม สภาพทางจิต เศรษฐกิจ วัฒนธรรม

หรือสังคม ซึ่ง GDPR มีบทนิยามเกี่ยวกับ ข้อมูลสุขภาพ[157]โดยเฉพาะ ว่าหมายถึงข้อมูลที่สัมพันธ์กับสถานะทางสุขภาพกาย สุขภาพจิต ทั้งในอดีต ปัจจุบันหรือที่อาจเกิดขึ้นในอนาคตของเจ้าของข้อมูลส่วนบุคคล รวมถึงข้อมูลที่เกิดจากการลงทะเบียนเพื่อรับบริการด้านสุขภาพ ข้อมูลที่เกิดจากการตรวจทางการแพทย์ ข้อมูลทางพันธุกรรม ข้อมูลการทดลองทางการแพทย์ เช่น ข้อมูลโรคประจำตัว ความพิการที่ตรวจพบ ประวัติทางการแพทย์รวมถึงการรักษาพยาบาล ข้อมูลจากการประมวลผลอย่าอิสระของบุคคลากรทางสาธารณสุขที่เกี่ยวข้อง

แต่คำนิยาม ข้อมูลส่วนบุคคลที่กล่าวมานั้น ข้อมูลของบุคคลที่เสียชีวิตแล้วไม่ได้รับการคุ้มครองตามของกฎหมายทั้ง 2 ฉบับนี้ จากการศึกษา พบว่าข้อมูลสุขภาพเป็นข้อมูลที่เกี่ยวกับประวัติการเจ็บป่วย ประวัติการรักษาพยาบาลเป็นหลัก ข้อมูลสุขภาพของผู้ที่เสียชีวิตแล้วจึงอาจเป็นประโยชน์ต่อผู้ที่เจ็บป่วยในปัจจุบัน จึงควรให้ความคุ้มครองข้อมูลสุขภาพของผู้ที่เสียชีวิตแล้วเช่นเดียวกับบุคคลที่ยังมีชีวิต

กฎหมายที่บัญญัติเกี่ยวกับข้อมูลสุขภาพที่ได้ทำการศึกษาได้แก่ ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติว่า ข้อมูลด้านสุขภาพของบุคคล[158] หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกในรูปเอกสาร การบันทึกภาพหรือเสียง ซึ่งการบันทึกนั้นอาจกระทำโดยการใช้เครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลส่วนบุคคลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด เช่น หมายเลขบัตรประจำตัวประชาชน น้ำหนัก ส่วนสูง หมู่เลือด ประวัติการรักษาพยาบาล เวชระเบียน บันทึกการรักษาพยาบาล ผลตรวจทางห้องปฏิบัติการ เช่นผลตรวจเลือด ปัสสาวะ อุจจาระ เสมหะและน้ำไขสันหลัง รวมถึงภาพหรือเสียงที่บันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้ แต่ไม่รวมถึง ชื่อ-สกุล อายุ อาชีพ หมายเลขโทรศัพท์ อีเมล์ ที่อยู่ และสถานที่ทำงาน ส่วนกฎหมายอีกฉบับที่ผู้วิจัยศึกษา คือ HIPAA ซึ่งหลักการของ HIPAA บัญญัติว่าข้อมูลสุขภาพที่ต้องได้รับความคุ้มครอง (Protected Health Information – PHI)[159]ภายใต้กฎความเป็นส่วนตัว คือ ข้อมูลสุขภาพที่ทำให้ระบุตัวบุคคล

---

[157] **Gdpr ฉบับภาษาไทย**, หน้า 37.

[158] ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561, "ราชกิจจานุเบกษา."

[159] Office for Civil Rights (OCR), **Summary of the Hipaa Privacy Rule**, Date cited july 2, 2018 Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

ข้อมูลสุขภาพที่อาจทำให้ระบุตัวบุคคลได้ รวมถึงข้อมูลใด ๆ ที่เกี่ยวกับการจ่ายเงินเพื่อดูแลสุขภาพของบุคคลทั้งสุขภาพกายและสุขภาพจิต ทั้งในอดีต ปัจจุบันและอนาคต ของบุคคลที่ยังมีชีวิตและเสียชีวิต แต่ไม่ครอบคลุมถึงข้อมูลสุขภาพของบุคคลที่เสียชีวิตมาแล้วเกินกว่า 50 ปี ข้อมูลสุขภาพที่กล่าวถึง อาทิเช่น การวินิจฉัยโรค การรักษาที่ได้รับ ผลการทดสอบทางการแพทย์ ยาที่ได้รับ บันทึกทางการแพทย์และรวมถึงข้อมูลพื้นฐานของผู้มารับบริการ คือ หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด เพศ เชื้อชาติและ บุคคลที่ให้ติดต่อกรณีฉุกเฉิน แต่ไม่รวมถึง ชื่อ–สกุล อายุ ที่อยู่ สถานที่ทำงาน หมายเลขโทรศัพท์ หมายเลขเครื่องรับ–ส่งเอกสาร อีเมล์ เลขประจำอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ (Serial Numbers) สัญลักษณ์เชิงหมายเลขที่กำหนดให้แก่เครือข่ายคอมพิวเตอร์ใช้อินเทอร์เน็ตในการสื่อสาร (Internet Protocol Address Numbers) ภาพถ่ายใบหน้าแบบเต็มหน้า ลายนิ้วมือ เสียง ลักษณะของจอประสาทตา (Retinal) หมายเลขบันทึกทางการแพทย์หรือเวชระเบียน และข้อมูลของบุคคลที่เสียชีวิตเกินกว่า 50 ปี

จากการศึกษาพบว่า คำนิยามของข้อมูลส่วนบุคคล และข้อมูลสุขภาพส่วนบุคคล มีความหมายแตกต่างกัน ส่งผลต่อความคุ้มครองข้อมูลแตกต่างกัน ฉะนั้น นิยามของข้อมูลสุขภาพส่วนบุคคลควรแยกออกมาจากคำว่าข้อมูลส่วนบุคคลและมีบทบัญญัติเฉพาะในการคุ้มครองข้อมูลสุขภาพส่วนบุคคล ควรบัญญัติกฎหมายให้ชัดเจนและครอบคลุมในทุกประเด็นที่อาจก่อให้เกิดปัญหาด้านการคุ้มครองข้อมูลสุขภาพส่วนบุคคล ผู้วิจัยจึงขอเสนอว่าควร เพิ่มนิยามข้อมูลสุขภาพส่วนบุคคล ดังนี้

นิยามข้อมูลสุขภาพส่วนบุคคล ควรมีข้อพิจารณาอยู่ 2 ประการ คือ ลักษณะของข้อมูลสุขภาพส่วนบุคคลโดยแท้ และขอบเขตของข้อมูลที่เกี่ยวกับสุขภาพหรือการรับบริการทางด้านสาธารณสุข

1. ลักษณะของข้อมูลสุขภาพส่วนบุคคลโดยแท้ ข้อมูลส่วนบุคคลด้านสุขภาพถูกจำแนกให้เป็นข้อมูลที่มีความละเอียดอ่อนสูงกว่าข้อมูลทั่วไป หากข้อมูลสุขภาพถูกเปิดเผยอาจส่งผลกระทบอย่างรุนแรงต่อเจ้าของข้อมูล เช่นทำให้อับอาย เสื่อมเสียชื่อเสียง ดังนั้นข้อมูลสุขภาพโดยแท้เป็นข้อมูลที่เกี่ยวกับสุขภาพเฉพาะตัวบุคคล เช่น โรคประจำตัว ประวัติการผ่าตัด ประวัติการคลอด ยาที่ใช้เป็นประจำ ประวัติการดื่มเหล้า สูบบุหรี่ การประเมินสุขภาพจิต เหล่านี้ล้วนเป็นข้อมูลสุขภาพ

2. ขอบเขตของข้อมูลที่เกี่ยวกับสุขภาพหรือการรับบริการทางด้านสาธารณสุข คือ ข้อมูลทั้งหมดที่บันทึกในเวชระเบียนของผู้มารับบริการแต่ละคน เช่น บันทึกทางการพยาบาล บันทึกของแพทย์ผู้ทำการรักษา การวางแผนการรักษาพยาบาล ความคิดเห็นในการวินิจฉัยโรค

หรืออาการของผู้มารับบริการรวมถึงข้อมูลที่อ้างอิงถึงผู้ที่บันทึกได้ เช่น ชื่อแพทย์ พยาบาล นักกายภาพบำบัด ข้อมูลดังกล่าวย่อมเป็นข้อมูลสุขภาพส่วนบุคคล

ดังนั้น เพื่อให้นิยามของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สอดคล้องกับนิยามข้อมูลด้านสุขภาพของบุคคล ตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 และเป็นไปตามคำนิยามของกฎหมายสากล จึงควรเพิ่มคำนิยาม “ข้อมูลสุขภาพส่วนบุคคล”ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้คุ้มครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบระเบียนอิเล็กทรอนิกส์ส่วนบุคคลอย่างครอบคลุม

2. มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่มีการจัดเก็บไว้ในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

ข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในโรงพยาบาล คือ เวชระเบียน ซึ่งในอดีตที่ผ่านมาการบันทึกข้อมูลทำได้ง่าย โดยวิธีการจดบันทึกไว้ในกระดาษแล้วรวบรวมเป็นเล่มเฉพาะของผู้รับบริการแต่ละบุคคล แต่ในยุคปัจจุบันได้มีการนำเทคโนโลยีเข้ามาใช้ในการบันทึกข้อมูลสุขภาพส่วนบุคคล ในส่วนของประเทศไทยได้พัฒนาโปรแกรมระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล (Personal Health Records–PHRs) มาใช้เพื่ออำนวยความสะดวกแก่ผู้มารับบริการในโรงพยาบาลและบุคลากรทางการแพทย์ ซึ่งเวชระเบียนแบบเดิมและระเบียนสุขภาพอิเล็กทรอนิกส์ ต่างมีข้อดีและข้อเสีย ดังตาราง 7

ตาราง 7 เปรียบเทียบเวชระเบียนแบบเดิมและระเบียนสุขภาพอิเล็กทรอนิกส์

เวชระเบียนแบบเดิม	ระเบียนสุขภาพอิเล็กทรอนิกส์
ข้อดี	**ข้อดี**
1. ทำง่าย	1. ค้นหาข้อมูลได้ง่าย ลดระยะเวลาในการค้นหาเอกสาร
2. หาอุปกรณ์ง่าย (กระดาษ ปากกา)	2. ส่งต่อข้อมูลได้รวดเร็วทั้งภายใน และภายนอกโรงพยาบาล
3. ไม่ต้องอาศัยเทคโนโลยี คนรุ่นเก่าทำได้	3. เก็บข้อมูลได้นาน ดูข้อมูลย้อนหลังได้
	4. ลดความสิ้นเปลืองการใช้กระดาษ
	6. ใช้บัตรประจำตัวประชาชนเพียงอย่างเดียวในการค้นหาข้อมูล
	7. เชื่อมโยงข้อมูลให้ใช้ร่วมกัน ระหว่างโรงพยาบาลและผู้มารับบริการ

เวชระเบียนแบบเดิม	ระเบียนสุขภาพอิเล็กทรอนิกส์
ข้อเสีย 1. สิ้นเปลืองพื้นที่ในการจัดเก็บเอกสาร 2. ใช้ระยะเวลาในการค้นหาเอกสารนาน 3. เอกสารสูญหายง่าย 4. เอกสารชำรุด เสื่อมสภาพจากการใช้งาน 5. เอกสารที่จัดเก็บมีไม่ครบถ้วน หรือ ข้อมูลสลับคน 6. อ่านลายมือผู้ที่บันทึกไม่ออก 7. ต้องใช้คนเดินเอกสาร ในการส่งต่อข้อมูลในโรงพยาบาล 8. ต้องใช้บัตรประจำตัวของโรงพยาบาลในการค้นหาเอกสาร	**ข้อเสีย** 1. อุปกรณ์หลักที่ใช้มีราคาแพง 2. ใช้เทคโนโลยีหลายขั้นตอน คนรุ่นเก่าใช้ไม่เป็น 3. เปิดดูข้อมูลได้ง่าย ผู้ที่ไม่มีส่วนเกี่ยวข้องสามารถดูข้อมูลได้ 4. ต้องใช้ไฟฟ้า และ อินเตอร์เน็ต 5. ผู้รับบริการลืมบัตรประจำตัวประชาชนไว้โรงพยาบาล

ที่มา:[160] รวบรวมและดัดแปลงข้อมูลจากโครงการพัฒนาการบริการเวชระเบียนในยุคอิเล็กทรอนิกส์ งานเวชระเบียน โรงพยาบาลศิริราช

จากการศึกษาพบว่าถึงแม้ว่าระเบียนสุขภาพอิเล็กทรอนิกส์จะมีข้อดีมากกว่าข้อเสีย แต่ข้อเสียเพียงเล็กน้อย อาจส่งผลกระทบที่รุนแรงต่อเจ้าของข้อมูลสุขภาพส่วนบุคคลได้ ดังนั้น ภาครัฐจึงควรมีมาตรการทางกฎหมายที่คุ้มครองข้อมูลสุขภาพส่วนบุคคลเพื่อป้องปรามผู้ที่จะกระทำการละเมิดข้อมูลที่จัดเก็บไว้ในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ จึงเป็นประเด็นที่ควรให้ความสำคัญ ประกอบด้วยหลักการ 2 ด้าน ดังนี้

2.1 หลักการคุ้มครองข้อมูลสุขภาพส่วนบุคคลตามกฎหมาย

หลักการคุ้มครองข้อมูลสุขภาพส่วนบุคคลตามกฎหมายหมายประกอบด้วย หลักการเก็บ รวบรวมและใช้ข้อมูลสุขภาพส่วนบุคคล หลักการปกปิดข้อมูลสุขภาพส่วนบุคคล หลักการเข้าถึงและแก้ไขข้อมูลสุขภาพส่วนบุคคล

2.1.1 หลักการเก็บ รวบรวมและใช้ข้อมูลสุขภาพส่วนบุคคล

---

[160] **การพัฒนาการบริการเวชระเบียนในยุคอิเล็กทรอนิกส์**, ค้นวันที่ 21 มีนาคม 2563, จาก https://www.si.mahidol.ac.th/office_h/medrecord/stunit/Ino-Download.htm

กระบวนการเก็บ รวบรวมและใช้ข้อมูลสุขภาพส่วนบุคคล เริ่มต้นตั้งแต่การลงทะเบียนประวัติข้อมูลทั่วไป การซักประวัติความเจ็บป่วย การวัดสัญญาณชีพ ซึ่งแต่ละขั้นตอนต้องใช้บุคลากรที่เกี่ยวข้องแต่ละด้านเป็นผู้เก็บบันทึกข้อมูลให้อยู่ในระเบียนสุขภาพส่วนบุคคล ในกรณีที่ผู้มารับบริการในโรงพยาบาล มาด้วยอาการเจ็บป่วย แพทย์ผู้ทำการรักษาหรือบุคคลากรทางการแพทย์ที่เกี่ยวข้องเป็นผู้รับข้อมูลและใช้ข้อมูลในระเบียนสุขภาพ แล้วจึงส่งต่อข้อมูลการรักษา เช่น สั่งยา สั่งเจาะเลือดให้แผนกอื่นที่เกี่ยวข้องได้รับข้อมูลของผู้มารับบริการต่อจนสิ้นสุดกระบวนการรักษาพยาบาล

ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติให้”ผู้ควบคุมข้อมูล” ซึ่งหมายถึงหน่วยงานโรงพยาบาลหรือส่วนราชการที่เกี่ยวข้อง เป็นผู้ทำหน้าที่จัดทำระเบียนสุขภาพ นำข้อมูลสุขภาพส่วนบุคคลจัดเก็บไว้อย่างเป็นระบบตามมาตรฐาน ส่งต่อข้อมูลสุขภาพส่วนบุคคลให้ “ผู้รับข้อมูล” เฉพาะผู้ที่เกี่ยวข้องเท่านั้น ระเบียบฯฉบับนี้มิได้บัญญัติหลักการเก็บ รวบรวมข้อมูลสุขภาพ โดยหลักแล้วข้อมูลสุขภาพเป็นส่วนหนึ่งของข้อมูลส่วนบุคคล หลักการพื้นฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย คือ พระราชคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัตินี้กำหนดให้ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ดำเนินการเก็บ รวบรวมข้อมูล เจ้าหน้าที่ของโรงพยาบาลผู้ซึ่งทำหน้าที่ ลงทะเบียนประวัติข้อมูลทั่วไป ซักถามประวัติความเจ็บป่วย วัดสัญญาณชีพ รายงานผลตรวจทางห้องปฏิบัติการ รวมถึงรายงานผลการวิเคราะห์ด้านต่าง ๆ ที่เกี่ยวข้องกับการมาโรงพยาบาลของผู้รับบริการ ล้วนคือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งทำหน้าที่เก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคล ภายใต้การควบคุมของผู้ควบคุมข้อมูลส่วนบุคคล การเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลจะกระทำมิได้หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลสุขภาพส่วนบุคคล การแสดงความยินยอมต้องทำโดยชัดแจ้งเป็นลายลักษณ์อักษร วิธีการทางอิเล็กทรอนิกส์หรือด้วยวาจา ในการขอความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์และระยะเวลาของการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคล ในกรณีที่ไม่สามารถกำหนดระยะเวลาในการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลที่ชัดเจนให้กำหนดระยะเวลาที่คาดหมายตามมาตรฐานการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคล

ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติให้ “ผู้รับข้อมูล” เป็นบุคคลหรือนิติบุคคล ที่ได้รับข้อมูลสุขภาพส่วนบุคคลจากผู้ควบคุมข้อมูลแล้วนำข้อมูลสุขภาพส่วนบุคคลนั้นไปใช้เพื่อให้เกิดประโยชน์ต่อเจ้าของข้อมูล กรณีที่ข้อมูลสุขภาพจัดเก็บเป็นระเบียนสุขภาพอิเล็กทรอนิกส์

องค์ประกอบในการเข้าถึงข้อมูลและควบคุมการใช้งานข้อมูลสุขภาพส่วนบุคคลในระบบอิเล็กทรอนิกส์ประกอบด้วย คือ การระบุตัวตน การยืนยันตัวตน อนุญาตเฉพาะผู้มีสิทธิเข้าถึงและความรับผิดชอบต่อผลการกระทำ ผู้ควบคุมข้อมูล มีหน้าที่กำหนดมาตรการรักษาความปลอดภัยของข้อมูล เพื่อให้ผู้ที่เป็นเจ้าของข้อมูลสุขภาพส่วนบุคคล มั่นใจว่าข้อมูลของตนถูกนำมาใช้เพื่อประโยชน์ส่วนตนอย่างแท้จริง ฉะนั้นการใช้ข้อมูลสุขภาพส่วนบุคคลต้องเป็นไปตามขอบเขตแห่งความจำเป็นตามวัตถุประสงค์ที่แจ้งไว้โดยเฉพาะและไม่เลือกปฏิบัติ ตามกฎการรักษาความปลอดภัย

พระราชคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายหลักในการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย หลักการเก็บและรวบรวมข้อมูลพระราชคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ทำหน้าที่ดำเนินการเก็บ รวบรวมข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล แต่ไม่ได้ทำหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล ข้อมูลสุขภาพมิได้มีบทบัญญัติคุ้มครองที่ชัดแจ้งในพระราชบัญญัติฉบับนี้ แต่บัญญัติห้ามมิให้เก็บ รวบรวมข้อมูลสุขภาพโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลสุขภาพส่วนบุคคล การขอความยินยอมต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูล แยกส่วนการขอความยินยอมออกจากข้อความอื่น เจ้าของข้อมูลสุขภาพส่วนบุคคลแสดงความยินยอมโดยชัดแจ้งเป็นลายลักษณ์อักษร วิธีการทางอิเล็กทรอนิกส์หรือด้วยวาจา การเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลให้เก็บข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์แจ้งระยะเวลาเก็บและรวบรวมข้อมูลสุขภาพส่วนบุคคลให้ชัดเจน ในกรณีที่ไม่สามารถกำหนดระยะเวลาในการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลที่ชัดเจนให้กำหนดระยะเวลาที่คาดหมายตามมาตรฐานการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคล

ในส่วนของการใช้ข้อมูลสุขภาพส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจตัดสินใจเกี่ยวกับการใช้และเปิดเผยข้อมูล แต่ต้องใช้ข้อมูลสุขภาพส่วนบุคคลภายใต้ความยินยอมจากเจ้าของข้อมูลและเป็นไปตามขอบเขตแห่งความจำเป็นตามวัตถุประสงค์ที่แจ้งไว้ อนึ่งผู้ใช้ข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บไว้ต้องไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

HIPAA เป็นกฎหมายที่มีข้อบังคับเกี่ยวกับการคุ้มครองข้อมูลสุขภาพส่วนบุคคลโดยเฉพาะของประเทศสหรัฐอเมริกา แต่หลักการเก็บและรวบรวมข้อมูลนั้น HIPAA มิได้มีบทบัญญัติเฉพาะเรื่องการเก็บและรวบรวมข้อมูลสุขภาพไว้ โดยหลักแล้วข้อมูลสุขภาพเป็นส่วนหนึ่งของข้อมูลส่วนบุคคล ผู้วิจัยจึงนำหลักการพื้นฐานของกฎหมายที่ว่าด้วยการ

คุ้มครองข้อมูลส่วนบุคคลในระดับสากล[161]มาอ้างอิง หลักการเก็บและรวบรวมข้อมูลสุขภาพส่วนบุคคลของ HIPAA ได้มาจากการซักประวัติ ตรวจร่างกาย การตรวจรักษา การตรวจสุขภาพและการวางแผนเกี่ยวกับสุขภาพ ไม่ว่าข้อมูลนั้นจะอยู่ในรูปเอกสาร ข้อมูลอิเล็กทรอนิกส์ หรือบันทึกด้วยวาจา แล้วจัดเก็บเป็นชุดข้อมูลเพื่อใช้ในการดูแลสุขภาพของแต่ละบุคคล ซึ่งการได้มาซึ่งข้อมูลสุขภาพเหล่านั้นเจ้าของข้อมูลต้องรับรู้ หรือให้ความยินยอม หลักการเก็บ รวบรวมข้อมูลของ HIPAA กำหนดให้การเก็บรวบรวมข้อมูลสุขภาพส่วนบุคคลเป็นไปอย่างจำกัด กล่าวคือ การเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลต้องเป็นไปภายใต้ขอบเขตแห่งความจำเป็นตามวัตถุประสงค์ที่แจ้งไว้โดยเฉพาะและไม่เลือกปฏิบัติ[162] เก็บและรวบรวมข้อมูลสุขภาพส่วนบุคคลอย่างจำกัด เป็นธรรมโดยชอบด้วยกฎหมาย

ในส่วนของการใช้ข้อมูลสุขภาพส่วนบุคคล HIPAA กำหนดหลักการว่าห้ามมิให้บุคคล นิติบุคคล หรือองค์กรซึ่งดำเนินงานเกี่ยวเนื่องกับการประกันสุขภาพ องค์กรกลางที่ควบคุมระบบข้อมูลบริการสาธารณสุข ผู้ให้บริการด้านสาธารณสุข หรือธุรกิจที่เกี่ยวข้อง ใช้ข้อมูลสุขภาพส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมาย HIPAA โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล หากได้รับความยินยอมและอนุญาตจากเจ้าของข้อมูลให้นำข้อมูลสุขภาพส่วนบุคคลไปใช้ การใช้ข้อมูลสุขภาพส่วนบุคคลต้องเป็นไปตามขอบเขตแห่งความจำเป็นตามวัตถุประสงค์ที่แจ้งไว้โดยเฉพาะและไม่เลือกปฏิบัติ ตามกฎการรักษาความปลอดภัยของข้อมูล

GDPR เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ให้ความคุ้มครองข้อมูลส่วนบุคคลประชาชนสหภาพยุโรปไม่ว่าอาศัยอยู่ที่ใด หลักการเก็บรวบรวมข้อมูลสุขภาพส่วนบุคคลของ GDPR มีบัญญัติว่า การประมวลผลข้อมูลส่วนบุคคลหมายถึงการเก็บ รวบรวมข้อมูลส่วนบุคคลหรือปฏิบัติการใด ๆ ที่ดำเนินการต่อชุดข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล ทำหน้าที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูล ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึงบุคคลหรือนิติบุคคล ที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล ฉะนั้น ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจเป็นบุคคลเดียวกันได้ GDPR กำหนดให้ข้อมูลสุขภาพส่วนบุคคลเป็นข้อมูลที่มีความละเอียดอ่อน หลักในการเก็บ รวบรวมข้อมูลเคร่งครัดกว่าข้อมูลส่วนบุคคลทั่วไป การเก็บรวบรวมข้อมูลสุขภาพส่วนบุคคล อยู่ภายใต้ความชอบด้วยกฎหมาย เพื่อวัตถุประสงค์ที่เฉพาะ

---

[161] จันทจิรา เอี่ยมมยุรา, "แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย," วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 653-657.

[162] (OCR), O. f. C. R., "Summary of the Hipaa Privacy Rule."

ด้วยวิธีการที่เข้ากับวัตถุประสงค์ ใช้ข้อมูลเท่าที่จำเป็นและปรับปรุงข้อมูลให้เป็นปัจจุบันเสมอ แต่ GDPR ไม่ได้วางหลักเกณฑ์กำหนดระยะเวลาการจัดเก็บข้อมูลสุขภาพไว้มีเพียงบทบัญญัติว่า ข้อมูลส่วนบุคคลอาจถูกเก็บไว้เป็นระยะเวลานานขึ้น เพื่อประโยชน์สาธารณะ เพื่อประโยชน์ทางการวิจัยหรือเพื่อทำจดหมายเหตุทางประวัติศาสตร์

ในส่วนของการใช้ข้อมูลสุขภาพส่วนบุคคล GDPR ใช้วิธีการทำโปรไฟล์ (Profiling) หมายถึง การประมวลผลข้อมูลส่วนบุคคลที่สัมพันธ์กับข้อมูลสุขภาพส่วนบุคคลด้วยวิธีประมวลผลในรูปแบบใด ๆ ก็ตามมาวิเคราะห์เกี่ยวกับสุขภาพของบุคคลนั้น GDPR กำหนดหลักว่า การใช้ข้อมูลสุขภาพส่วนบุคคลจะชอบด้วยกฎหมายเมื่อ เจ้าของข้อมูลสุขภาพส่วนบุคคลยินยอมให้ประมวลผลข้อมูล การใช้ข้อมูลสุขภาพส่วนบุคคลที่ประมวลผลสำเร็จแล้วนั้นเป็นการใช้ข้อมูลเพื่อคุ้มครองผลประโยชน์ของเจ้าของข้อมูล เพื่อบุคคลอื่นหรือเพื่อประโยชน์สาธารณะ

จากการศึกษาหลักการเก็บ รวบรวมและใช้ข้อมูลสุขภาพส่วนบุคคล พบว่ามีปัญหาความไม่ชัดเจนของบทบัญญัติในการเก็บ รวบรวมและใช้ข้อมูลสุขภาพส่วนบุคคลในกฎหมายแต่ละฉบับ สรุปเป็นปัญหาที่พบดังนี้

1) ความไม่ชัดเจนระหว่างบทบาทของ ผู้ควบคุมข้อมูลส่วนบุคคล กับ ผู้ประมวลผลข้อมูลส่วนบุคคล หลักของพระราชคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่รักษาความปลอดภัยของข้อมูลที่มีการจัดเก็บไว้แต่ให้ ผู้ประมวลผลข้อมูลส่วนบุคคล เป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลแต่ไม่ได้เป็นผู้ควบคุมข้อมูลเอง โดยมีข้อกำหนดที่ชัดเจนว่า ผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลห้ามเป็นบุคคลเดียวกัน ขัดแย้งกับ GDPR ที่บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคล ทำหน้าที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูล ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึงบุคคลหรือนิติบุคคล ผู้ซึ่งทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล ฉะนั้น ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจเป็นบุคคลเดียวกันหรือคนละบุคคลได้

ผู้วิจัยจึงขอเสนอว่า กฎหมายควรบัญญัติบทบาทหน้าที่การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลอย่างชัดเจนไม่ทับซ้อน เพื่อกำหนดผู้รับผิดชอบตามกฎหมาย กรณีข้อมูลสุขภาพเปิดเผยสู่สาธารณะโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล

2) ระยะเวลาที่ใช้เก็บรักษาข้อมูลสุขภาพส่วนบุคคล ระเบียบกระทรวง

สาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บัญญัติให้แจ้งระยะเวลาเก็บและรวบรวมข้อมูลสุขภาพส่วนบุคคล แต่ในกรณีที่ไม่สามารถกำหนดระยะเวลาในการเก็บ รวบรวมข้อมูลสุขภาพส่วนบุคคลที่ชัดเจนให้กำหนดระยะเวลาที่คาดหมาย ในขณะที่ GDPR ไม่ได้วางหลักเกณฑ์กำหนดระยะเวลาการจัดเก็บข้อมูลสุขภาพ แต่ HIPAA กำหนดระยะเวลาการจัดเก็บเวชระเบียนทางการแพทย์ไว้นาน 6 ปี นับแต่การจัดเก็บข้อมูลครั้งสุดท้าย กฎหมายเกี่ยวกับการเก็บรักษาเวชระเบียนของประเทศไทยเดิมกำหนดระยะเวลาในการเก็บรักษา 5 ปี

ผู้วิจัยจึงขอเสนอว่า กฎหมายควรบัญญัติระยะเวลาเก็บและรวบรวมข้อมูลสุขภาพส่วนบุคคลไว้ในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล 10 ปีนับจากการบันทึกข้อมูลสุขภาพข้อมูลส่วนบุคคลครั้งสุดท้าย เนื่องจากเมื่อเกิดการละเมิดข้อมูลสุขภาพสิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดนั้นมีอายุความ 10 ปี ตามประมวลกฎหมายแพ่งและพาณิชย์

2.1.2 หลักการปกปิดข้อมูลสุขภาพส่วนบุคคล

การรักษาความลับของผู้ป่วย เป็นหลักจริยธรรมของผู้ประกอบวิชาชีพทางการแพทย์ที่ต้องยึดถืออย่างเคร่งครัด ข้อมูลสุขภาพส่วนบุคคลคือความลับด้านสุขภาพส่วนบุคคลย่อมได้รับเอกสิทธิ์การปกปิดข้อมูลจากบุคลลากรทางการแพทย์ที่เกี่ยวข้อง

ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติให้ข้อมูลสุขภาพส่วนบุคคลเป็นความลับส่วนบุคคลเปิดเผยมิได้ ผู้ควบคุมข้อมูลต้องเก็บรวบรวมข้อมูลด้วยวิธีที่เหมาะสม มีมาตรการรักษาความปลอดภัยของข้อมูลอย่างรัดกุม การเปิดเผยข้อมูลสุขภาพส่วนบุคคลกระทำได้เมื่อเจ้าของข้อมูลให้ความยินยอมและการเปิดเผยข้อมูลสุขภาพส่วนบุคคลนั้นต้องไม่ก่อความเสียหายต่อเจ้าของข้อมูล กรณีที่ข้อมูลสุขภาพส่วนบุคคลถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม ผู้ควบคุมข้อมูลคือผู้รับผิดชอบหลักตามระเบียบฯนี้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นองค์กรหรือหน่วยงานที่มีการประมวลผลข้อมูลที่มีความอ่อนไหว ดังเช่น ข้อมูลสุขภาพส่วนบุคคล ต้องแต่งตั้งให้มี “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” เพื่อดูแลความปลอดภัยของข้อมูลโดยเฉพาะ โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่รักษาความลับของข้อมูลสุขภาพส่วนบุคคลที่ได้ล่วงรู้จากการปฏิบัติหน้าที่ ไม่มีสิทธิใช้หรือเปิดเผยข้อมูลและต้องตรวจสอบการทำงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลให้เปิดเผยข้อมูลสุขภาพส่วนบุคคลที่ได้รับมา ต้องเป็นไปตาม

พระราชบัญญัตินี้ กรณีที่ข้อมูลสุขภาพส่วนบุคคลถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือผู้รับผิดชอบหลักตามพระราชบัญญัตินี้

HIPAA กำหนดหลักการปกปิดข้อมูลสุขภาพส่วนบุคคลว่า ห้ามมิให้ บุคคล หน่วยงาน หรือองค์กรซึ่งดำเนินงานเกี่ยวกับการประกันสุขภาพ ผู้ให้บริการด้านสุขภาพและสาธารณสุข หรือธุรกิจที่เกี่ยวข้อง เปิดเผยข้อมูลสุขภาพส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมายนี้ซึ่งตนได้ครอบครองข้อมูลหรือได้รับข้อมูลนั้นมา การเปิดเผยข้อมูลสุขภาพส่วนบุคคลจะกระทำได้เมื่อเจ้าของข้อมูลให้ความยินยอม

GDPR กำหนดหลักการปกปิดข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลที่จัดเก็บในระบบอิเล็กทรอนิกส์ โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลนำมาตรการทางเทคนิค กระบวนการทดสอบและประเมินประสิทธิภาพของมาตรการทางเทคนิคเพื่อรับประกันความปลอดภัยของข้อมูลให้เป็นความลับ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” เป็นบุคคลที่ถูกแต่งตั้งโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เป็นผู้ซึ่งมีความรู้ ความชำนาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและด้านกฎหมาย กรณีที่ข้อมูลสุขภาพส่วนบุคคลถูกเผยแพร่สู่สาธารณะโดยที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือผู้รับผิดชอบหลักตาม GDPR

จากการศึกษา พบว่าข้อมูลสุขภาพส่วนบุคคลเป็นข้อมูลอ่อนไหว การเปิดเผยข้อมูลสุขภาพส่วนบุคคลออกสู่สาธารณะอาจส่งผลกระทบต่อเจ้าของข้อมูลทั้งด้านสังคมและจิตใจ เช่นทำให้เสียชื่อเสียงและทำให้อับอาย กฎหมายของทุกประเทศจึงให้ความสำคัญกับการคุ้มครองข้อมูลสุขภาพส่วนบุคคล แม้จะมีบทลงโทษที่แตกต่างกันแต่ล้วนมีวัตถุประสงค์เดียวกันคือ การกำหนดบทลงโทษเพื่อป้องปรามการกระทำความผิดทุกหน่วยงานที่จัดเก็บข้อมูลส่วนบุคคลจึงแต่งตั้ง หน่วยงานหรือบุคคลทำหน้าที่กำกับดูแลการรักษาความปลอดภัยของข้อมูล กรณีที่ข้อมูลสุขภาพส่วนบุคคลเผยแพร่ออกสู่สาธารณะโดยที่เจ้าของข้อมูลไม่ให้ความยินยอมบทลงโทษควรแบ่งออกเป็น 3 กรณี ดังนี้

1) ผู้ควบคุมข้อมูลสุขภาพส่วนบุคคล เป็นหน่วยงานหลักที่ดูแลข้อมูลสุขภาพส่วนบุคคลของผู้เสียหาย ต้องรับผิดกรณีไม่รู้ว่าความเสียหายเกิดขึ้นเพราะเหตุใด

2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องรับผิด กรณีอนุญาตให้ผู้ควบคุมข้อมูลสุขภาพส่วนบุคคลหรือผู้ประมวลผลข้อมูลสุขภาพส่วนบุคคลนำข้อมูลไปใช้โดยผิดจากวัตถุประสงค์ที่แจ้งไว้ต่อเจ้าของข้อมูลสุขภาพส่วนบุคคล

3) ผู้รับข้อมูล ต้องรับผิด กรณีนำข้อมูลสุขภาพส่วนบุคคลของเจ้าของข้อมูลไปใช้โดยประมาทจนทำให้เจ้าของข้อมูลสุขภาพส่วนบุคคลได้รับความเสียหาย

2.1.3 หลักการเข้าถึงและแก้ไขข้อมูลสุขภาพส่วนบุคคล

หลักการเข้าถึงข้อมูลสุขภาพส่วนบุคคล ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 กำหนดให้การขอสำเนาข้อมูลสุขภาพอาจกระทำโดยบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลแต่ต้องขอความยินยอมจากเจ้าของข้อมูลก่อน ผู้ขอต้องปฏิบัติตามวัตถุประสงค์ที่แจ้งแก่ผู้ควบคุมข้อมูล หากมีความเสียหายเกิดขึ้นกับเจ้าของข้อมูลสุขภาพส่วนบุคคล ผู้ขอทำสำเนาต้องเป็นผู้รับผิดชอบ

ในส่วนของหลักการแก้ไขข้อมูลสุขภาพส่วนบุคคล ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 กำหนดให้เจ้าของข้อมูลมีสิทธิแก้ไขข้อมูลสุขภาพส่วนบุคคลของตน โดยร้องขอต่อผู้ควบคุมข้อมูลและต้องรอคำสั่งอนุมัติให้ทำการแก้ไขข้อมูล เมื่อมีการแก้ไขต้องมีการลงชื่อผู้แก้ไขและพยานในการบันทึกทุกครั้ง

หลักการเข้าถึงข้อมูลสุขภาพส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลของตน ขอรับสำเนาข้อมูลของตนจากผู้ควบคุมข้อมูลส่วนบุคคลและขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งต่อหรือโอนข้อมูลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น รวมถึงขอให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยที่มาของข้อมูลที่ตนไม่ให้ความยินยอมจัดเก็บ

ในส่วนของหลักการแก้ไขข้อมูลสุขภาพส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ลบ ทำลายหรือทำให้ข้อมูลที่จัดเก็บไว้ไม่สามารถระบุตัวบุคคล รวมถึงระงับการใช้ข้อมูลที่จัดเก็บไว้

หลักการเข้าถึงข้อมูลสุขภาพส่วนบุคคล HIPAA กำหนดให้บุคคลเจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลสุขภาพส่วนบุคคลของตนที่ถูกจัดเก็บไว้เพื่อตรวจสอบความถูกต้องของข้อมูล และมีสิทธิร้องขอสำเนาบันทึกเกี่ยวกับข้อมูลสุขภาพส่วนบุคคลของตนจากหน่วยงานที่เก็บรวบรวมข้อมูลไว้ตลอดระยะเวลาที่ข้อมูลถูกเก็บบันทึกไว้ หน่วยงานที่เก็บรวบรวมข้อมูลไว้ต้องดำเนินการตามที่เจ้าของข้อมูลสุขภาพส่วนบุคคลร้องขอภายในระยะเวลาไม่เกิน 30 วัน นับจากวันที่ได้รับคำร้อง

ในส่วนของหลักการแก้ไขข้อมูลสุขภาพส่วนบุคคล HIPAA กำหนดให้บุคคลเจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานที่เก็บรวบรวมข้อมูลสุขภาพส่วนบุคคลของตน

แก้ไขข้อมูลสุขภาพส่วนบุคคลของตนที่ไม่ถูกต้องรวมถึงให้ลบข้อมูลที่ไม่ต้องการให้จัดเก็บไว้ในระเบียนสุขภาพได้ตลอดระยะเวลาที่ข้อมูลถูกเก็บบันทึกไว้ หน่วยงานที่เก็บรวบรวมข้อมูลต้องดำเนินการแก้ไขข้อมูลตามที่เจ้าของข้อมูลสุขภาพส่วนบุคคลร้องขอภายในระยะเวลาไม่เกิน 60 วัน นับจากวันที่ได้รับคำร้อง

หลักการเข้าถึงข้อมูลสุขภาพส่วนบุคคล GDPR กำหนดให้ผู้ถูกประมวลผลข้อมูลส่วนบุคคลมีสิทธิรับรู้ว่าการประมวลผลข้อมูลสุขภาพของตนนั้นชอบด้วยกฎหมายหรือไม่ มีสิทธิรับรู้ระยะเวลาที่ข้อมูลสุขภาพส่วนบุคคลของตนถูกใช้เพื่อประมวลผลจากผู้ควบคุมข้อมูลส่วนบุคคล สิทธิที่จะรับรู้ข้อมูลสุขภาพส่วนบุคคลของตนโดยผู้ควบคุมต้องจัดให้มีการเข้าถึงข้อมูลจากระยะไกลด้วยระบบที่ปลอดภัยอันจะทำให้ผู้ถูกประมวลผลข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตนได้โดยตรง

ในส่วนของหลักการแก้ไขข้อมูลสุขภาพส่วนบุคคล GDPR กำหนดให้ผู้ถูกประมวลผลมีสิทธิแก้ไขข้อมูลสุขภาพส่วนบุคคลของตนให้ถูกต้อง ผู้ถูกประมวลผลมีสิทธิลบข้อมูลของตนที่จัดเก็บไว้ในระบบ รวมถึงสิทธิในการร้องขอให้ผู้ควบคุมข้อมูลส่งต่อข้อมูลสุขภาพส่วนบุคคลของตนไปยังผู้ควบคุมอื่นโดยตรง และผู้ถูกประมวลผลมีสิทธิคัดค้านการประมวลผลของข้อมูลส่วนบุคคลใด ๆ ที่สัมพันธ์กับข้อมูลสุขภาพส่วนบุคคลของตน

อนึ่ง ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล บทบาทของผู้รับบริการในโรงพยาบาลหรือเจ้าของข้อมูลสุขภาพส่วนบุคคล คือ การบันทึกข้อมูลของตนเอง ดูข้อมูลของตนเองที่บันทึกไว้ในระบบ แต่การสำเนาข้อมูลของตนเองจากโรงพยาบาลที่มารับบริการแล้วส่งต่อข้อมูลหรือนำข้อมูลไปใช้ต้องขออนุญาตจากผู้ควบคุมข้อมูล เนื่องจากข้อมูลส่วนบุคคลด้านสุขภาพเป็นข้อมูลส่วนบุคคลที่ถูกจำแนกอยู่ในประเภทของข้อมูลที่มีความละเอียดอ่อนหรือข้อมูลที่มีความอ่อนไหวมากกว่าข้อมูลส่วนบุคคลประเภททั่วไป ดังนั้นการนำข้อมูลส่วนบุคคลมาใช้ จัดเก็บหรือเปิดเผยต้องทำด้วยความระมัดระวัง ไม่ว่าข้อมูลส่วนบุคคลด้านสุขภาพนั้นจะนำมาใช้เพื่อการพัฒนาระบบสาธารณสุข เพื่อการรักษาพยาบาล หรือเพื่อประโยชน์สาธารณะก็ตาม ซึ่งองค์ประกอบในการพิจารณาว่าข้อมูลเป็นความลับหรือไม่[163]นั้นประกอบด้วย 1) การเปิดเผยข้อมูลทำให้เจ้าของข้อมูลได้รับความเสียหาย และบุคคลอื่นได้รับประโยชน์จากการเปิดเผยข้อมูลนั้น 2) เจ้าของข้อมูลเชื่อว่าข้อมูลดังกล่าวเป็นความลับและไม่ใช่ข้อมูลที่เป็นประโยชน์ต่อสาธารณะ 3)การเชื่อตามข้อ (1) และ (2) เป็นไปอย่างสมเหตุสมผล 4) ข้อมูลดังกล่าวถูกนำมาใช้เพื่อประโยชน์ในเชิงพาณิชย์ ดังนั้นการใช้หรือเปิดเผยข้อมูลสุขภาพควรคำนึงสิทธิที่จะได้รับการรักษาความลับด้านสุขภาพของบุคคลซึ่งเป็น

---

[163] David I. Bainbridge, "Computor and the Law," ed. 3 rd (London: Pitman Publishing, 1996). p 37.

เจ้าของข้อมูลนั้นด้วย ซึ่งสิทธิที่จะได้รับการรักษาความลับข้อมูลส่วนบุคคลด้านสุขภาพนี้มีบทบัญญัติเฉพาะในกฎหมาย HIPAA โดยยึดหลักปกปิดให้มากที่สุด เปิดเผยเฉพาะที่จำเป็น เจ้าของข้อมูลและผู้ที่เกี่ยวข้องสามารถเข้าถึงและแก้ไขข้อมูลได้ ผู้ที่ไม่เกี่ยวข้องไม่มีสิทธิ์เข้าถึงข้อมูล แต่ไม่มีการกล่าวถึงสิทธินี้ในกฎหมายอื่นที่ผู้วิจัยศึกษา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติในเรื่องของสิทธิของเจ้าของข้อมูลส่วนบุคคลสอดคล้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคลตาม GDPR และหลักของสิทธิมนุษยชน โดยกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังนี้

1) สิทธิในเข้าถึงข้อมูลของตนเองและขอให้เปิดเผยถึงการได้มาซึ่งข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอดูการประมวลผลข้อมูลของตนเองว่าจัดเก็บตามวัตถุประสงค์ที่ได้รับแจ้งจากผู้ควบคุมข้อมูล ดังนั้นในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล เจ้าของข้อมูลมีสิทธิในการเข้าไปดูข้อมูลและการประมวลผลข้อมูลสุขภาพของตนแต่ไม่มีสิทธิในการแก้ไขการประมวลผลข้อมูล

2) สิทธิในการขอเคลื่อนย้ายข้อมูลของตนเอง ขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน หรือขอให้ผู้ควบคุมข้อมูลโอนย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลอื่น โดยผู้ควบคุมข้อมูลต้องทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้ทั่วไป เช่นการส่งข้อมูลผ่านทางโปรแกรมคอมพิวเตอร์ ส่งทางอีเมล์ การส่งต่อในรูปแบบเอกสาร และการโอนข้อมูลอัตโนมัติซึ่งการโอนข้อมูลโดยวิธีอัตโนมัตินั้นต้องมีระดับความคุ้มครองข้อมูลที่เท่าเทียมกัน ดังนั้นในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลเจ้าของข้อมูลสุขภาพจึงมีสิทธิที่จะขอเคลื่อนย้ายข้อมูลสุขภาพของตนเองจากผู้ควบคุมข้อมูลส่วนบุคคลผ่านทางระบบอิเล็กทรอนิกส์

3) สิทธิในการโต้แย้ง หรือ คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ในกรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมโดยได้รับการยกเว้นไม่ต้องขอความยินยอมเพื่อประโยชน์ของสาธารณะหรือเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการประมวลผลข้อมูลดังกล่าว

4) สิทธิในการขอให้ลบทำลาย หรือเปลี่ยนแปลงข้อมูลให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เมื่อเจ้าของข้อมูลเห็นว่าหมดความจำเป็นในการเก็บรักษาข้อมูล หรือบรรลุวัตถุประสงค์ในการใช้ข้อมูลแล้ว

สิทธิต่าง ๆ ที่ได้กล่าวมาทั้งหมด ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้พิทักษ์ ผู้อนุบาล ผู้แทนโดยชอบธรรมหรือผู้ที่ได้รับมอบอำนาจจากเจ้าของข้อมูลส่วนบุคคลมีสิทธิดังกล่าวด้วยเช่นกัน แต่ต้องร้องขอผ่านผู้ควบคุมข้อมูลส่วน

บุคคลซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

สิทธิของเจ้าของข้อมูลที่บัญญัติไว้ใน GDPR แต่ไม่ได้บัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือ

1) สิทธิในการจำกัดการประมวลผล GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องขอให้องค์กรจำกัดการประมวลผลข้อมูล โดยผู้เก็บข้อมูลสามารถเก็บข้อมูลส่วนบุคคลต่อไปได้ แต่ไม่สามารถนำไปประมวลผลข้อมูลได้อีกต่อไป เว้นแต่เจ้าของข้อมูลจะให้ความยินยอมหรือได้รับการยกเว้นตามที่กฎหมายกำหนด

2) สิทธิในการคัดค้านการตัดสินใจแทนโดยอัตโนมัติ เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการตัดสินใจโดยอิงจากการประมวลผลโดยอัตโนมัติ ซึ่งการตัดสินใจแทนโดยอัตโนมัตินั้นมีผลทางกฎหมายหรือส่งผลกระทบอย่างยิ่งยวดต่อเจ้าของข้อมูล ยกเว้นในบางกรณี เช่น การตัดสินใจนั้นจำเป็นต่อการปฏิบัติตามข้อสัญญา การตัดสินใจนั้นได้รับอนุญาตจากกฎหมายของสหภาพยุโรปหรือรัฐสมาชิก หรือได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล

จากการศึกษาหลักการเข้าถึงและแก้ข้อมูลสุขภาพส่วนบุคคล พบว่าหลักการนี้ให้สิทธิกับเจ้าของข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของข้อมูล แก้ไขข้อมูลผิด ลบข้อมูลที่ไม่ต้องการหรือไม่อนุญาตให้ผู้อื่นนำข้อมูลไปใช้ แต่สิทธิดังกล่าวเหล่านี้ต้องร้องขอหรือได้รับการอนุญาตจากหน่วยงานที่จัดเก็บข้อมูลสุขภาพส่วนบุคคลไว้

2.2 หลักการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล

การคุ้มครองข้อมูลสุขภาพส่วนบุคคลเป็นหลักกฎหมายที่เป็นสากล อย่างไรก็ตามการคุ้มครองข้อมูลสุขภาพส่วนบุคคลมิใช่ข้อกำหนดเด็ดขาด กฎหมายแต่ละฉบับหลักการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลไว้ในกรณี ดังต่อไปนี้

เหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล ตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 บัญญัติว่า ผู้ควบคุมข้อมูลไม่ต้องขอความยินยอมจากเจ้าของข้อมูลสุขภาพส่วนบุคคลล่วงหน้าในกรณี เพื่อประโยชน์ทางการศึกษาวิจัยด้านสุขภาพ

เหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติฉบับนี้กำหนดข้อยกเว้นที่ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลคือเพื่อประโยชน์ของสาธารณะ โดยเฉพาะกิจการของภาครัฐ

ซึ่งเกี่ยวข้องกับข้อมูลสุขภาพส่วนบุคคลของประชาชนที่ได้รับการยกเว้นไว้แล้ว กิจกรรมนั้นสามารถทำได้ได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[164] ถ้าข้อมูลนั้นจัดเก็บหรือใช้เพื่อป้องกันหรือระงับเหตุที่ก่อให้เกิดอันตรายต่อชีวิตและร่างกายหรือก่อให้เกิดอันตรายต่อสุขภาพของบุคคล ดังนั้นเพื่อช่วยชีวิตบุคคลซึ่งเป็นเจ้าของข้อมูลสุขภาพ จึงจำเป็นต้องเข้าถึงข้อมูลที่เกี่ยวกับสุขภาพ เช่น หมู่เลือด ประวัติโรคประจำตัว ประวัติการแพ้ยา โดยไม่ต้องขอความยินยอมในการเข้าถึงข้อมูลเพื่อนำข้อมูลมาใช้ในการรักษาพยาบาล และยังเปิดช่องให้เจ้าหน้าที่หรือบุคคลากรที่เกี่ยวข้องนำข้อมูลสุขภาพของบุคคลหนึ่งไปใช้เพื่อประโยชน์ในการดูแลสุขภาพของบุคคลอื่นได้

เหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล HIPAA มิได้กำหนดเหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลไว้โดยชัดแจ้งแต่อย่างใด อย่างไรก็ตามจากแนวปฏิบัติเกี่ยวกับข้อมูลที่เป็นธรรมและแนวปฏิบัติเกี่ยวกับความเป็นส่วนตัวและความปลอดภัยระดับชาติสำหรับการแลกเปลี่ยนข้อมูลส่วนบุคคลด้านสุขภาพทางอิเล็กทรอนิกส์สามารถสรุปเหตุแห่งการยกเว้นหลักการเก็บรวบรวมข้อมูลส่วนบุคคลด้านสุขภาพที่สำคัญ คือความยินยอมของบุคคลซึ่งเป็นเจ้าของข้อมูล และกรณีเก็บรวบรวมข้อมูลเพื่อบรรลุวัตถุประสงค์ที่กำหนดขึ้นโดยเฉพาะหรือการใช้อำนาจตามกฎหมายของหน่วยงานที่เกี่ยวข้อง เช่น การใช้ข้อมูลสุขภาพส่วนบุคคลเพื่อประโยชน์ต่อเจ้าของข้อมูลสุขภาพ กรณีเป็นไปเพื่อการบำบัดรักษา การชำระค่าใช้จ่าย หรือ การดำเนินการเกี่ยวกับการดูแลสุขภาพ การใช้ข้อมูลสุขภาพส่วนบุคคลเพื่อประกอบการตัดสินใจในการเข้ารับบริการด้านสุขภาพ การใช้ข้อมูลสุขภาพส่วนบุคคลเพื่อส่วนได้เสียของสาธารณะ และประโยชน์สาธารณะ เป็นต้น

เหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล GDPR บัญญัติว่าการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษด้วยเหตุผลความจำเป็นเพื่อประโยชน์ของสาธารณะในด้านสาธารณสุขทำได้โดยไม่ต้องขอความยินยอมจากผู้ถูกประมวลผลข้อมูล การประมวลผลดังกล่าวควรอยู่ภายใต้มาตรการทางกฎหมายที่เหมาะสมและเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลสุขภาพ[165] การประมวลผลข้อมูลดังกล่าวต้องเกี่ยวข้องกับสุขภาวะอันเป็นไปเพื่อประโยชน์สาธารณะ เช่นการป้องกันโรคระบาด การช่วยชีวิตเจ้าของข้อมูลกรณีฉุกเฉิน แต่มิใช่เพื่อบุคคลที่สาม เช่น นายจ้าง บริษัทประกันชีวิตหรือประกันภัยและธนาคาร

---

[164] มาตรา 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[165] Regulation (EC) No. 1338/2008 of the European Union and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work

ฉะนั้นการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล ให้หน่วยงานที่ต้องการใช้ข้อมูลสุขภาพส่วนบุคคลมีสิทธิเข้าถึงข้อมูลโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลสุขภาพส่วนบุคคลจึงเป็นการกระทำที่กฎหมายรองรับว่ามิใช่การกระทำผิดกฎหมาย ข้อกำหนดยกเว้นการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในกรณียึด "ประโยชน์สาธารณะเป็นสำคัญ" หน่วยงานของรัฐนำข้อมูลมาใช้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่นในกรณีการเกิดโรคระบาด ก็เท่ากับเป็นการเปิดช่องว่างให้หน่วยงานของรัฐนำข้อมูลส่วนบุคคลด้านสุขภาพมาใช้ได้ เหตุแห่งการยกเว้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคลจึงเข้าข่ายว่าแม้ข้อมูลที่มีความอ่อนไหวก็มิใช่ความลับ มิอาจพ้นจากการสอดส่องและควบคุมของภาครัฐ

บทที่ 5

สรุปและข้อเสนอแนะ

บทสรุป

ในยุคปัจจุบันเทคโนโลยีสารสนเทศถูกพัฒนาให้ก้าวหน้ามากขึ้น การเข้าถึงและการส่งต่อข้อมูลต่าง ๆ สามารถกระทำได้โดยง่ายและรวดเร็ว ทำให้เกิดการล่วงละเมิดข้อมูลส่วนบุคคลเพื่อแสวงหาประโยชน์โดยมิชอบเป็นเหตุให้เจ้าข้อมูลส่วนบุคคลได้รับความเสียหาย การคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) ซึ่งเป็นบ่อเกิดและรากฐานของสิทธิมนุษยชนโดยใช้แนวคิดตามกฎหมายธรรมชาติ เนื่องจากแนวคิดนี้เห็นว่าสิทธิเหล่านั้นมีอยู่แล้วตามธรรมชาติไม่ใช่เป็นสิ่งที่มนุษย์คิดสร้างขึ้น เพียงแต่มนุษย์เป็นผู้ค้นพบเท่านั้น ธรรมชาติได้สอนให้มนุษย์ไม่ทำร้ายซึ่งกันและกันเพราะเป็นวิธีเดียวที่จะรักษาชีวิตของตนเองไว้ได้ในสังคมตามธรรมชาติ มนุษย์ทุกคนจึงมีสิทธิที่จะลงโทษผู้ฝ่าฝืนธรรมชาติเพื่อประโยชน์แก่ทุกคนในชุมชน จนกระทั่งการเจริญเติบโตของวิทยาศาสตร์และเทคโนโลยี ได้ท้าทายอุดมการณ์สิทธิมนุษยชนปรัชญาสิทธิธรรมชาติ หลังสงครามโลกครั้งที่สองจึงมีการจัดตั้งสหประชาชาติและมีการยกร่างปฏิญญาสากลว่าด้วยสิทธิมนุษยชนขึ้น

แนวคิดความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล มีวิวัฒนาการมาอย่างยาวนานเนื่องจากเป็นสิทธิขั้นพื้นฐานของมนุษย์ทุกคน ข้อมูลส่วนบุคคลด้านสุขภาพเป็นข้อมูลที่ถูกจำแนกให้เป็นข้อมูลอ่อนไหวหรือข้อมูลที่มีความละเอียดอ่อน ซึ่งข้อมูลดังกล่าวนี้หากถูกเปิดเผยจะส่งผลลบต่อเจ้าของข้อมูลทำให้เกิดความอับอายหรือก่อให้เกิดความเสียหายอย่างร้ายแรงต่อเจ้าของข้อมูล ตัวอย่างของข้อมูลส่วนบุคคลด้านสุขภาพที่มีการเก็บบันทึกไว้ในสถานพยาบาล คือเวชระเบียนหรือบันทึกทางการรักษาพยาบาล ซึ่งในอดีตมีการเก็บบันทึกไว้เป็นรูปแบบกระดาษเอกสาร เวชระเบียนจะบันทึกข้อมูลทั้งหมดของผู้มารับบริการในโรงพยาบาล เช่น ข้อมูลส่วนตัว ประวัติการรักษา ประวัติความเจ็บป่วยของครอบครัว ประวัติการแพ้ยา ประวัติความเจ็บป่วยในอดีต ผลการตรวจทางห้องปฏิบัติการ ผลเอกซเรย์ รวมถึงการบันทึกใด ๆ ที่เกิดจากการรักษาพยาบาล เอกสารยินยอมให้รักษาพยาบาล การกระทำตามคำสั่งของผู้มีอำนาจในการรักษาพยาบาลตามที่สถานบริการสาธารณสุขกำหนดไว้ และยังรวมถึงเอกสารทางการแพทย์ที่จัดเก็บอยู่ในระบบอิเล็กทรอนิกส์

จากการพัฒนาอย่างรวดเร็วของเทคโนโลยีสารสนเทศ ภาครัฐจึงได้บูรณาการระบบอิเล็กทรอนิกส์มาจัดเก็บข้อมูลของผู้มารับบริการในโรงพยาบาล เรียกว่าระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลทดลองใช้ใน 5 จังหวัดนำร่อง ได้แก่ นครนายก ภูเก็ต ร้อยเอ็ด เพชรบูรณ์ และ กาญจนบุรี เพื่ออำนวยความสะดวกให้ประชาชนที่มารับบริการในโรงพยาบาลและสถานพยาบาลภายใต้กำกับของภาครัฐ ได้รับทราบข้อมูลด้านสุขภาพของตนเอง ติดตามผลการรักษาสุขภาพ รวมถึงวางแผนการดูแลสุขภาพของตนเองได้ผ่านทางระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล แต่ปัญหาหรือการกระทำความผิดที่เกิดกับการใช้ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลนี้ยังไม่ปรากฏข้อเท็จจริงที่สามารถนำมาเป็น กรณีศึกษาได้ หรือแม้ว่าจะมีกรณีผิดพลาดเกิดขึ้นความเสียหายอาจยังไม่ปรากฏให้เห็น อีกทั้งเป็นการยากที่หน่วยงานที่เกี่ยวข้องจะเปิดเผยถึงข้อผิดพลาดและความเสียหายที่เกิดขึ้นจากการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล เนื่องจากจะทำให้ภาพลักษณ์ขององค์กรเสียหาย และทำให้ประชาชนผู้ใช้บริการขาดความเชื่อมั่นกับระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล

แม้ว่าข้อมูลส่วนบุคคลด้านสุขภาพเป็นเรื่องสำคัญที่ต้องได้รับการคุ้มครองแต่หลักการคุ้มครองตามกฎหมายต้องคำนึงถึงความสมดุลระหว่างประโยชน์ของเจ้าของข้อมูลและประโยชน์สาธารณะ งานวิจัยเล่มนี้จึงทำการศึกษาการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพตามกฎหมายของยุโรปและสหรัฐอเมริกา โดยศึกษากฎหมายที่มีหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพสูง ได้แก่กรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development–OECD) เรื่อง Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (Regulation (EU) 2016/679 General Data Protection Regulation –GDPR) และกฎหมายที่บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพโดยเฉพาะ ได้แก่พระราชบัญญัติว่าด้วยการควบคุมและการส่งผ่านข้อมูลทางด้านการประกันสุขภาพของสหรัฐอเมริกา (The Health Insurance Portability and Accountability Act of 1996 – HIPAA) จากการศึกษาพบว่ากฎหมายบัญญัติให้ข้อมูลส่วนบุคคลด้านสุขภาพเป็นความลับ เจ้าของข้อมูลมีสิทธิได้รับการคุ้มครองตามกฎหมายและกฎหมายต่างประเทศที่ผู้วิจัยได้กล่าวมาเบื้องต้น กำหนดมาตรการในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลด้านสุขภาพไว้หลายประการ คือการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลด้านสุขภาพ การเข้าถึงและขอใช้ข้อมูลส่วนบุคคลด้านสุขภาพ เป็นต้น แต่ได้กำหนดเหตุแห่งการยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพไว้เช่นกัน ซึ่งเหตุแห่ง

การยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพมี 3 ประการ ได้แก่ ความยินยอมจากเจ้าของข้อมูล เพื่อประโยชน์สาธารณะ และเพื่อประโยชน์ด้านสุขภาพของบุคคล เดิมประเทศไทยมีกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล คือ พระราชบัญญัติสุขภาพแห่งชาติ แต่เพื่อให้ประเทศไทยมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาลที่เป็นสากลทัดเทียมกับกฎหมายต่างประเทศและสอดคล้องกับวิวัฒนาการของเทคโนโลยี ภาครัฐได้บัญญัติกฎหมายได้แก่ ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในสถานพยาบาลต่าง ๆ ขึ้น จากการศึกษาพบว่ากฎหมายทั้ง 2 ฉบับยังมีปัญหาความไม่ครอบคลุมอยู่หลายประการ ได้แก่ ปัญหาขาดบทนิยามของข้อมูลสุขภาพส่วนบุคคล ปัญหาความไม่ชัดเจนของบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลด้านสุขภาพส่วนบุคคล นอกจากนี้ กฎหมายไทยยังไม่มีแนวปฏิบัติกลางเกี่ยวกับการจัดการข้อมูลด้านสุขภาพของบุคคลที่มีมาตรฐานเดียวกันระหว่างสถานพยาบาลของภาครัฐและภาคเอกชน

ข้อเสนอแนะ

จากการศึกษาผู้วิจัยเห็นว่าถึงแม้ว่าปัจจุบันประเทศไทยจะมีกฎหมายที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคลในภาพรวมและยังมีกฎระเบียบในเรื่องข้อมูลสุขภาพโดยเฉพาะซึ่งรวมถึงข้อมูลสุขภาพในระบบเวชระเบียนอิเล็กทรอนิกส์ (Electronic Health Records) อยู่แล้วก็ตาม แต่เป็นที่ทราบอยู่แล้วว่าข้อมูลสุขภาพมีลักษณะพิเศษต่างจากข้อมูลอื่น ๆ และในบางครั้งจำต้องมีการเปิดเผยข้อมูลสุขภาพส่วนบุคคลเพื่อประโยชน์ของส่วนรวม เช่นในกรณีเกิดโรคระบาด หรือเพื่อความปลอดภัยและคุณภาพชีวิตของผู้ป่วยในการรักษาพยาบาล บางครั้งจำเป็นต้องมีการแลกเปลี่ยนข้อมูลสุขภาพกันภายในกลุ่มผู้ให้การบริการด้านการรักษาพยาบาล ปัจจุบันเทคโนโลยีสารสนเทศที่ใช้ให้บริการด้านสุขภาพมีอยู่หลากหลายและแตกต่างกันในส่วนของสถานพยาบาลภาครัฐและเอกชน ทำให้ข้อมูลบางส่วนไม่สามารถเชื่อมต่อหรือบูรณาการข้อมูลด้วยกันจัดว่าเป็นการพัฒนาที่ไม่ก่อให้เกิดประโยชน์ กฎหมายที่มีบทบัญญัติเกี่ยวกับคุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่จัดเก็บในระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลยังไม่ครอบคลุม เนื่องจากปัญหาความไม่ชัดเจนของบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลด้านสุขภาพส่วนบุคคล ปัญหาการขาดบทนิยามที่เหมาะสม และความขัดแย้งกันเองของบทบัญญัติเดิมที่มีอยู่แล้ว

ผู้วิจัยจึงขอเสนอแนะแนวทางแก้ไขปัญหา 2 ประการ ดังนี้

1. แก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้ครอบคลุมทั้งข้อมูลส่วนบุคคลและข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ ผู้วิจัยจึงขอเสนอให้แก้ไขปรับปรุงดังนี้

1.1 เสนอให้เพิ่มเติมใน มาตรา 6 แห่งพระราชบัญญัตินี้โดยให้เพิ่มนิยาม “ข้อมูลสุขภาพส่วนบุคคล” ดังนี้

“ข้อมูลสุขภาพส่วนบุคคล หมายถึง ชื่อสกุล อายุ อาชีพ หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล์ ผลตรวจทางห้องปฏิบัติการ เช่น ผลตรวจเลือด ปัสสาวะ อุจจาระ เสมหะและน้ำไขสันหลัง ภาพหรือเสียงที่บันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ รวมถึงข้อมูลที่เกี่ยวเนื่องกับการรับบริการทางการแพทย์ เช่น ประวัติโรคประจำตัว ประวัติการผ่าตัด ประวัติการทำฟัน ประวัติการคลอด ยาที่ใช้เป็นประจำ ประวัติการดื่มเหล้า สูบบุหรี่ การประเมินสุขภาพจิต บันทึกทางการพยาบาล บันทึกของแพทย์ผู้ให้การรักษา การวางแผนการรักษาพยาบาล ความคิดเห็นในการวินิจฉัยโรคหรืออาการของผู้รับบริการ รวมถึงข้อมูลที่อ้างอิงถึงผู้ที่บันทึกได้ ซึ่งคลอบคลุมถึงข้อมูลของผู้ที่เสียชีวิตไปแล้วแต่ไม่เกิน 50 ปี”

1.2 เสนอให้เพิ่มเติมในหมวด 2 การเก็บรวบรวมข้อมูลส่วนบุคคล มาตรา 24 (2) โดยใช้ข้อความว่า เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพส่วนบุคคลของเจ้าของข้อมูล

1.3 เสนอให้เพิ่มเติมในหมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรา 31 ควรให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึง ใช้ เปิดเผยและส่งต่อข้อมูลส่วนบุคคลของตนเองไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นได้โดยไม่ต้องผ่านผู้ควบคุมข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลด้านสุขภาพเนื่องจากในปัจจุบันการเก็บรวบรวมข้อมูลส่วนบุคคลส่วนใหญ่มักเก็บไว้ในรูปแบบข้อมูลอิเล็กทรอนิกส์ทำให้การส่งต่อข้อมูลทำได้ง่ายขึ้น และเป็นการเพิ่มประสิทธิภาพในการดูแลรักษาพยาบาลในภาวะเจ็บป่วยทั้งฉุกเฉินและไม่ฉุกเฉิน โดยเพิ่มว่า

มาตรา 31 (3) การเข้าถึง ใช้ เปิดเผยและส่งต่อข้อมูลส่วนบุคคลของตนเองที่มีอยู่ยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น ในกรณีเร่งด่วน ฉุกเฉิน

1.4 เสนอให้เพิ่มเติมในหมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรา 37 ควรกำหนดกรอบระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลสุขภาพส่วนบุคคลโดยมีระยะเวลาในการเก็บข้อมูลไว้ไม่น้อยกว่า 10 ปี นับตั้งแต่การเข้ามารับบริการในโรงพยาบาลครั้งสุดท้าย เนื่องจากพระราชบัญญัติฉบับนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล

ต้องลบข้อมูลเมื่อพ้นระยะเวลาในการเก็บรักษา แต่มิได้พูดถึงระยะเวลาในการเก็บรักษาว่านานเท่าใดที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรักษาข้อมูลไว้ได้ ส่งผลให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้กำหนดระยะเวลาในการรักษาข้อมูลได้เอง จึงอาจทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรักษาข้อมูลส่วนบุคคลไว้นานเกินกว่าที่จำเป็น

2. แก้ไขเพิ่มเติมระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ในข้อ 4 แห่งระเบียบฉบับนี้ ให้เพิ่มนิยาม“ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล” ดังนี้

“ข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล หมายความว่า ทะเบียนหรือรายการข้อมูลด้านสุขภาพของบุคคลซึ่งจัดเก็บในรูปแบบอิเล็กทรอนิกส์ ที่สถานพยาบาลนำมาเก็บ จัดการใช้ เปิดเผยและส่งต่อข้อมูลเพื่อประโยชน์ของเจ้าของข้อมูลตามระเบียบนี้ได้”

จากการศึกษา ผู้วิจัยเห็นว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นต่อสังคมยุคปัจจุบันเพื่อเป็นบรรทัดฐานในกำหนดมาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบอิเล็กทรอนิกส์ งานวิจัยฉบับนี้จึงมุ่งหวังเพื่อจัดทำเป็นข้อเสนอแนะสำหรับประเทศไทยในการกำหนดมาตรการทางกฎหมายให้เหมาะสมสำหรับให้ภาครัฐและภาคเอกชนนำไปปฏิบัติตามเพื่อคุมครองข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บไว้ในระบบระเบียนสุขภาพส่วนบุคคลโดยเฉพาะ ดังนั้นการบังคับใช้กฎหมายจึงจำเป็นต้องกำหนดหลักเกณฑ์ที่รัดกุมในการเก็บและประมวลผลข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล รวมทั้งจำเป็นต้องมีคณะกรรมการเพื่อวางนโยบายและกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลส่งผลให้ข้อมูลส่วนบุคคลที่จัดเก็บในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลได้รับการคุ้มครองอย่างแท้จริง

บรรณานุกรม

(OCR), O. f. C. R. **Summary of the Hipaa Privacy Rule**. Retrieved july 2, 2018, from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Charles Ornstein. 13 Hospital Workers Fired for Snooping in Britney Spears' Medical Records. **Los Angeles Times**. Retrieved May 1, 2018, from: https://www.latimes.com/archives/la-xpm-2008-mar-15-me-britney15-story.html

David I. Bainbridge. (1996). **Computor and the Law**. London: Pitman Publishing.

The Eu General Data Protection Regulation (Gdpr) Is the Most Important Change in Data Privacy Regulation in 20 Years., Retrieved july 2, 2018, from: https://eugdpr.org/the-regulation/

Gdpr ฉบับภาษาไทย. (2562). แปลโดย นคร เสรีรักษ์, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร และนิชานันท์ นันทศิริศรณ์,. กรุงเทพฯ: พี.เพรส จำกัด.

Journal, H. **What Are the Penalties for Hipaa Violations.** Retrieved December 2, 2018, from: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Laurie Zabel, **10 Common Hipaa Violations and Preventative Measures to Keep Your Practice in Compliance**. Retrieved May 22,2019, from: https://www.beckershospitalreview.com/healthcare-information-technology/10-common-hipaa-violations-and-preventative-measures-to-keep-your-practice-in-compliance.html

Office for Civil Rights (OCR). **Summary of the Hipaa Privacy Rule**. Retrieved june 1, 2018, from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Protected Health Information. Retrieved july 2, 2018, from: https://www.truevault.com/protected-health-information

Reed Tinsley. **Hipaa and Britney Spears**. Retrieved july 2, 2018, from: http://www.rtacpa.com/blog/hipaa-and-britn

Social Security. **Wrongful Disclosure of Individually Identifiable Health Information**.

Retrieved june 7, 2018, from: https://www.ssa.gov/OP_Home/ssact/title11/1177.htm

U.S. Department of Health and Human Services Office for Civil Rights. "Hipaa Administrative Simplification Regulation Text (45 Cfr Parts 160, 162, and 164) ", March 2013.

กมลชัย รัตนสกาวงศ์. (2522). **ความยินยอมในกฎหมายอาญา**. วิทยานิพนธ์ น.ม., มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

กรมคุ้มครองสิทธิและเสรีภาพ. (2556). บทวิเคราะห์ข้อมูล สถานการณ์ และเชื่อมโยงเพื่อวางทิศทางแผนสิทธิมนุษยชนแห่งชาติ ฉบับที่ 3 (พ.ศ. 2557-2561). จัดทำโดยคณะรัฐมนตรีและราชกิจจานุเบกษา.

คณาธิป ทองรวีวงศ์. (2560). "The Oecd Privacy Framework " ใน **รายงานวิจัยฉบับสมบูรณ์ เรื่อง การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน** (43-44). กรุงเทพฯ: ม.ป.ท.

คำนิยาม, ค้นวันที่ 2 ธันวาคม 2561 จาก http://service.nso.go.th/nso/nso_center/ project/ table/files/S-hospital-p/2555/000/00_S-hospital-p_2555_000_ 000000_ 00002.pdf

จรัญ โฆษณานันท์. (2545). **สิทธิมนุษยชนไร้พรมแดน ปรัชญา กฎหมายและความเป็นจริงทางสังคม**. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

จันทจิรา เอี่ยมมยุรา. (2557). แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคลของประเทศไทย. **วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์**, 34(4), 653-657.

ไชยวัฒน์ จิรกิจไพบูลย์และคณะ. **ผู้ช่วยวิจัยได้อะไรบ้างจากการเข้าร่วมงาน Pdpa – Privacy for All**. สืบค้นเมื่อ 25 มีนาคม 2563 จาก https://medium.com/@mybooboy/%E0%B8%9C%E0%B8%B9%E0%B9%89%E0%B8%8A%E0%B9%88%E0%B8%A7%E0%B8%A2%E0%B8%A7%E0%B8%B4%E0%B8%88%E0%B8%B1%E0%B8%A2%E0%B9%84%E0%B8%94%E0%B9%89%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3%E0%B8%9A%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%88%E0%B8%B2%E0%B8%81%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%B2%E0%B8%A3%E0%B9%88%E0%B8%A7%E0%B8%A1%E0%B8%87%E0%B8%B2%E0%B8%99-pdpa-privacy-for-all-7fbef5a83d82.

โซเชียลซัด"เดลินิวส์" ไร้จรรยาบรรณลงภาพ "ปอ" ป่วย "รามา" ยันชุดคนป่วยไม่ใช่ของ รพ..

หนังสือพิมพ์ผู้จัดการออนไลน์. ค้นวันที่ 31 ธันวาคม 2562 จาก https://mgronline.com/onlinesection/detail/9580000125380.

ณาตยา ฉาบนาค. (2548). **ระบบสารสนเทศเพื่อการสื่อสาร.** (หน้า118) กรุงเทพฯ: เอส.พี. ซี.บุ๊คส.

ธาริณี มณีรอด. (2559). **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล**. วิทยานิพนธ์ น.ม., มหาวิทยาลัยธุรกิจบัณฑิตย์, กรุงเทพฯ.

นคร เสรีรักษ์. (ม.ป.พ.). **ข้อมูลส่วนบุคคลสำคัญไฉน**. สืบค้นเมื่อ 25 มีนาคม 2563, จาก http://www.fpps.or.th/news.php?detail=n1156791089.news.

นิธิพัฒน์ เจียรกุล. (2556). **จริยธรรมทางการแพทย์ยุคปัจจุบัน**. สืบค้นเมื่อ 30 กรกฎาคม 2561, จาก file:///C:/Users/User/Downloads/file%204.pdf.

ผู้เข้าอบรมหลักสูตรการพัฒนาความเชี่ยวชาญด้านนโยบายและยุทธศาสตร์สุขภาพ. (2561). **Flow Policy Adoption เรื่อง เทคโนโลยีสารสนเทศ Digital Transformation กระทรวงสาธารณสุข**. สืบค้นเมื่อ 2 ธันวาคม 2562, จาก http://164.115.25.41/ expertcenter/wp- content/uploads/2018/conference/ HPT3/ Report/G6.Paper-Digital-Transformation.pdf.

พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554. สืบค้นเมื่อ 3 ธันวาคม 2561, จาก http://www.royin.go.th/dictionary/.

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. สืบค้นเมื่อ 2 เมษายน 2562, จาก http://www.dla.go.th/upload/service/2554/6/21.pdf.

"พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562." หน้า 52-95, 24 พฤษภาคม 2562.

พลพร ปิยวรรณ และสุภาพร เชิงเอี่ยม. (2555). **ระบบสารสนเทศเพื่อการจัดการ**. หน้า 13. กรุงเทพฯ: ออฟเซ็ทพลัส.

เมธา สุวรรณสาร. (2552). **แนวทาง/กรอบการบริหารความเสี่ยงทั่วทั้งองค์กร**. สืบค้นเมื่อ 2 เมษายน 2562, จาก http://www.itgthailand.com/tag/risk-assessment-matrix/.

ยกเคสแชร์ภาพป่วย “ปอ ทฤษฎี” ทำไกด์ไลน์หมอใช้โซเชียล ชี้หารืออาการป่วยใน “กรุ๊ปไลน์” ได้แต่ห้ามแคปส่งต่อ. **หนังสือพิมพ์ผู้จัดการออนไลน์.** สืบค้นเมื่อ 1 มิถุนายน 2561, จาก: https://mgronline.com/qol/detail/9580000125416

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ.

2561. (28 มีนาคม 2561). **ราชกิจจานุเบกษา**. 135 (ตอนพิเศษ124 ง). สืบค้นเมื่อ 31 ธันวาคม 2562, จาก http://www.ratchakitcha.soc.go.th/ DATA/ PDF/ 2561/E/124/1.PDF.

วไล ณ ป้อมเพชร. (2551). สิทธิมนุษยชน/ลักษณะเฉพาะของสิทธิมนุษยชน. ใน **สารานุกรมไทยสำหรับเยาวชน** (หน้า126). กรุงเทพฯ: ม.ป.ท.

ศักดา สถิรเรืองชัย. (2556). **การรักษาความลับของผู้ป่วย. เวชบันทึกศิริราช**, 6(2), 1-6.

ศิริกุล ภู่พันธ์. "ข้อความคิดว่าด้วยข้อมูลส่วนบุคคล." กรุงเทพฯ, 2548.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC). **ระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล-Phr**. สืบค้นเมื่อ 2 ธันวาคม 2561, จาก https://www.nectec.or.th/innovation/innovation-software/phr.html

ศูย์เทคโนโลยีสารสนเทศและการสื่อสาร. **แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**. สืบค้นเมื่อ 2 ธันวาคม 2561, จาก https://wwwnno.moph. go.th/ downloads/policy/570813ictriskplan.pdf.

สอนชัย สิรารียกุล. **หมายเหตุท้ายฎีกา เรื่องความลับทางการค้า**. สืบค้นเมื่อ 22 กุมภาพันธ์ 2561, จาก https://www.lawsiam.com/?name=lawyer-download&file =filedetail&max=2497.

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์. **แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร**. สืบค้นเมื่อ 2 ธันวาคม 2561, จาก https://www. moph.go.th/downloads/policy/570813ictriskplan.pdf.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. **กฎหมาย Gdpr ฉบับรวบรัด**. สืบค้นเมื่อ 15 มีนาคม 2563, จาก https://www.etda.or.th/content/gdpr-in-a-nutshell

สำนักงานเลขาธิการวุฒิสภา. (2560). **รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560**. กรุงเทพฯ: ม.ป.ท.

สุพัชรินทร์ อัศวธิตานนท์. (2551). **พัฒนาการของหลักกฎหมาย Volenti Non Fit Injuria : ศึกษาการปรับใช้กับประเทศไทย**. วิทยานิพนธ์ น.ม., จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ.

สุรทศ ไตรติลานันท์ และสุรพล รวยสูงเนิน. (2559). กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล. **วารสารโรงพยาบาลขอนแก่น**, 26(2), 29-40.

อธิพร สิทธิธีรรัตน์. (2555). **ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์**. วิทยานิพนธ์ น.ม., มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

ภาคผนวก

ภาคผนวก ก ระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561



ระเบียบกระทรวงสาธารณสุข
เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑

โดยที่กระทรวงสาธารณสุขมีนโยบายที่จะให้ประชาชนทุกคนสามารถเข้าถึงบริการด้านการให้คำแนะนำด้านสุขภาพและวินิจฉัยโรคเบื้องต้น โดยบูรณาการระบบประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์เชื่อมต่อกันทั้งประเทศที่ประชาชนสามารถเข้าถึงและบริหารจัดการข้อมูลสุขภาพของตนเองได้ เพื่ออำนวยความสะดวกในการเข้ารับการรักษาและเป็นข้อมูลสำคัญประกอบการรักษากรณีฉุกเฉิน นอกจากนี้ข้อมูลสุขภาพด้านบุคคลยังสามารถนำไปใช้ประโยชน์ในการพัฒนาระบบสุขภาพของประเทศต่อไป ดังนั้นจึงมีความจำเป็นที่จะต้องมีการควบคุม กำกับเพื่อให้การได้มา การบริหารจัดการ การใช้และการคุ้มครองข้อมูลด้านสุขภาพของบุคคลมีความสะดวก ปลอดภัย เกิดประโยชน์สูงสุดแก่ประชาชนเจ้าของข้อมูล หน่วยบริการและระบบสุขภาพของประเทศไทย จึงเป็นการสมควรมีระเบียบ เรื่องการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล เพื่อกำหนดหลักเกณฑ์ วิธีการ และแนวทางปฏิบัติให้เหมาะสม สอดคล้องกับพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายอื่นที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๐ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม รัฐมนตรีว่าการกระทรวงสาธารณสุขจึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกระทรวงสาธารณสุขเรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวัน (๑๒๐ วัน) นับจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในกรณีที่การดำเนินการใดๆ เกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ระเบียบนี้ไม่ได้กำหนดไว้ให้ปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศหรือคำสั่งที่ออกตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายอื่นที่เกี่ยวข้อง

ข้อ ๔ ในระเบียบนี้

“ข้อมูลด้านสุขภาพของบุคคล” หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อมูลด้านสุขภาพของบุคคลที่เป็นเอกสารหรือข้อความในรูปแบบอิเล็กทรอนิกส์

“ระเบียน...

“ระเบียนสุขภาพ” หมายความว่า ทะเบียนหรือรายการ ข้อมูลด้านสุขภาพของบุคคลที่กระทรวงสาธารณสุข หน่วยงานทั้งภาครัฐและเอกชน นำมาเก็บ จัดการ ใช้และเปิดเผยเพื่อประโยชน์ของเจ้าของข้อมูลตามระเบียบนี้

“เจ้าของข้อมูล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลด้านสุขภาพ

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

“ผู้บริหารจัดการข้อมูล” หมายความว่า กระทรวงสาธารณสุขรวมถึงบุคคลหรือหน่วยงานที่ได้รับมอบหมายจากกระทรวงสาธารณสุข

"ผู้รับข้อมูล" หมายความว่า บุคคลหรือนิติบุคคลที่ได้รับข้อมูลด้านสุขภาพของบุคคลจากผู้ควบคุมข้อมูลและนำข้อมูลนั้นไปใช้เพื่อประโยชน์ของเจ้าของข้อมูล

"คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล

"เจ้าหน้าที่" หมายความว่า ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างของกระทรวงสาธารณสุขที่ปฏิบัติงานเกี่ยวกับข้อมูลด้านสุขภาพของกระทรวงสาธารณสุข

ข้อ ๕ การจัดทำระเบียนสุขภาพ การจัดการ เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลด้านสุขภาพของบุคคลต้องเป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลหรือเพื่อดำเนินงานตามหน้าที่และอำนาจของผู้ควบคุมข้อมูล หรือหน้าที่และอำนาจของกระทรวงสาธารณสุขตามที่ได้รับมอบหมาย

หมวด ๑
คณะกรรมการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล

ข้อ ๖ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า "คณะกรรมการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล" ประกอบด้วย

(๑) ปลัดกระทรวงสาธารณสุขเป็นประธานกรรมการ

(๒) รองปลัดกระทรวงสาธารณสุขผู้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกระทรวงสาธารณสุขเป็นรองประธานกรรมการ

(๓) ผู้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำสำนักงานปลัดกระทรวงสาธารณสุข ผู้แทนกรมควบคุมโรค ผู้แทนกรมสุขภาพจิต ผู้แทนกรมการแพทย์ ผู้แทนกรมสนับสนุนบริการสุขภาพ ผู้แทนนายแพทย์สาธารณสุขจังหวัด ผู้แทนโรงพยาบาลในสังกัดสำนักงานปลัดกระทรวงสาธารณสุขและผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่ปลัดกระทรวงสาธารณสุขแต่งตั้งจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค สำนักงานคณะกรรมการกฤษฎีกา และสำนักงานคณะกรรมการสุขภาพแห่งชาติหน่วยงานละ ๑ คน เป็นกรรมการ

(๔) นักวิชาการที่ปลัดกระทรวงสาธารณสุขแต่งตั้งจำนวน ๒ คนเป็นกรรมการ

(๕) ผู้อำนวยการ...

(๕) ผู้อำนวยการกองบริหารการสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๖) ผู้อำนวยการกองกฎหมาย สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๗) ผู้อำนวยการกองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๘) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการและเลขานุการ

ให้เลขานุการแต่งตั้งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจำนวนไม่เกิน ๒ คนเป็นผู้ช่วยเลขานุการ

ข้อ ๗ ให้คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) กำหนดข้อมูลที่จะต้องนำไปไว้ในระเบียนสุขภาพ

(๒) กำหนดนโยบายการดำเนินการและการพัฒนาข้อมูลด้านสุขภาพของบุคคลและระเบียนสุขภาพ

(๓) กำหนดข้อมูลด้านสุขภาพของบุคคลตามข้อ ๑๑ (๕)

(๔) ออกประกาศ ข้อกำหนด หลักเกณฑ์หรือแนวทางการปฏิบัติในการจัดการข้อมูลด้านสุขภาพของบุคคลให้เกิดประโยชน์สูงสุดกับเจ้าของข้อมูลตามข้อ ๒๙

(๕) ออกประกาศ ข้อกำหนด หลักเกณฑ์หรือแนวทางปฏิบัติตามข้อ ๓๐ และข้อ ๓๑

(๖) ออกประกาศ ข้อกำหนด หลักเกณฑ์เกี่ยวกับทะเบียนผู้ควบคุมข้อมูลและผู้รับข้อมูลตามข้อ ๓๓

(๗) ดำเนินการต่าง ๆ เพื่อให้เป็นไปตามวัตถุประสงค์ของระเบียนสุขภาพตามข้อ ๒๗

(๘) ติดตาม กำกับการดำเนินการจัดการข้อมูลด้านสุขภาพของบุคคล

(๙) เสนอแนะหรือให้คำปรึกษาแก่รัฐมนตรีว่าการกระทรวงสาธารณสุขหรือปลัดกระทรวงสาธารณสุขในการดำเนินการเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลของกระทรวงสาธารณสุข

(๑๐)แต่งตั้งคณะอนุกรรมการหรือที่ปรึกษาเพื่อดำเนินการตามระเบียบนี้หรือตามที่คณะกรรมการมอบหมาย

(๑๑)พิจารณาทบทวนระเบียบนี้ให้มีความเหมาะสมกับสถานการณ์ และเสนอแก้ไขระเบียบต่อรัฐมนตรีว่าการกระทรวงสาธารณสุข

(๑๒)ปฏิบัติการอื่นใดเพื่อให้บรรลุวัตถุประสงค์ของระเบียบนี้

ข้อ ๘ การประชุมคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงจะเป็นองค์ประชุม

ในการประชุมคณะกรรมการถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ให้รองประธานกรรมการเป็นประธานในที่ประชุม ถ้ารองประธานกรรมการไม่มาหรือไม่อาจปฏิบัติหน้าที่ได้ให้ที่ประชุมเลือกกรรมการคนหนึ่งทำหน้าที่ประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงในการลงคะแนนเท่ากันให้ประธานกรรมการออกเสียงเพิ่มอีกหนึ่งเสียงเป็นเสียงชี้ขาด

ข้อ ๙ การประชุมคณะอนุกรรมการให้นำข้อ ๘ มาบังคับใช้โดยอนุโลม

ข้อ ๑๐ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ทำหน้าที่สำนักงานเลขานุการคณะกรรมการ เพื่อดำเนินการตามที่คณะกรรมการมอบหมายและตามที่กำหนดไว้ในระเบียบนี้

หมวด ๒
การคุ้มครองข้อมูลด้านสุขภาพของบุคคล

ข้อ ๑๑ ข้อมูลดังต่อไปนี้ถือเป็นข้อมูลด้านสุขภาพของบุคคล

(๑) ประวัติสุขภาพเฉพาะของบุคคล เช่น ส่วนสูง น้ำหนัก หมู่เลือด รูปร่างลักษณะทั่วไปของร่างกายเป็นต้น

(๒) ประวัติการรักษาพยาบาล เช่น เวชระเบียน บันทึกการพยาบาล การตรวจทางห้องปฏิบัติการ ฟิล์มเอ็กซ์เรย์ เป็นต้น

(๓) เอกสารและวัตถุต่างๆ ที่เกี่ยวกับ (๑) และ (๒)

(๔) ภาพถ่ายการปฏิบัติงานรักษาพยาบาลผู้ป่วยของบุคลากรทางการแพทย์หรือเจ้าหน้าที่อื่นในการรักษาพยาบาล รวมถึงการกระทำด้วยประการใดๆ ให้ปรากฏภาพ เสียงของบุคคลดังกล่าว

(๕) ข้อมูลที่คณะกรรมการกำหนด

ข้อ ๑๒ ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดให้มีสถานที่เก็บรวบรวมข้อมูลด้านสุขภาพของบุคคลให้อยู่ในสภาพที่เหมาะสม มีมาตรการด้านความปลอดภัยที่รัดกุม

เจ้าหน้าที่ต้องเป็นผู้ที่มีความรู้ด้านการจัดการข้อมูลและด้านกฎหมายที่เกี่ยวข้อง

ข้อ ๑๓ ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล จะเปิดเผยได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลหรือผู้มีอำนาจกระทำการแทนตามข้อ ๑๔ (๒) - (๕) และตามที่กฎหมายบัญญัติไว้เท่านั้น และการเปิดเผยจะทำให้เกิดความเสียหายแก่เจ้าของข้อมูลและผู้ครอบครองข้อมูลไม่ได้

ข้อ ๑๔ บุคคลดังต่อไปนี้ มีสิทธิขอให้เปิดเผยข้อมูลด้านสุขภาพของบุคคล

(๑) ผู้เป็นเจ้าของข้อมูล

(๒) ผู้ที่ได้รับมอบอำนาจจากผู้เป็นเจ้าของข้อมูล

(๓) ผู้ที่ได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล

(๔) ผู้มีอำนาจกระทำการแทนเจ้าของข้อมูล คือ ผู้แทนโดยชอบธรรม กรณีเจ้าของข้อมูลเป็นเด็กหรือผู้เยาว์ ผู้อนุบาล กรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถหรือผู้พิทักษ์ กรณีเจ้าของข้อมูลเป็นคนเสมือนไร้ความสามารถ ทั้งนี้ถ้าผู้เยาว์อายุ ๑๕ ปีบริบูรณ์แล้วต้องได้รับความยินยอมจากผู้เยาว์นั้นก่อน

(๕) ทายาท ในกรณีผู้เป็นเจ้าของข้อมูลเสียชีวิต

ทายาทตาม (๕) หมายถึง สามีหรือภรรยาโดยชอบด้วยกฎหมาย บุตรหรือผู้สืบสันดานตามความเป็นจริง บุตรบุญธรรมตามกฎหมาย บิดาหรือมารดาตามความเป็นจริง

ข้อ ๑๕...

ข้อ ๑๕ บุคคลดังต่อไปนี้มีอำนาจขอให้ผู้ควบคุมข้อมูล เปิดเผยข้อมูลด้านสุขภาพของบุคคลโดยไม่จำต้องได้รับความยินยอมจากเจ้าของข้อมูลหรือผู้มีอำนาจกระทำการคือ ศาล พนักงานสอบสวนเจ้าหน้าที่ตำรวจ คณะกรรมาธิการ คณะกรรมการ คณะอนุกรรมการและเจ้าหน้าที่ที่มีกฎหมายให้อำนาจในการเรียกเอกสารข้อมูลด้านสุขภาพของบุคคลได้ ทั้งนี้ ต้องอยู่ภายใต้หลักการไม่เป็นการนำข้อมูลไปใช้ในทางให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือทายาท

ข้อ ๑๖ ผู้ขอข้อมูลจะต้องดำเนินการดังต่อไปนี้

(๑) ยื่นคำขอเป็นหนังสือและลงลายมือชื่อผู้ขอ

(๒) ระบุวัตถุประสงค์ของการขอข้อมูลว่าจะนำไปใช้ประโยชน์อย่างไร

(๓) แนบเอกสารประกอบการขอข้อมูลตามที่กำหนดไว้

(๔) รับทราบเงื่อนไขที่ผู้ควบคุมข้อมูลกำหนด

ข้อ ๑๗ เอกสารประกอบคำขอตามข้อ ๑๖ (๓) มีดังนี้

(๑) สำเนาบัตรประจำตัวผู้ขอ

(๒) กรณีเป็นผู้รับมอบอำนาจ ต้องมีสำเนาบัตรประจำตัวผู้มอบอำนาจ ผู้รับมอบอำนาจและหนังสือมอบอำนาจ (ติดอากรแสตมป์) ด้วย

(๓) กรณีเจ้าของข้อมูลให้ความยินยอม ต้องมีหนังสือแสดงความยินยอมที่ลงลายมือชื่อเจ้าของข้อมูลมาแสดงด้วย (ถ้าเป็นสำเนาควรขอดูตัวจริง)

(๔) กรณีทายาท ต้องมีใบมรณะบัตรและเอกสารแสดงการเป็นทายาท เช่น ใบทะเบียนสมรส สำเนาทะเบียนบ้าน สูติบัตร คำสั่งศาล เป็นต้น

(๕) กรณีเป็นทารก เด็ก ผู้เยาว์ หรือผู้ที่ไม่สามารถช่วยเหลือตนเองได้หรือเป็นผู้พิการไม่สามารถรับรู้การกระทำหรือเป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ ผู้แทนโดยชอบธรรมคือบิดาหรือมารดาตามความเป็นจริง ผู้ปกครองที่ศาลตั้ง ผู้อนุบาลหรือผู้พิทักษ์ต้องแสดงคำสั่งศาลหรือหลักฐานที่แสดงการเป็นผู้ปกครอง ผู้อนุบาล ผู้พิทักษ์ หรือผู้แทนโดยชอบธรรม

(๖) เอกสารอื่นๆตามที่ผู้ควบคุมข้อมูลกำหนด

ข้อ ๑๘ เมื่อเจ้าหน้าที่ได้รับคำขอให้ตรวจคำขอและเอกสารที่เกี่ยวข้องให้ถูกต้องครบถ้วนแล้วจึงเสนอคำขอพร้อมความเห็นไปให้ผู้มีอำนาจพิจารณาอนุมัติให้เปิดเผยข้อมูลดังกล่าวหรืออาจนำเสนอคณะกรรมการข้อมูลข่าวสารของผู้ควบคุมข้อมูลก่อนก็ได้

ผู้มีอำนาจกระทำการแทนผู้ควบคุมข้อมูลหรือผู้ที่ได้รับมอบหมายเป็นผู้มีอำนาจอนุมัติการเปิดเผยข้อมูลด้านสุขภาพของบุคคล

ข้อ ๑๙ ในกรณีผู้ขอให้เปิดเผยข้อมูล ขอสำเนาข้อมูลด้านสุขภาพของบุคคลให้กำหนดเงื่อนไข ดังนี้

(๑) ผู้ขอต้องใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

(๒) ผู้ขอต้องไม่นำข้อมูลไปเผยแพร่ จำหน่าย จ่าย แจก หรือกระทำโดยประการใดๆ ในลักษณะเช่นว่านั้น

(๓) ผู้ขอต้องไม่นำข้อมูลไปใช้ในทางที่อาจจะก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือผู้ควบคุมข้อมูล หากมีความเสียหายเกิดขึ้น ผู้ขอต้องรับผิดชอบทั้งสิ้น

เมื่อผู้ขอข้อมูลลงนามรับทราบเงื่อนไขดังกล่าวแล้วจึงมอบสำเนาข้อมูลดังกล่าวแก่ผู้ขอต่อไป ในกรณีผู้ขอรับทราบเงื่อนไขแล้วไม่ยอมลงนามให้บันทึกไว้และเจ้าหน้าที่ลงนามกำกับพร้อมพยานและมอบสำเนาข้อมูลให้ผู้ขอ

ข้อ ๒๐...

ข้อ ๒๐ ในกรณีผู้ขอข้อมูลไม่ใช่เจ้าของข้อมูล และเจ้าหน้าที่เห็นว่า ควรมีการขอความยินยอมจากเจ้าของข้อมูลก่อน ให้ผู้ขอดำเนินการขอความยินยอมจากเจ้าของข้อมูลก่อน

ข้อ ๒๑ ผู้ควบคุมข้อมูล อาจขอให้เจ้าของข้อมูลให้ความยินยอมล่วงหน้าในการเปิดเผยข้อมูลด้านสุขภาพของบุคคล ในกรณีดังต่อไปนี้

(๑) ต่อบุคลากรทางการแพทย์ของผู้ควบคุมข้อมูล ในการปฏิบัติงานในหน้าที่หรือเพื่อประโยชน์ของเจ้าของข้อมูล

(๒) เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อ หรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลด้านสุขภาพของบุคคลใด

(๓) เป็นการจำเป็นเพื่อการป้องกัน หรือระงับอันตรายต่อชีวิต หรือสุขภาพของบุคคล

(๔) มีเหตุจำเป็นอื่น ๆ เพื่อประโยชน์ของเจ้าของข้อมูล (ถ้ามี)

ในการดำเนินการตามวรรคหนึ่ง ต้องอธิบายให้เจ้าของข้อมูลทราบและเข้าใจด้วย

ในกรณีเป็นการศึกษา วิเคราะห์ วิจัยเพื่อการพัฒนางานด้านสุขภาพของผู้ควบคุมข้อมูลถือเป็นการปฏิบัติงานในหน้าที่และอำนาจของผู้ควบคุมข้อมูลให้สามารถดำเนินการได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล

ข้อ ๒๒ เมื่อได้ดำเนินการจนเสร็จสิ้นแล้ว ให้เก็บเอกสารต่าง ๆ ไว้เป็นหลักฐานด้วย

หมวด ๓
การแก้ไขข้อมูลด้านสุขภาพของบุคคล

ข้อ ๒๓ เจ้าของข้อมูลมีสิทธิที่จะขอให้แก้ไขข้อมูลด้านสุขภาพของตนเอง โดยยื่นคำขอต่อผู้ควบคุมข้อมูลพร้อมพยานหลักฐานแสดงข้อมูลที่ถูกต้องตามความเป็นจริงเมื่อเจ้าหน้าที่ได้ตรวจสอบแล้วเห็นว่าถูกต้องให้เสนอผู้มีอำนาจอนุมัติและทำการแก้ไขข้อมูลดังกล่าวแล้วแจ้งเจ้าของข้อมูลทราบต่อไป

ข้อ ๒๔ เจ้าหน้าที่ผู้เขียนข้อมูลด้านสุขภาพของบุคคลอาจแก้ไขข้อมูลได้ โดยอยู่ในเงื่อนไขดังนี้

(๑) ต้องแก้ไขตามความเป็นจริง

(๒) ไม่ควรแก้ไข โดยลบหรือขีดฆ่าโดยไม่จำเป็น ถ้าต้องการแก้ไขโดยขีดฆ่าต้องเซ็นชื่อกำกับทุกครั้ง

(๓) การเพิ่มเติมแก้ไขทุกครั้งให้เขียนเหตุผลไว้ด้วย โดยอาจมีบันทึกติดไว้กับเวชระเบียน หรือทำรายการไว้ท้ายเวชระเบียนหน้านั้น ๆ

(๔) เมื่อมีการแก้ไขให้มีหัวหน้าหน่วยและผู้ที่อยู่ในเหตุการณ์ลงชื่อเป็นพยานด้วย

(๕) ไม่ควรแก้ไขเมื่อมีการร้องเรียนหรือฟ้องร้องคดีแล้ว

หมวด ๔...

หมวด ๔
ข้อมูลทางอิเล็กทรอนิกส์

ข้อ๒๕ ผู้ควบคุมข้อมูลและผู้บริหารจัดการข้อมูลที่ดำเนินการเก็บ รวมรวม ใช้ และเปิดเผยข้อมูลด้านสุขภาพส่วนบุคคลโดยวิธีการทางอิเล็กทรอนิกส์ต้องมีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ซึ่งเป็นวิธีการที่เชื่อถือได้อย่างน้อยต้องครอบคลุมหัวข้อดังต่อไปนี้

(๑) การเข้าถึงและควบคุมการใช้งาน โดยต้องมีองค์ประกอบดังนี้

(ก) การระบุตัวตน (Identification)

(ข) การยืนยันตัวตน (Authentication)

(ค) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

(ง) ความรับผิดชอบต่อผลการกระทำ (Accountability)

ทั้งนี้เพื่อให้สามารถยืนยันได้ว่าข้อมูลอิเล็กทรอนิกส์ที่มีการจัดทำหรือแปลงได้ดำเนินการโดยผู้มีสิทธิเข้าถึงเท่านั้น ผู้มีสิทธิในการเข้าถึงดังกล่าวให้หมายความรวมถึงผู้รับผิดชอบดำเนินงานจัดทำหรือแปลงเอกสารหรือข้อความและผู้มีสิทธิตรวจสอบซึ่งจะเป็นคนเดียวกันหรือไม่ก็ได้

(๒) จัดให้มีระบบการใช้งานและระบบสำรองซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงของระบบที่ใช้อย่างสม่ำเสมอ

ข้อ๒๖ ในการส่งต่อข้อมูลทางอิเล็กทรอนิกส์ ผู้ควบคุมข้อมูล และผู้บริหารข้อมูลต้องจัดให้มีการบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบการจัดการข้อมูลด้านสุขภาพของบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้วและต้องมีการดำเนินการดังนี้

(๑) ฝึกอบรมสร้างความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักในผลกระทบที่อาจเกิดจากการใช้งานระบบการจัดการข้อมูลด้านสุขภาพของบุคคล รวมถึงการกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ให้งาน (user registration) โดยต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบแล้วและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access right) โดยต้องจัดให้มีกระบวนการทบทวนการเข้าถึงสิทธิของผู้ใช้งานระบบการจัดการข้อมูลด้านสุขภาพของบุคคลตามระยะเวลาที่กำหนดไว้

(๖) การป้องกัน...

(๖) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์โดยต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๗) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์โดยต้องควบคุมไม่ให้สินทรัพย์ เช่น เอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

(๘) การควบคุมเครือข่าย (network access control)

(๙) การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

ทั้งนี้ให้เป็นไปตามประกาศนโยบายการรักษาความมั่นคงปลอดภัยของกระทรวงสาธารณสุข ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งมาตรการตามเอกสารหมายเลข ๑ แนบท้ายระเบียบนี้

หมวด ๕
ระเบียนสุขภาพ

ข้อ ๒๗ ระเบียนสุขภาพจัดทำขึ้นเพื่อ

(๑) รวบรวมข้อมูลด้านสุขภาพของบุคคลของประชาชน

(๒) คุ้มครองข้อมูลด้านสุขภาพของบุคคล

(๓) นำข้อมูลด้านสุขภาพของบุคคลไปใช้ประโยชน์ในการดูแลสุขภาพของเจ้าของข้อมูลนั้น

(๔) นำไปศึกษา วิเคราะห์ วิจัย เพื่อพัฒนาระบบสุขภาพของประเทศ

(๕) ให้หน่วยงานที่เกี่ยวข้องสามารถนำข้อมูลด้านสุขภาพของบุคคลไปใช้เพื่อประโยชน์ของเจ้าของข้อมูล และหน่วยงานนั้น

(๖) การอื่นที่คณะกรรมการกำหนด

ข้อ ๒๘ ระเบียนสุขภาพ ประกอบด้วยข้อมูลด้านสุขภาพของบุคคล ทั้งนี้ให้เป็นไปตามเอกสารหมายเลข ๒ แนบท้ายของระเบียบนี้

ข้อ ๒๙ ผู้บริหารจัดการข้อมูลเป็นผู้ดำเนินการบริหารจัดการข้อมูลเพื่อประโยชน์ของเจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องตามหลักเกณฑ์ เงื่อนไข และวิธีการที่คณะกรรมการกำหนด

ข้อ ๓๐ ผู้บริหารจัดการข้อมูลต้องจัดให้มีสถานที่จัดเก็บข้อมูลด้านสุขภาพของบุคคลที่เหมาะสม มีระบบการรักษาความปลอดภัยของการเก็บ การรวบรวม การใช้และการเปิดเผยข้อมูลตามที่คณะกรรมการกำหนด

ข้อ ๓๑ ผู้ควบคุมข้อมูลต้องเป็นผู้ดำเนินการส่งมอบข้อมูลด้านสุขภาพของบุคคลให้ผู้บริหารจัดการข้อมูลเพื่อจัดทำระเบียนสุขภาพรวมทั้งขอความยินยอมจากเจ้าของข้อมูลตามแบบที่กำหนดท้ายระเบียบนี้หรือตามที่คณะกรรมการกำหนด

ในกรณีเจ้าของข้อมูลไม่ยินยอมให้บันทึกไว้เป็นหลักฐานด้วย

ข้อ ๓๒...

ข้อ ๓๒ ผู้ควบคุมข้อมูลมีหน้าที่ต้องตรวจสอบและบันทึกข้อมูลให้เป็นปัจจุบันเสมอและส่งมอบให้ผู้บริหารจัดการข้อมูลภายในเวลาที่กำหนด

ข้อ ๓๓ ผู้บริหารจัดการข้อมูลต้องจัดให้มีทะเบียนผู้ควบคุมข้อมูลและผู้รับข้อมูลการจัดการข้อมูลตามหลักเกณฑ์ วิธีการ และเงื่อนไขการใช้งานข้อมูลด้านสุขภาพของบุคคลที่คณะกรรมการกำหนด

ข้อ ๓๔ เมื่อผู้รับข้อมูลได้รับข้อมูลและใช้ประโยชน์แล้ว ต้องส่งข้อมูลด้านสุขภาพของบุคคลที่เป็นปัจจุบันของเจ้าของข้อมูลไปให้ผู้บริหารจัดการข้อมูลเพื่อเก็บรวบรวม และใช้ประโยชน์ตามที่ระเบียบนี้กำหนดไว้ต่อไป

ข้อ ๓๕ ให้ปลัดกระทรวงสาธารณสุขเป็นผู้รักษาการตามระเบียบนี้

ประกาศ ณ วันที่ ๒๘ เดือน มีนาคม พ.ศ. ๒๕๖๑

(นายปิยะสกล สกลสัตยาทร)
รัฐมนตรีว่าการกระทรวงสาธารณสุข

ภาคผนวก ข หนังสือแสดงความยินยอม

หนังสือแสดงความยินยอมให้เปิดเผยข้อมูลด้านสุขภาพของบุคคลทางอิเล็กทรอนิกส์

สถานที่.....
วันที่.....เดือน.....พ.ศ. .....
เวลา.....น.

1. ข้าพเจ้า นาย / นาง / นางสาว .....อายุ.....ปี
   - ❑ เลขประจำตัวประชาชน ☐-☐☐☐☐-☐☐☐☐☐-☐☐-☐
   - ❑ ใบสำคัญประจำตัวคนต่างด้าวเลขที่ .....
   - ❑ อื่นๆ เช่น หนังสือเดินทางเลขที่.....

   วันออกบัตร ...../...../..... วันบัตรหมดอายุ ...../...../.....
   ออกให้โดย.....
   ในฐานะ ❑ ผู้ป่วย
   ❑ ผู้มีอำนาจกระทำแทนผู้ป่วยเกี่ยวข้องเป็น.....ของผู้ป่วย
   ชื่อ นาย/นาง/นางสาว/เด็กชาย/เด็กหญิง/อื่น ๆ.....
   ชื่อ..... สกุล.....

2. ข้าพเจ้า ได้รับการอธิบายจากสถานพยาบาลที่อยู่ภายใต้โครงการพัฒนาระบบระเบียนสุขภาพส่วนบุคคล (Personal Health Record : PHRs) (โรงพยาบาล.....) ให้ทราบถึงวัตถุประสงค์ในการให้คำยินยอมเพื่อการแลกเปลี่ยนข้อมูลระหว่างสถานพยาบาล โดยสามารถนำข้อมูลระดับบุคคลไปใช้ประโยชน์ในการบริการดูแลสุขภาพ อาทิการจัดเก็บข้อมูลการตรวจรักษา/การผ่าตัด/การใช้ยา/ตรวจรักษาทางรังสีและกระทำหัตถการ ทั้งนี้ รวมถึงความเสี่ยงผลข้างเคียงและภาวะแทรกซ้อนไว้โดยวิธีการทางอิเล็กทรอนิกส์เพื่อประโยชน์ในการดูแลสุขภาพของข้าพเจ้าแล้ว

3. ข้าพเจ้า ❑ ยินยอมเข้าสู่โครงการพัฒนาระบบระเบียนสุขภาพส่วนบุคคล (PHRs)
   ❑ ยินยอมให้สถานพยาบาลเปิดเผยข้อมูล/ส่งข้อมูล ทางอิเล็กทรอนิกส์ (สำเนาข้อมูล) เพื่อการรักษาพยาบาลแก่ผู้ประกอบวิชาชีพด้านสาธารณสุข (บุคลากรที่ได้รับอนุญาตในการรักษาพยาบาล) และสถานพยาบาลที่ให้บริการรักษาได้
   ❑ ไม่ยินยอม* ให้สถานพยาบาลเปิดเผยข้อมูล/ส่งข้อมูล ทางอิเล็กทรอนิกส์ (สำเนาข้อมูล) เพื่อการรักษาพยาบาลแก่ผู้ประกอบวิชาชีพด้านสาธารณสุข (บุคลากรที่ได้รับอนุญาตในการรักษาพยาบาล) และสถานพยาบาลที่ให้บริการรักษาได้

4. หากสถานพยาบาลนำข้อมูลสุขภาพส่วนบุคคลของข้าพเจ้าไปใช้เพื่อการอื่นใดอันไม่เป็นประโยชน์ต่อการรักษาพยาบาล ต้องได้รับคำยินยอมจากข้าพเจ้าเว้นแต่การเปิดเผยตามที่กฎหมายบัญญัติหรือมีคำสั่งศาลให้เปิดเผย

5. ข้าพเจ้า สามารถยกเลิกความยินยอมได้ แต่ไม่มีผลลบล้างความยินยอมและผลแห่งความยินยอม ซึ่งได้กระทำไปแล้วก่อนหน้านั้น โดยการยกเลิกความยินยอมต้องมีหลักฐานเป็นลายลักษณ์อักษร

ลงชื่อ.....ผู้ป่วย/ผู้มีอำนาจกระทำแทน
(.....)

ลงชื่อ.....ผู้แทนสถานพยาบาล
(.....)

ลงชื่อ.....พยาน
(.....)

ลงชื่อ.....พยาน
(.....)

หมายเหตุ : ผู้มีอำนาจกระทำแทนผู้ป่วยได้แก่

1. ผู้ป่วยกรณีบรรลุนิติภาวะ และมีสติสัมปชัญญะสมบูรณ์
2. สามีหรือภรรยาตามกฎหมาย และฝ่ายใดฝ่ายหนึ่งไม่มีสติสัมปชัญญะ (ไม่รู้สึกตัว)
3. ผู้แทนโดยชอบธรรม กรณีผู้ป่วยยังไม่บรรลุนิติภาวะ
4. ผู้อนุบาล กรณีผู้ป่วยเป็นคนวิกลจริต หรือคนไร้ความสามารถ
5. ผู้พิทักษ์ กรณีผู้ป่วยเป็นคนเสมือนไร้ความสามารถ

ไม่ยินยอม* ผู้ป่วยจะได้รับการรักษาพยาบาล แต่ในกรณีที่ต้องใช้ข้อมูลระหว่างสถานพยาบาล (ส่งต่อ) เพื่อการรักษา หรือกรณีฉุกเฉินหรือกรณีพิเศษ สถานพยาบาลต้องให้ผู้ป่วย/ผู้ให้คำยินยอมอนุญาตก่อน มีการส่งข้อมูลตามระบบปกติ

ภาคผนวก ค มาตรฐานข้อมูลระบบประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์

รูปแบบมาตรฐาน 3 กลุ่ม ตามลักษณะข้อมูล

1. ข้อมูลการตรวจสุขภาพ
2. ข้อมูลการส่งเสริมสุขภาพป้องกันโรค
3. ข้อมูลการรักษาพยาบาล

1. ข้อมูลการตรวจสุขภาพ

Part 1. การตรวจร่างกาย

1. ชื่อ-นามสกุล..... 2. อายุ.....   3. เพศ..... 4. วันที่ตรวจ.....
5. โรคประจำตัว.....
6. น้ำหนัก..... 7. ส่วนสูง.....   8. ดัชนีมวลกาย.....   การแปลผล .....ข้อแนะนำ.....
9. รอบเอว.....   การแปลผล .....ข้อแนะนำ.....
10. ความดันโลหิต.....มม.ปรอท ค่าปกติ.....มม.ปรอท   11. ชีพจร.....   การแปลผล .....ข้อแนะนำ.....
12. ผลการตรวจร่างกายโดยแพทย์   ....   ข้อแนะนำ..... .....

Part 2. การตรวจทางห้องปฏิบัติการ

- ผลการตรวจเลือด ปัสสาวะ อุจจาระ ฯลฯ
- การแปลผล และ คำแนะนำ

Part 3. สรุปผล

1. สรุปผลการตรวจสุขภาพ ☐ ปกติ ☐ ผิดปกติเล็กน้อย ☐ ผิดปกติควรพบแพทย์ คำแนะนำ.....
2. ภาวะสุขภาพที่ต้องติดตาม.....

- แพทย์ผู้ตรวจ.....

2. ข้อมูลการส่งเสริมสุขภาพป้องกันโรค เริ่มให้บริการ 2 กลุ่ม เป้าหมายหลัก

- การฝากครรภ์
- การให้วัคซีนและติดตามพัฒนาการเด็กแรกเกิด จนถึงอายุ 6 ปี
  - ข้อมูลตรวจครั้งแรก (ดำเนินการครั้งเดียว)
  - LMP (กำหนดคลอด)
  - น้ำหนักครั้งแรก
  - ประวัติการได้รับวัคซีนบาดทะยัก
  - GPAL
  - ระดับความเสี่ยงของหญิงตั้งครรภ์
    - BMI
    - ประวัติพ่อแม่พี่น้องเป็นเบาหวาน
    - ตรวจน้ำตาลในปัสสาวะ
    - มีประวัติโรคเบาหวานขณะตั้งครรภ์
    - เคยคลอดบุตรที่มีน้ำหนักแรกเกิด มากกว่า 4,000 กรัม
    - ทารกเสียชีวิตในครรภ์ไม่ทราบสาเหตุ
    - โรคประจำตัว

- ผล Lab /คัดกรองก่อนการตั้งครรภ์
- ประวัติการคลอดครั้งที่แล้ว

- **ข้อมูลตรวจเพิ่มเติม (ดำเนินการทุกครั้งที่มา)**
  - อายุครรภ์ปัจจุบัน
  - ประวัติเด็กดิ้น (ดิ้น/ไม่ดิ้น)
  - น้ำหนักปัจจุบัน (แสดงแนวโน้ม)
  - ข้อมูลฉีดบาดทะยักในการฝากครรภ์ครั้งนี้
  - สรุปผลการตรวจร่างกายทั่วไป
    - ☐ ปกติ ☐ ผิดปกติ ระบุ.....
  - ข้อมูลความดันโลหิต (แสดงแนวโน้ม)
  - ขนาดของมดลูก (ซม.) (แสดงแนวโน้ม)
  - เสียงหัวใจเด็ก (จำนวนครั้ง)
  - ผลการตรวจอัลตร้าซาวด์
    - ☐ ปกติ ☐ ผิดปกติ ระบุ.....
  - ผล Lab เช่น น้ำตาลและอัลบูมินในปัสสาวะ
    - ☐ ปกติ ☐ ผิดปกติ ระบุ.....
  - ผลตรวจสุขภาพช่องปาก
    - ☐ ปกติ ☐ ผิดปกติ ระบุ.....

- **ข้อมูลตรวจครั้งแรก (ดำเนินการครั้งเดียว)**
    - วันเกิด
    - อายุครรภ์ตอนคลอด
    - ผลการตรวจ Lab เมื่อแรกเกิด เช่น TSH,
    - ธาลัสซีเมีย
- **ข้อมูลตรวจเพิ่มเติม (ดำเนินการทุกครั้งที่มา)**
    - ภาวะโภชนาการเด็ก (ส่วนสูง น้ำหนัก)
    - อายุเด็กปัจจุบัน
    - การได้รับวัคซีน
    - พัฒนาการเด็ก
        - ผลคัดกรองโดยเจ้าหน้าที่สาธารณสุข (4 ช่วงวัย : 9, 18, 30, 42 เดือน)
    - พัฒนาการตามคลินิกเด็กดี
        - สรุปแต่ละช่วงผลพัฒนาการเด็ก
        - (สมวัย/สงสัยล่าช้า)
        - วัดเส้นรอบศีรษะเด็ก (แสดงแนวโน้ม)
    - ข้อมูลทันตกรรม
        - (ฟันขึ้น ฟันที่ผุ หรือถอน ฟันหลุด อนามัยช่องปาก เคลือบฟลูออไรด์)

3. **ข้อมูลการรักษาพยาบาล**

- วันและเวลาที่รับบริการ
- สิทธิการรักษา
- ชื่อสถานพยาบาล
- เลข 13 หลัก

- HN/AN
- น้ำหนัก ส่วนสูง BMI
- ผลการซักประวัติ (Medical History)
    - อาการสำคัญ
    - ประวัติปัจจุบัน
    - ประวัติเจ็บป่วยในอดีต
    - ประวัติครอบครัว
    - พฤติกรรมเสี่ยงต่อสุขภาพ เช่น สูบบุหรี่ ดื่มสุรา
- ผลการตรวจร่างกาย
    - ☐ ปกติ ☐ ผิดปกติ ระบุ.....
- ผล LAB
- ผลการตรวจเอ็กซเรย์
- คำวินิจฉัยโรค (ชื่อโรคห้ามใช้รหัส ICD-10)
- การรักษา เช่น รายละเอียดยาที่ได้รับ การทำผ่าตัดหรือหัตถการ
- การติดตามผลการรักษา (วันที่นัดครั้งต่อไป)
- คำแนะนำ
- แพทย์/พยาบาล ผู้ให้การรักษา.....

ภาคผนวก ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๓๒ มาตรา ๓๓ และมาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่บทบัญญัติในหมวด ๒ หมวด ๓ หมวด ๕ หมวด ๖ หมวด ๗ และความในมาตรา ๙๕ และมาตรา ๙๖ ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(๑) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(๒) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(๔) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(๕) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(๖) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (๒) (๓) (๔) (๕) และ (๖) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

มาตรา ๕ พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(๑) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(๒) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

มาตรา ๖ ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

"บุคคล" หมายความว่า บุคคลธรรมดา

"คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"สำนักงาน" หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"เลขาธิการ" หมายความว่า เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๗ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้

หมวด ๑
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๘ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(๑) ประธานกรรมการ ซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(๒) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ

(๓) กรรมการโดยตำแหน่ง จำนวนห้าคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และอัยการสูงสุด

(๔) กรรมการผู้ทรงคุณวุฒิ จำนวนเก้าคน ซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ประธานอนุกรรมการ อนุกรรมการ ประธานกรรมการผู้เชี่ยวชาญ และกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนดโดยความเห็นชอบของกระทรวงการคลัง

มาตรา ๑๘ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการ ให้นำความในมาตรา ๑๔ และมาตรา ๑๕ มาใช้บังคับโดยอนุโลม

หมวด ๒
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑
บททั่วไป

มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้

มาตรา ๒๐ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา ๒๗ แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ดำเนินการ ดังต่อไปนี้

(๑) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา ๒๒ มาตรา ๒๓ หรือมาตรา ๒๔ แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

(๒) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

ให้นำความในวรรคหนึ่ง วรรคสอง และวรรคสาม มาใช้บังคับกับการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล และการอื่นใดตามพระราชบัญญัตินี้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ โดยอนุโลม

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา ๒๑ และการแจ้งรายละเอียดตามมาตรา ๒๓ มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

(๑) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๓) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา ๒๓ ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

ประวัติผู้วิจัย

ชื่อ-สกุล	กิจจา ทรงความเจริญ
วัน เดือน ปี เกิด	28 พฤศจิกายน 2523
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	น.บ. มหาวิทยาลัยราชภัฏเชียงราย เชียงราย
ที่อยู่ปัจจุบัน	20 ม. 8 ต.ดอนศรีชุม อ.ดอกคำใต้ จ.พะเยา
ผลงานตีพิมพ์	กิจจา ทรงความเจริญ (ผู้บรรยาย) (24-25 มกราคม 2562). มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้มารับบริการในโรงพยาบาล: ศึกษากรณีการจัดเก็บข้อมูลในระบบระเบียนสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล. Legal Measures for Personal Data Protection of The Hospital Service Recipients: A study of an Electronic Personal Health Record Application. ใน การประชุมวิชาการพะเยาวิจัยครั้งที่ 8 (หน้า 2256-2272): พะเยา. กองบริหารงานวิจัยและประกันคุณภาพการศึกษามหาวิทยาลัยพะเยา.
รางวัลที่ได้รับ	-