บทความวิชาการ

ปัญหาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐ*

ISSUES IN THE ENFORCEMENT OF PERSONAL DATA PROTECTION LAWS IN PUBLIC HOSPITALS

ศิริกร สีสดดี

Sirikron Seesonddee

กระทรวงสาธารณสุข สำนักงานสาธารณสุขจังหวัดฉะเชิงเทรา โรงพยาบาลพุทธโสธร ฉะเชิงเทรา ประเทศไทย

Ministry of Public Health, Chachoengsao Provincial Public Health Office,Buddhasothorn Hospital, Chachoengsao, Thailand

*Corresponding author E-mail: sirikron.kawfang@gmail.com

บทคัดย่อ

ปัจจุบันเทคโนโลยีที่เข้ามามีบทบาทต่อการเก็บรวบรวมข้อมูลส่วนบุคคล และการดำเนินงานในองค์กรภาครัฐ รัฐวิสาหกิจ และเอกชน โดยเฉพาะอย่างยิ่งในโรงพยาบาลของรัฐซึ่งเป็นหน่วยงานที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลด้านสุขภาพของผู้รับบริการ ที่ได้รับการคุ้มครองตามความในมาตรา 7 แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ซึ่งแต่เดิมหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลยังถูกกำหนดให้อยู่ภายใต้บังคับมาตรา 24 แห่งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 จนกระทั่งประเทศไทยได้ตระหนักถึงสิทธิแห่งความเป็นส่วนตัว (Right to Privacy) ในข้อมูลส่วนบุคคล อันเป็นสิทธิซึ่งได้รับการยอมรับในกฎหมายสิทธิมนุษยชนระหว่างประเทศโดยเฉพาะอย่างยิ่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) อีกทั้งยังเป็นสิทธิมนุษยชนขั้นพื้นฐานตามที่บัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 จึงได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาบังคับใช้ โดยมีวัตถุประสงค์เพื่อการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลที่หมายความรวมถึงข้อมูลส่วนบุคคลด้านสุขภาพอันเป็นข้อมูลที่มีความเกี่ยวข้องกับการรับบริการทางการแพทย์และการสาธารณสุขของบุคคลและสภาวะทางสุขภาพอนามัยของบุคคลเป็นสำคัญ จึงเป็นข้อมูลส่วนบุคคลเฉพาะตัวที่มีความละเอียดอ่อน ดังนั้นการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลโรงพยาบาลในกำกับของรัฐจึงเป็นหน่วยงานที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในขณะเดียวกันพบปัญหาที่เกิดขึ้นจากบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับโรงพยาบาลของรัฐทางปหอยู่หลายประการ ได้แก่ 1) ปัญหาการไม่มีบทนิยามความหมายของข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal data)" และ "ข้อมูลสุขภาพ" ที่ชัดเจนนำมาสู่ปัญหาการตีความกฎหมาย 2) ปัญหาการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลซึ่งยังไม่มีหลักเกณฑ์ที่ใช้ในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 3) ปัญหาการกำหนดอำนาจหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการประเมินความเสี่ยงของผลกระทบจากการประมวลผลข้อมูล และ 4) ปัญหาเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ไม่ได้กำหนดให้มีการบันทึกรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลไว้เป็นหลักฐานส่งผลให้ยากต่อการตรวจสอบ

* Received 11 December 2024; Revised 10 March 2025; Accepted 20 March 2025

ซึ่งปัญหาดังกล่าวส่งผลกระทบโดยตรงต่อการปฏิบัติงานในโรงพยาบาลของรัฐซึ่งหากปราศจากมาตรการทางกฎหมายที่มีความรัดกุมอาจนำไปสู่การเกิดเหตุการณ์ไม่พึงประสงค์เกี่ยวกับข้อมูลส่วนบุคคลของผู้รับบริการในโรงพยาบาลของรัฐได้ จึงเป็นการสมควรแก้ไขเพิ่มพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดย 1) กำหนดนิยามความหมายของข้อมูลส่วนบุคคลที่อ่อนไหว และข้อมูลด้านสุขภาพให้ชัดเจน 2) กำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานเดียวกัน 3) กำหนดเพิ่มเติมให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการประเมินผลกระทบของความเสี่ยงก่อนการประมวลผลข้อมูลเพื่อประโยชน์ของการจัดการและวางแผนในกระบวนการคุ้มครองข้อมูลส่วนบุคคล และ 4) กำหนดให้มีแนวปฏิบัติในการบันทึกรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลไว้เป็นหลักฐานที่สามารถตรวจสอบได้เพื่อประโยชน์ในการแสวงหาพยานหลักฐานอันเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล และกระบวนการตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

คำสำคัญ: การคุ้มครองข้อมูลส่วนบุคคล, เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล, การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

Abstract

At present, technology plays a significant role in the collection of personal data and the operations of government agencies, state enterprises, and private organizations. This is particularly evident in public hospitals, which handle personal health data of service recipients, a category of data protected under Section 7 of the National Health Act B.E. 2550 (2007). Previously, the principles governing personal data protection were subject to Section 24 of the Official Information Act B.E. 2540 (1997). Until Thailand recognized the right to privacy in personal data — a right acknowledged under international human rights law, particularly the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), and further enshrined as a fundamental human right in the Constitution of the Kingdom of Thailand B.E. 2560 (2017)— the country enacted the Personal Data Protection Act B.E. 2562 (2019).This law aims to safeguard personal data rights, which encompass personal health data, as such data pertains to individuals' medical and public health services as well as their health conditions. Given its sensitive nature, personal health data requires strict protection. Consequently, public hospitals, as state-supervised institutions handling personal data, must comply with the Personal Data Protection Act B.E. 2562 (2019).

Nonetheless, various issues have arisen in the enforcement of the Personal Data Protection Act B.E. 2562 (2019) in public hospitals. These issues include: 1) the absence of clear definitions for "sensitive personal data" and "health data," leading to difficulties in legal interpretation; 2) the lack of established criteria for appointing Data Protection Officers; 3) ambiguity regarding the

authority and responsibilities of Data Protection Officers in assessing risks associated with data processing; and 4) deficiencies in personal data breach notification requirements, as the law does not mandate the recording of details related to data breaches, thereby complicating the verification process. These issues directly impact the operations of public hospitals. Without stringent legal measures, undesirable incidents involving patients' personal data could arise. Therefore, amendments to the Personal Data Protection Act B.E. 2562 (2019) are warranted to: 1) clearly define the terms “sensitive personal data” and “health data”; 2) establish uniform qualifications for Data Protection Officers; 3) assign Data Protection Officers the duty to assess risk impacts before processing data, ensuring effective management and planning in personal data protection processes; and 4) require the documentation of personal data breaches in a verifiable manner to facilitate the collection of evidence related to breaches and the legal compliance audit process.

Keywords: Personal Data Protection, Data Protection Officer, Data Breach Notification, Personal Data Protection Act

บทนำ

ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนเอาไว้เป็นประการสำคัญ เนื่องจากในประเทศที่ปกครองในรูปแบบประชาธิปไตยมองว่า สิทธิเสรีภาพ และความเสมอภาคเปรียบเสมือนเกียรติยศและศักดิ์ศรีของความเป็นมนุษย์ (รัฐธรรมนูญแห่งราชอาณาจักรไทย, 2560) จึงกำหนดให้ประชาชนมีเสรีภาพในข้อมูลส่วนบุคคลของตนเอง หรือที่เรียกว่าสิทธิแห่งความเป็นส่วนตัว (Right of Privacy) ที่หมายความรวมถึงการคุ้มครองสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลของผู้เป็นเจ้าของข้อมูลโดยบุคคลอื่นจะละเมิดไม่ได้ (บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม, 2558) สิทธิดังกล่าวเป็นรากฐานสำคัญของแนวความคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการยอมรับในกฎหมายสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะอย่างยิ่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) (จุมพต สายสุนทร, 2550) ประเทศไทยจึงได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาบังคับใช้เพื่อการคุ้มครองข้อมูลส่วนบุคคลของประชาชน ซึ่งการยกร่างกฎหมายดังกล่าวได้รับอิทธิพลมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR)

โดยสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลนั้นมีความสัมพันธ์กับบทบาทและภารกิจการเข้ารับบริการทางการแพทย์ และการสาธารณสุขของโรงพยาบาลของรัฐ กล่าวคือ เมื่อผู้รับบริการก้าวเข้าสู่การใช้บริการที่โรงพยาบาลของรัฐปราการด่านแรกที่ต้องพบเจอ คือ แผนกเวชระเบียน ซึ่งมีหน้าที่เก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญของผู้เข้ารับบริการคลอบคลุม ทั้งชื่อ ที่อยู่ เลขประจำตัวประชาชน ข้อมูลเพศ หมู่โลหิต วันเดือนปีเกิด อายุ

ข้อมูลเกี่ยวกับสุขภาพอนามัย ประวัติการรักษา ประวัติการใช้ยา รวมถึงข้อมูลส่วนบุคคลดังกล่าวข้างต้นของบุคลากรภายในองค์กรถือเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของโรงพยาบาลด้วยเช่นกัน ภารกิจของโรงพยาบาลจึงมีความสัมพันธ์กับข้อมูลส่วนบุคคลโดยตรง (ชาติชาย มิตรกูล, 2558) จึงอาจกล่าวได้ว่าโรงพยาบาลนับว่าเป็นศูนย์กลางของข้อมูลขนาดใหญ่ที่เก็บรวบรวมข้อมูลส่วนบุคคลของผู้ป่วยที่เข้ามารับบริการไว้จำนวนมาก และเป็นองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลแทบจะทุกช่วงเวลาที่เป็นวงจรของชีวิตมนุษย์ตั้งแต่การเกิด การแก่ การเจ็บป่วย หรือแม้แต่กระทั่งการเสียชีวิต (แสวง บุญเฉลิมวิภาส, 2554) ส่งผลให้กิจกรรมการเก็บรวบรวม การประมวลผล และการใช้ข้อมูลส่วนบุคคล ภายในโรงพยาบาลย่อมเกิดขึ้นทุกวันอย่างหลีกเลี่ยงไม่ได้ แต่เดิมโรงพยาบาลของรัฐมีหลักเกณฑ์คุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดไว้ในพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ประกอบกับการดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคลของหน่วยงานราชการต้องเป็นไปตามหลักเกณฑ์ที่พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 โดยกำหนดห้ามหน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารส่วนบุคคล หรือข้อมูลข่าวสารราชการที่อยู่ในความควบคุมให้แก่หน่วยงาน หรือบุคคลอื่น โดยที่เจ้าของข้อมูลไม่ยินยอม เว้นแต่เป็นการเปิดเผยข้อมูลซึ่งจำเป็น หรือระงับอันตรายต่อชีวิต หรือสุขภาพของบุคคล จนกระทั่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ และกำหนดหลักเกณฑ์ กลไก อำนาจหน้าที่ของผู้ที่เกี่ยวข้องมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลให้แก่องค์กรยึดถือปฏิบัติ

สำหรับประเทศไทยแม้ว่าหลักความเป็นส่วนตัวจะถูกพัฒนาขึ้นเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อการคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชน แต่ในทางปฏิบัติพบว่ายังมีปัญหาเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ส่งผลต่อการปฏิบัติงานเกี่ยวการคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐที่ส่งผลกระทบต่อการปฏิบัติหน้าที่ของบุคลากรจากหลายภารกิจ อาทิเช่น งานเวชระเบียน งานเวชสถิติ งานส่งเสริมสุขภาพและป้องกันโรคติดต่อ งานด้านชีวอนามัย งานด้านทรัพยากรบุคคล งานด้านการประมวลผลข้อมูลสารสนเทศทางการแพทย์ ดังต่อไปนี้

1) ปัญหาการไม่มีบทนิยามความหมายของ“ข้อมูลส่วนบุคคล” แต่ละประเภทให้ชัดเจน กล่าวคือ ในมาตรา 6 ไม่ได้นิยามความหมายของคำว่า “ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)” และ “ข้อมูลสุขภาพ” เอาไว้ โดยที่ภารกิจหลักของโรงพยาบาลของรัฐ คือ การให้บริการด้านการแพทย์และการสาธารณสุขมีความเกี่ยวข้องกับการเก็บรวบรวม การประมวลผล การใช้ และการเผยแพร่ข้อมูลส่วนบุคคลทั้งสองประเภทโดยตรง ซึ่งโดยหลักการประมวลผลข้อมูลดังกล่าวจะต้องได้รับความยินยอมจากเจ้าของข้อมูล แต่เมื่อกฎหมายไม่ได้กำหนดนิยามความหมายของข้อมูลข้างต้นไว้ การพิจารณาว่าข้อมูลส่วนบุคคลใดเป็นข้อมูลอ่อนไหว หรือ ข้อมูลสุขภาพ จึงก่อให้เกิดปัญหาการตีความกฎหมายที่ส่งผลกระทบโดยตรงต่อการกระทำใดๆ เกี่ยวกับข้อมูลส่วนบุคคล เช่น กรณีผู้ป่วยชายอายุ 19 ปี ประสบอุบัติเหตุหมดสติไม่สามารถให้ความยินยอมในการเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคลได้ โรงพยาบาลสามารถเก็บข้อมูลส่วนบุคคลของผู้ป่วยได้แม้จะเป็นข้อมูลส่วนบุคคลที่อ่อนไหวจึงมีประเด็นปัญหาเกิดขึ้นว่าแล้วข้อมูลใดบ้างที่โรงพยาบาลได้รับมาเป็นข้อมูลอ่อนไหวที่จะต้องให้การระมัดระวังเป็นพิเศษ เป็นต้น

2. ปัญหาเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 เนื่องจากโรงพยาบาลในกำกับของรัฐมีการดำเนินกิจกรรมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อ่อนไหวจำนวนมาก จึงต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ซึ่งในมาตรา 41 ไม่ได้กำหนดคุณสมบัติของผู้ที่จะได้รับการแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ และปัจจุบันยังไม่มีการประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับหลักเกณฑ์เกี่ยวกับคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานเจ้าหน้าที่ของโรงพยาบาลของรัฐ ที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลที่อาจเป็นเจ้าหน้าที่จากหน่วยงานภายในที่มีหน้าที่เกี่ยวกับการประมวลผลข้อมูล อาทิเช่น เจ้าหน้าที่เวชสถิติ เจ้าหน้าที่ข้อมูลสารสนเทศ เป็นต้น หรืออาจเป็นผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล อาจเป็นกรณีที่โรงพยาบาลของรัฐได้ดำเนินการทำสัญญาว่าจ้างบุคคล หรือนิติบุคคล มาดำเนินการประมวลผลข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ตามวิธีการที่กำหนดไว้ในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 (พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ, 2560)จึงเป็นอุปสรรคต่อปฏิบัติราชการว่าโรงพยาบาลของรัฐในฐานะควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้จะใช้หลักเกณฑ์ใดในการแต่งตั้งบุคคลมาปฏิบัติหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3. ปัญหาเกี่ยวกับอำนาจหน้าที่ของผู้คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 42 ที่กฎหมายไม่ได้กำหนด ถึงหน้าที่ในการประเมินผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกระบวนการสำคัญที่มีส่วนช่วยให้โรงพยาบาลของรัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลสามารถจัดลำดับความสำคัญ จำกัดขอบเขตของความเสี่ยงที่มีอยู่ในกระบวนการคุ้มครองข้อมูลส่วนบุคคล และช่วยให้สามารถวางแผนวิธีการที่เลือกใช้ในประมวลผลข้อมูล หรือกำหนดมาตรการเพิ่มเติมเพื่อป้องกันเหตุไม่พึงประสงค์ต่าง ๆ ที่จะเกิดขึ้นในกระบวนการคุ้มครองข้อมูลส่วนบุคคลได้ เช่น ในกรณีระบบคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลเกิดขัดข้องโดยไม่ทราบสาเหตุ แต่โรงพยาบาลได้มีการวิเคราะห์ความเสี่ยงที่จะเกิดเหตุดังกล่าวจึงได้ดำเนินจัดหาระบบจัดเก็บข้อมูลที่สามารถตรวจสอบ ติดตามการวิเคราะห์ และการเฝ้าระวังครือข่ายเพื่อเพิ่มประสิทธิภาพของมาตรการในการดูแลความปลอดภัยของระบบเครือข่ายข้อมูลส่วนบุคคลภายในหน่วยงาน เป็นต้น

4. ปัญหาเกี่ยวการแจ้งเหตุข้อมูลส่วนบุคคลถูกละเมิดตามมาตรา 37 (4) ที่ไม่ได้กำหนดให้บันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูล รวมทั้งผลกระทบและการเยียวยาที่ได้ดำเนินการไว้เป็นหลักฐาน ส่งผลให้ยากต่อการตรวจสอบ และแสวงหาพยานหลักฐานในกรณีที่มีเหตุละเมิดข้อมูลส่วนบุคคลที่โรงพยาบาลของรัฐเป็นผู้ความควบคุมข้อมูลส่วนบุคคล ทำให้หน่วยงานที่มีหน้าที่ตรวจสอบ และบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตรวจสอบการปฏิบัติหน้าที่ตามกฎหมายของผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลได้ยากขึ้น เช่น กรณีเมื่อเดือนกันยายน พ.ศ. 2564 ได้เกิดเหตุการณ์ข้อมูลของผู้ป่วยที่มีอยู่ในกระทรวงสาธารณสุขจำนวนประมาณ 16 ล้านรายการ ประกอบด้วย ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขโทรศัพท์ ที่อยู่ รวมถึงชื่อแพทย์เจ้าของไข้ รหัสเข้าใช้ระบบโรงพยาบาล ถูกแฮกเกอร์เข้าถึงข้อมูลและนำไปจำหน่าย ผ่านเว็บบอร์ด และกล่าวอ้างว่านำมาจากระบบของกระทรวงสาธารณสุขประเทศไทย (พบประกาศขายข้อมูลคนไข้ของ สธ. ล่าสุดลิงค์หายไปแล้ว, 2564) เป็นต้น

ปัญหาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้นกับโรงพยาบาลของรัฐดังกล่าวข้างต้น ล้วนเป็นอุปสรรคต่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล การผลักดันให้กฎหมายเกิดความชัดเจนจะสามารถนำมาบังคับใช้กับการจัดการข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐได้อย่างมีธรรมาภิบาล และสอดคล้องกับภารกิจด้านการแพทย์และการสาธารณสุขอย่างยั่งยืนต่อไป

ขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐ

ในการดำเนินงานเกี่ยวกับข้อมูลข่าวสารต่าง ๆ รวมถึงข้อมูลส่วนบุคคลของโรงพยาบาลในกำกับของรัฐนั้นอยู่ภายใต้บังคับแห่งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ซึ่งเป็นกฎหมายบังคับใช้กับหน่วยงานราชการเพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชนที่ให้อำนาจหน่วยงานราชการในการที่จะสามารถเปิดเผยข้อมูลข่าวสาร และข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานต่อสาธารณะได้ โดยอยู่ภายใต้หลักความยินยอม หลักความจำเป็น และหลักประโยชน์สาธารณะ กล่าวคือ ในมาตรา 24 (7) หน่วยงานของรัฐจะเปิดเผยข้อมูลสุขภาพส่วนบุคคลไม่ได้ หากไม่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล โดยที่กฎหมายได้กำหนดข้อยกเว้นหากเป็นกรณีเพื่อความจำเป็นในการป้องกัน หรือระงับอันตรายต่อชีวิต หรือสุขภาพของบุคคล เช่น กรณีกระทรวงสาธารณสุขสั่งการให้โรงพยาบาลในสังกัดทั่วประเทศรายงานการสอบสวนโรคติดเชื้อไวรัสโคโรนา (COVID-19) ซึ่งมีข้อมูลที่มีรายละเอียดเกี่ยวกับชื่อ สกุล เพศ อายุ เลขประจำตัวประชาชน ผลการตรวจทางห้องปฏิบัติการ ประวัติการให้ยา การรักษาที่ได้รับ เพื่อวางแผนกำหนดมาตรการควบคุมการแพร่กระจายของโรค หรือในกรณีที่แพทย์เวรมีการส่งต่อรายละเอียดการรักษาพยาบาลผู้ป่วยซึ่งมีข้อมูลที่ประกอบด้วยชื่อ สกุล เพศ อายุ รสนิยมทางเพศ เพื่อให้การรักษาและป้องกันการติดเชื้อรุนแรงจากการมีเพศสัมพันธ์ เป็นต้น ทั้งนี้หากโรงพยาบาลของรัฐเห็นว่ารายงานการแพทย์ หรือข้อมูลข่าวสารส่วนบุคคลซึ่งจะเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควรอาจใช้อำนาจในการไม่เปิดเผยข้อมูลนั้นตามมาตรา 15 (5) แห่งพระราชบัญญัติดังกล่าวได้ มาตรา 15 (5) แห่งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (พระราชบัญญัติข้อมูลข่าวสารของทางราชการ, 2540) ดังเช่นกรณีโรงพยาบาลส่งรายงานผลการตรวจสุขภาพของพนักงานไปยังหน่วยงานต้นสังกัดที่มีข้อมูลระบุว่า มีพนักงานใช้สารเสพติดจำนวน 5 คน หน่วยงานต้นสังกัดจึงยื่นคำร้องขอให้โรงพยาบาลเปิดเผยข้อมูลเพื่อจะได้ทราบว่าเป็นบุคคลใด โรงพยาบาลสามารถปฏิเสธคำร้องขอนั้นได้

เมื่อประเทศไทยมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เข้ามากำหนดมาตรการเพื่อคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัย โดยมีหลักการที่สำคัญ คือ หลักการจัดเก็บข้อมูลและประมวลผลเท่าที่จำเป็น (Data Minimization) หลักความปลอดภัยของข้อมูล (Data Security) และหลักความชอบด้วยกฎหมาย (Lawful Basis for Processing) (Guidelines on the Protection of Privacy and Trans border Data Flows of Personal Data part 2, Article 7-14) ซึ่งหลักการคุ้มครองข้อมูลส่วนบุคคลที่ปรากฏอยู่ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยยอิทธิพลมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) (คณาธิป ทองรวีวงศ์, 2564) ที่กำหนดให้มีผู้เกี่ยวข้องดังต่อไปนี้

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายความว่า บุคคลที่ข้อมูลส่วนบุคคลระบุไปถึง ซึ่งกฎหมายให้การรับรองและคุ้มครองสิทธิในข้อมูลส่วนบุคคล เจ้าของข้อมูลจึงต้องเป็นบุคคลธรรมดาเท่านั้น

ไม่รวมไปถึงนิติบุคคล เจ้าของข้อมูลส่วนบุคคลอาจจะเป็นเจ้าหน้าที่ของโรงพยาบาล หรือ คนไข้ ที่เข้ามารับบริการที่โรงพยาบาลก็ได้ จึงสรุปได้ว่าบุคคลทุกคนสามารถเป็นเจ้าของข้อมูลส่วนบุคคลได้โดยไม่จำกัดสถานะทางกฎหมายที่มีสิทธิในการที่จะปกป้องข้อมูลส่วนบุคคลของตนเอง ดังนั้นการกระทำใด ๆ เกี่ยวข้องกับการเก็บข้อมูลส่วนบุคคล ประมวลผลข้อมูลส่วนบุคคล หรือเผยแพร่ข้อมูลส่วนบุคคลจำเป็นต้องได้รับคำยินยอม (Consent) จากเจ้าของข้อมูลก่อนเริ่มดำเนินการ แต่อย่างไรก็ตามกฎหมายได้ยกเว้นกรณีที่ไม่ต้องขอคำยินยอมตามกฎหมาย ได้แก่ การประมวลข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะด้านการสาธารณสุขจากโรคติดต่ออันตรายซึ่งแพร่กระจายอย่างรวดเร็วที่ส่งผลกระทบต่อสภาวะสุขภาพของประชาชน ทั้งนี้ในการประมวลผลข้อมูลส่วนบุคคลจะต้องพิจารณาจากฐานทางกฎหมายอื่นที่รองรับประกอบฐานความยินยอมด้วย เช่น ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest) ฐานภารกิจของรัฐ (Public Task) ฐานสัญญา (Contract) ฐานจดหมายเหตุวิจัยหรือสถิติ (Historical Document, Research, or Statistics) เป็นต้น (สำนักอำนวยการ สถาบันวิจัยและพัฒนาพื้นที่สูง (กลุ่มงานนิติการ สำนักอำนวยการ, 2565)

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายความว่า ผู้มีอำนาจตัดสินใจเกี่ยวกับกระบวนการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การเก็บข้อมูล ประมวลผลข้อมูล ไปจนถึงการเปิดเผยข้อมูล โดยอาจเป็นบุคคลหรือนิติบุคคลก็ได้ และมีหน้าที่กำหนดมาตรการความปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคล ตรวจสอบการลบ หรือทำลายข้อมูลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา บันทึกรายการ เมื่อมีการเก็บรวบรวม การใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงาน และเจ้าของข้อมูลส่วนบุคคลทราบในกรณีมีความเสี่ยงสูงที่จะกระทบต่อสิทธิเสรีภาพ พร้อมกับแนวทางการเยียวยา มาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) ตามแนวทางการแจ้งเหตุละเมิดที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด (ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565) อย่างไรก็ตามเมื่อพิจารณาบริบทโรงพยาบาลของรัฐที่มีการแบ่งแยกส่วนราชการออกจากสำนักงานปลัดกระทรวงสาธารณสุข และมีการแบ่งแยกโครงสร้างการปฏิบัติราชการของโรงพยาบาลเป็นส่วนงานย่อยที่มีหน้าที่ตามภารกิจแตกต่างกันออกไป เช่น กลุ่มงานเวชระเบียน กลุ่มงานการพยาบาล กลุ่มงานการเงิน กลุ่มงานสารสนเทศทางการแพทย์ กลุ่มงานนิติเวช กลุ่มงานจิตเวช เป็นต้น โดยมีข้าราชการ พนักงานราชการ หรือลูกจ้างที่ปฏิบัติงานตามตำแหน่งหน้าที่ในส่วนงานย่อยต่างๆ แต่ทั้งโรงพยาบาลของรัฐ และส่วนงานย่อยภายในโรงพยาบาลของรัฐไม่ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีสถานะเพียงเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล คือ สำนักงานปลัดกระทรวงสาธารณสุขเท่านั้น ดังนั้นผู้ควบคุมข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐจึงหมายถึงสำนักงานปลัดกระทรวงสาธารณสุข

การที่โรงพยาบาลของรัฐไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลโดยตรงจึงไม่มีอำนาจตัดสินใจเกี่ยวกับกระบวนการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การเก็บข้อมูล ประมวลผลข้อมูล ไปจนถึงการเปิดเผยข้อมูลได้โดยลำพังแต่ต้องได้รับความเห็นชอบจากสำนักงานปลัดกระทรวงสาธารณสุข หรือหัวหน้าส่วนราชการในราชการบริหารส่วนภูมิภาคที่ได้รับมอบอำนาจ เช่น โรงพยาบาลประจำจังหวัดเป็นราชการบริหารส่วนภูมิภาค มีสำนักงานสาธารณสุขจังหวัดเป็นหน่วยงานที่กำกับดูแลการปฏิบัติราชการ ซึ่งอยู่ภายใต้การควบคุม กำกับ

ติดตาม การปฏิบัติราชการของผู้ว่าราชการจังหวัดที่ได้รับมอบอำนาจจากปลัดกระทรวงสาธารณสุขให้ปฏิบัติราชการแทน การดำเนินการตามแบบแผนของทางราชการดังกล่าวมีขั้นตอนที่ยุ่งยากซับซ้อนต้องผ่านประบวนการกลั่นกรองงานที่เสนอไปหลายขั้นตอน และค่อนข้างใช้ระยะเวลานาน ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคลในเรื่องที่โรงพยาบาลได้ขอความเห็นชอบไม่สามารถดำเนินการได้ทันที บางกรณีอาจล้าหลังกว่าการเปลี่ยนแปลงของสภาพสังคมในปัจจุบัน (สำนักงานปลัดกระทรวงสาธารณสุข หนังสือที่ สธ 0202.3.6/ว1915, 2563)

ดังที่ได้กล่าวมาข้างต้นกระบวนการคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐมีความแตกต่างไปจากโรงพยาบาลเอกชน กล่าวคือ โรงพยาบาลเอกชนดำเนินการภายใต้บุคคลหรือหลายบุคคลร่วมกันจัดตั้งโรงพยาบาล ในขณะที่โรงพยาบาลรัฐดำเนินการภายใต้กระทรวงสาธารณสุขโดยงบประมาณของรัฐบาล โรงพยาบาลเอกชนจึงเป็นผู้คุ้มครองข้อมูลส่วนบุคคลได้ด้วยตนเอง จึงมีอำนาจตัดสินใจ วางแผนในการเก็บรวบรวม ประมวลผล ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้รับบริการที่อยู่ในความควบคุมของตนเองได้ ทั้งนี้โดยต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายความว่า ผู้ดำเนินการเกี่ยวกับกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลหรือผู้แทน ซึ่งอาจเป็นบุคคล หรือนิติบุคคลก็ได้ มีหน้าที่ปฏิบัติตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูล กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมสำหรับการประมวลผลข้อมูล รวมทั้งแจ้งเหตุข้อมูลส่วนบุคคลถูกละเมิดต่อผู้ควบคุมข้อมูลทราบ จัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูล (Record of Processing Activity) มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) ดังนั้นโรงพยาบาลของรัฐจึงมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามคำสั่ง หรือ นโยบาย มาตรการรักษาความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงสาธารณสุขที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล เช่น กระทรวงสาธารณสุขกำหนดมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลโดยกำหนดแบบฟอร์มที่เป็นมาตรฐานสำหรับใช้ในการยื่นคำร้องขอประวัติการรักษาพยาบาล และแบบฟอร์มการยินยอม และแบบยกเลิกความยินยอมในการเปิดเผยข้อมูลส่วนบุคคล โรงพยาบาลจึงต้องนำแบบฟอร์มดังกล่าวมาใช้เพื่อให้เป็นไปตามมาตรฐานความปลอดภัย เป็นต้น

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หมายความว่า ผู้มีหน้าที่ให้คำแนะนำตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูล ประสานงานและให้ความร่วมมือกับสำนักงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รักษาความลับของข้อมูล มาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) โดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายในหน่วยงานหากเข้าในกรณีใดดังต่อไปนี้

1) กรณีที่เป็นหน่วยงานของรัฐ (มาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

2) มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่มีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคล หรือระบบอย่างสม่ำเสมอเนื่องจากมีข้อมูลส่วนบุคคลเป็นจำนวนมาก

3) มีภารกิจหลักที่ต้องดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) (ข้อ 13.1 บัญชีแนบท้าย ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้

ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566)

โดยที่ภารกิจหลักของโรงพยาบาลรัฐมีการประมวลผลข้อมูลด้านสุขภาพซึ่งเป็นข้อมูลที่ความอ่อนไหวจึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด สำนักงานปลัดกระทรวงสาธารณสุขจึงดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (คำสั่งสำนักงานปลัดกระทรวงสาธารณสุข ที่ 1189/2565 ลงวันที่ 25 พฤษภาคม 2565 เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล) ดังนั้น ผู้ที่ได้รับแต่งตั้งจึงมีฐานะเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ทั้งนี้ ในราชการส่วนภูมิภาค ได้มีการมอบหมายให้เลขานุการคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ ระดับจังหวัดทุกจังหวัดปฏิบัติหน้าที่เจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด (คำสั่งสำนักงานปลัดกระทรวงสาธารณสุข ที่ 1480/2565, 2565) แต่ในระดับโรงพยาบาลเมื่อกฎหมายไม่ได้กำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกฎหมายเอาไว้ จึงเป็นปัญหาในทางปฏิบัติว่าบุคคลใดเหมาะสมที่จะได้รับการแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ดังนั้นเมื่อพิจารณาบทบาทหน้าที่ของโรงพยาบาลในกำกับของรัฐตามโครงสร้างขององค์กร และหน้าที่ของผู้ที่เกี่ยวข้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการเก็บ รวบรวม ใช้ ประมวลผล และเปิดเผยข้อส่วนบุคคล ตลอดจนมีการใช้ และประมวลผลข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ข้อมูลเกี่ยวกับสุขภาพอยู่เป็นประจำอย่างหลีกเลี่ยงไม่ได้ บริบทของโรงพยาบาลจึงถือว่าเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หน่วยงานประกันสังคม หรือบริษัทประกัน หรือบริษัทที่โรงพยาบาลได้มีสัญญาว่าจ้างให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล คือ ผู้ประมวลผลข้อมูล (Data Processor) และในกรณีที่มีการส่งตัวผู้ป่วยไปรับการรักษาต่อและต้องมีการส่งข้อมูลระหว่างโรงพยาบาล โรงพยาบาลแรกที่รับเคสผู้ป่วยถือเป็นผู้ควบคุมข้อมูล (Data Controller) ส่วนโรงพยาบาลที่รับเคสส่งต่อผู้ป่วยถือเป็นผู้ประมวลผลข้อมูล (Data Processor) ซึ่งมีหน้าที่ต้องปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายเช่นเดียวกัน

อย่างไรก็ตามการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องพิจารณาร่วมกับพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ในการที่โรงพยาบาลของรัฐจะปฏิบัติ หรือดำเนินการใดๆเกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามมาตรการของการคุ้มครองข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายอย่างมีประสิทธิภาพ และเมื่อพิจารณาขอบเขตของการคุ้มครองข้อมูลส่วนบุคคลจะเห็นได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมุ่งคุ้มครองบุคคลที่มีสิทธิและหน้าที่ตามของกฎหมายเท่านั้น (มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรา 15 แห่งประมวลกฎหมายแพ่งและพาณิชย์) แต่พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 มีขอบเขตการคุ้มครองไปถึงข้อมูลข่าวสารส่วนบุคคลของผู้ที่เสียชีวิตแล้ว (มาตรา 4 แห่งพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540) ในขณะที่พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 (พระราชบัญญัติสุขภาพแห่งชาติ, 2550) ได้กำหนดหลักเกณฑ์ความคุ้มครองไปถึงข้อมูลสุขภาพ ส่วนบุคคลให้เป็นความลับ (Right to Confidentiality) (Bundesministerium fur Gesundheit, 2024) แต่ยังไม่มีกฎหมายฉบับใดนิยามความหมายของข้อมูลสุขภาพ

และข้อมูลส่วนบุคคลที่อ่อนไหวเอาไว้ นำมาสู่ปัญหาที่เป็นอุปสรรคต่อการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐดังที่จะกล่าวถึงในหัวข้อถัดไป

ปัญหาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐ

1. ปัญหาการไม่มีบทนิยามความหมายของ “ข้อมูลส่วนบุคคลที่อ่อนไหว” และ “ข้อมูลสุขภาพ”

เมื่อพิจารณาถึงข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ข้อมูล ดังต่อไปนี้

1.1 ข้อมูลส่วนบุคคลทั่วไป (Personal Data) หมายถึง สิ่งที่สามารถระบุตัวบุคคลได้ไม่ว่าโดยตรงหรือ โดยอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่เสียชีวิตแล้ว (มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) เช่น ชื่อ นามสกุล ชื่อเล่น หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ ทะเบียนรถ ที่อยู่ ข้อมูลการศึกษา ข้อมูลสถานที่ปฏิบัติงาน เป็นต้น

ตัวอย่างเช่น นาย ก เป็นแพทย์ผู้เชี่ยวชาญด้านอายุรศาสตรโรคไตประจำโรงพยาบาล H พยาบาลคนนี้มีชื่อเล่นว่า B พักอยู่หอพักหลังโรงพยาบาล

นาย ข เป็นเจ้าของข้อมูลส่วนบุคคล ต่อมา นาย ข เสียชีวิต เช่นนี้ นาย ข จึงไม่ใช่เจ้าของข้อมูลส่วนบุคคล และข้อมูลของนาย ข ไม่ถือว่าเป็นข้อมูลส่วนบุคคล

1.2 ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data) หมายถึง ข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อการกระทบสิทธิของเจ้าของข้อมูล และเป็นเรื่องส่วนตัวโดยแท้ เช่น ข้อมูลเชื้อชาติ เผ่าพันธุ์ ข้อมูลสุขภาพ ความเชื่อ เพศวิถี ข้อมูลอาชญากรรม เป็นต้น (มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

ตัวอย่างเช่น รายงานผลตรวจทางห้องปฏิบัติการ

ข้อมูลเกี่ยวกับรสนิยมทางเพศ เช่น การเป็นเพศทางเลือก (LGBTQ) (American Nurses Association, 2018) การมีรสนิยมชอบความเจ็บปวด (Masochist) เป็นต้น (อลิซอน, แอล. และคณะ, 2544)

โดยมีคำแถลงการณ์ของแพทยสมาคมโลกว่าด้วยประเด็นจริยธรรมเกี่ยวกับฐานข้อมูลสุขภาพ ค.ศ. 2002 ได้ให้คำจำกัดความของข้อมูลสุขภาพ (Health Information) ว่าหมายถึง ข้อมูลที่แสดงถึงปัญหาและสภาวะทางด้านสุขภาพอนามัยของบุคคลที่สามารถระบุไปยังบุคคลได้ ไม่ว่าจะถูกบันทึกไว้ในรูปแบบใดก็ตาม (Lynskey, O., 2016) เมื่อพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. 2562 ไม่ได้ให้นิยามความหมาย ของข้อมูลสุขภาพ และข้อมูลที่อ่อนไหวเอาไว้ จึงต้องอาศัยการตีความทางกฎหมายส่งผลให้ในทางปฏิบัติเกิดความสับสนในการแยกประเภทของข้อมูลส่วนบุคคล และมีผลกระทบต่อการกำหนดมาตรการความปลอดภัยของข้อมูลที่เหมาะสม (Rubemfeld, J., 1989) อีกทั้งยังไม่สอดคล้องกับความเป็นสากลด้านการแพทย์และการสาธารณสุขอีกด้วย ซึ่งแตกต่างจากกฎหมายซึ่งเป็นต้นแบบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป (General Data Protection Regulation (GDPR)) ดังนี้

กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป (General Data Protection Regulation (GDPR)) ได้กำหนดให้ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data) เป็นข้อมูลประเภทพิเศษ (Article 9 of General Data Protection Regulation (GDPR)) และกำหนดความหมายของข้อมูลด้านสุขภาพของบุคคลไว้เป็นการเฉพาะพิเศษ (Article 4 (15) of General Data Protection Regulation (GDPR)) เพื่อไม่ให้เกิดปัญหาการตีความกฎหมาย โดยข้อมูลส่วนบุคคลที่ให้ความคุ้มครองมีดังนี้

1. “ข้อมูลส่วนบุคคล” (Personal Data) หมายถึง ข้อมูลสารสนเทศในรูปแบบใดก็ตามที่สามารถระบุตัวตนโดยอ้างอิงจากอัตลักษณ์เฉพาะตัวของบุคคลธรรมดา ไม่ว่าจะโดยตรง หรือโดยอ้อม (Article 4 (1) of General Data Protection Regulation (GDPR)) เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ภาพถ่าย ข้อมูลการเงิน เป็นต้น

2. “ข้อมูลส่วนบุคคลชนิดพิเศษ” หมายถึง ข้อมูลที่มีไว้เพื่อวัตถุประสงค์ในการระบุอัตลักษณ์ของบุคคลธรรมดาอย่างเฉพาะเจาะจง เช่น ข้อมูลที่เกี่ยวข้องกับสุขภาพ ข้อมูลเกี่ยวกับชีวิตทางเพศ หรือวิถีทางเพศ เชื้อชาติ ความเชื่อ เป็นต้น (Article 9 of General Data Protection Regulation (GDPR))

โดยได้กำหนดนิยามความหมายของข้อมูลสุขภาพ อันเกี่ยวข้องกับวงการแพทย์และการสาธารณสุขไว้เป็นการเฉพาะ ดังนี้

“ข้อมูลเกี่ยวกับสุขภาพ” หมายถึง ข้อมูลเกี่ยวกับสุขภาพกาย ข้อมูลสุขภาพจิต ข้อมูลเกี่ยวกับการจัดการบริการสาธารณสุขที่เปิดเผยข้อมูลเกี่ยวกับสถานะทางสุขภาพของบุคคลธรรมดา (Article 4 (15) of General Data Protection Regulation (GDPR)) เช่น รายงานผลการตรวจร่างกาย ประวัติการรักษาพยาบาล ข้อมูลการปรึกษาจิตแพทย์ หมู่โลหิต ประวัติการแพ้อาหาร เป็นต้น

2. ปัญหาการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ในประเด็นเรื่องของการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนี้นับว่าเป็นปัญหาที่สำคัญของกระบวนการคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐ กล่าวคือ แม้ว่าสำนักงานปลัดกระทรวงสาธารณสุขจะได้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในระดับจังหวัดแล้ว แต่ในระดับโรงพยาบาลยังประสบปัญหาในเรื่องของคุณสมบัติของผู้ที่เหมาะสมจะเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 41 ไม่ได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของผู้ที่จะได้รับแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเอาไว้ กำหนดเพียงว่าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) ซึ่ง ณ ปัจจุบันยังไม่มีการประกาศหลักเกณฑ์เกี่ยวกับการกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล นอกจากนี้รูปแบบ และจำนวนของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกฎหมายก็ไม่ได้กำหนดไว้เช่นกัน จึงเป็นปัญหาในการที่จะปฏิบัติราชการว่าโรงพยาบาลของรัฐในฐานะส่วนหนึ่งของควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้จะใช้หลักเกณฑ์ใดในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในระดับโรงพยาบาลเพื่อให้คำแนะนำกับเจ้าหน้าที่ผู้ปฏิบัติงาน เช่น งานด้านเวชระเบียน เวชสถิติ ศูนย์คอมพิวเตอร์ งานทรัพยากรบุคคล เป็นต้น

ตรวจสอบการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล และประสานงานกับหน่วยงานส่วนกลาง หรือ หน่วยงานระดับจังหวัดกรณีราชการส่วนภูมิภาค

ในเรื่องคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนี้กฎหมายไทยมีความแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป (General Data Protection Regulation (GDPR)) ที่มีการกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ใน มาตรา 37 วรรคห้าโดยคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลถูกกำหนดไว้ใน มาตรา 37 วรรคห้า ว่าเจ้าหน้าที่คุ้มครองอมูลส่วนบุคคลต้องพิจารณาจากคุณสมบัติทางวิชาชีพ และโดยเฉพาะอย่างยิ่งความรู้ความเชี่ยวชาญในกฎหมาย และการปฏิบัติการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงความสามารถในการปฏิบัติภารกิจตามที่กฎหมายกำหนด (Article 37 of General Data Protection Regulation (GDPR))

สาระสำคัญที่เหมือนกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย และสหภาพยุโรป คือ การกำหนดหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคล และการกำหนดหน้าที่ของผู้กำกับดูแล และประมวลผลข้อมูลส่วนบุคคล โดยแบ่งออกเป็น เจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล (Data Controller) ผู้ประมวลผลข้อมูล (Data Processor) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) ในกรณีที่กิจกรรมหลักของผู้ควบคุมหรือผู้ประมวลผลประกอบด้วยการประมวลผลขนาดใหญ่ของข้อมูลประเภทพิเศษ ตามมาตรา 9 และข้อมูลส่วนบุคคลที่เกี่ยวกับการตัดสินโทษและความผิดทางอาญา เช่น ข้อมูลสุขภาพ ข้อมูลประวัติอาชญากรรม เป็นต้น

นอกจากนี้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมีการกำหนดสิทธิแก่ที่ผู้เป็นเจ้าของข้อมูลส่วนบุคคลสามารถใช้หวงกันมิให้ผู้ควบคุมข้อมูล หรือ ผู้ประมวลผลข้อมูลเข้ามาแสวงหาประโยชน์จากข้อมูลของตนได้ และในกรณีที่ไม่ปฏิบัติตามกฎหมายมีบทลงโทษปรับในอัตราที่ค่อนข้างสูงเพื่อให้การบังคับใช้กฎหมายมีผลสัมฤทธิ์ผลเป็นรูปธรรมมากยิ่งขึ้น แต่บทลงโทษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยแบ่งเป็นความรับผิดทางแพ่ง ความรับผิดทางอาญา และความรับผิดทางปกครอง จะเห็นได้ว่าในเชิงเนื้อหากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยไม่ได้แตกต่างไปจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเนื่องจากยกร่างกฎหมายโดยอาศัยหลักการพื้นฐานเดียวกัน คือ การคุ้มครองความเป็นส่วนตัวให้สอดคล้องกับปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights (UDHR)) (จุมพต สายสุนทร, 2550, น. 227) เพื่อให้มนุษย์สามารถมีชีวิตอยู่ในสังคมได้อย่างเสรี เท่าเทียม และมีศักดิ์ศรี (Rubemfeld, 1989)

3. ปัญหาการกำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ปัญหาเกี่ยวกับอำนาจหน้าที่ของผู้คุ้มครองข้อมูลส่วนบุคคล ไม่ครอบคลุมเหมาะสมกับยุคแห่งเทคโนโลยีที่พัฒนาไปข้างหน้า แต่ในขณะเดียวกันก็มีผู้ใช้ประโยชน์จากเทคโนโลยีในการแสวงหาประโยชน์โดยมิชอบในรูปแบบต่าง ๆ จากข้อมูลส่วนบุคคลของผู้อื่น และหากปัญหาการละเมิดข้อมูลส่วนบุคคลนี้หากเกิดกับโรงพยาบาลของรัฐที่เก็บรวบรวม ใช้ ประมวลผลข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่อ่อนไหวง่ายจำนวนมาก ย่อมกระทบต่อสิทธิส่วนตัว เกียรติยศ ชื่อเสียงของเจ้าของข้อมูล และ เกิดความเสียหายอย่างมหาศาล ซึ่งเหตุการณ์ข้อมูลส่วนบุคคลถูกละเมิดนี้มีปรากฏให้เห็นทั้งในประเทศไทย ดังเช่น กรณีโรงพยาบาลสระบุรีถูกโจมตีด้วย Ransomware หรือไวรัสเรียกค่าไถ่ ทำให้ไม่สามารถเรียกดูข้อมูล ของผู้ป่วยในระบบของโรงพยาบาลได้ ส่งผลให้การดำเนินการล่าช้าและเกิดข้อมูลส่วนบุคคลรั่วไหล (รพ.สระบุรีโดนมัลแวร์เรียกค่าไถ่ ระบบคอมฯ พัง ต้องซักประวัติใหม่ทำล่าช้า,

2563) และในต่างประเทศ เช่น กรณีบริษัท Dedalus Biologie ที่ดำเนินการเกี่ยวกับโปรแกรมสำหรับห้องปฏิบัติการตรวจวิเคราะห์ทางการแพทย์ได้ทำข้อมูลส่วนตัวของผู้ป่วย และข้อมูลที่เกี่ยวกับสุขภาพ รั่วไหลสู่สาธารณชนสำนักงานที่กำกับดูแลเกี่ยวกับข้อมูลส่วนบุคคลของฝรั่งเศสจึงมีคำสั่งลงโทษปรับเป็นเงินจำนวน 1.5 ล้านยูโร (European Data Protection Board, 2022) เป็นต้น

การประเมินผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นกระบวนการที่ถูกกำหนดให้ต้องทราบผลกระทบ และ มาตรการที่เหมาะสมกับผลกระทบและความเสี่ยงเพื่อดำเนินการหามาตรการบรรเทาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้อย่างมีประสิทธิภาพที่มีส่วนช่วยให้ผู้ควบคุมข้อมูลสามารถจัดลำดับความสำคัญจำกัดขอบเขตของความเสี่ยงในกระบวนการคุ้มครองข้อมูลส่วนบุคคล และช่วยให้สามารถวางแผนเพื่อป้องกันเหตุละเมิดข้อมูล หรือเหตุข้อมูลรั่วไหลได้ โดยเฉพาะอย่างยิ่งในสังคมปัจจุบันข้อมูลส่วนบุคคลมีค่ามากเสียยิ่งกว่าทองคำ (ธัญญานุช ตันติกุล, 2560) ซึ่งในมาตรา 42 ไม่ได้กำหนดให้การประเมินผลกระทบหรือความเสี่ยงจากการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยตรง

ในขณะที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป (General Data Protection Regulation (GDPR)) ได้กำหนดหลักเกณฑ์เกี่ยวกับหน้าที่ในการประเมินความเสี่ยงจากการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้ประเมินความเสี่ยงต่อผลกระทบที่จะเกิดขึ้นกับข้อมูลส่วนบุคคลก่อนที่ผู้ควบคุมและผู้ประมวลผลจะเริ่มกิจกรรม และ กำหนดหลักเกณฑ์ในการประเมินความเสี่ยงเอาไว้อย่างชัดเจนปรากฏอยู่ในมาตรา 35 (7) (Article 35 (7) of General Data Protection Regulation (GDPR))

ตัวอย่าง การวิเคราะห์ความเสี่ยงและประเมินความรุนแรงและจัดลำดับความรุนแรงของเหตุการณ์

ตารางที่ 1 แสดงตัวอย่างการวิเคราะห์ความเสี่ยงและประเมินความรุนแรงของเหตุการณ์

สถานการณ์/ภาวะฉุกเฉิน	ระดับความรุนแรง (5 คะแนน)			จัดเรียงลำดับ		
	ระบบงาน	พันธกิจ	ประชาชน	รวม	จัดลำดับ	แผนป้องกัน
กรณีการบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยี สารสนเทศจากภายนอก เพื่อสร้างความเสียหาย หรือ ทำลายระบบข้อมูล	5	4	3	12	1	มี
กรณีไฟฟ้าดับ	5	3	2	10	2	มี
กรณีไวรัสคอมพิวเตอร์	5	2	3	9	3	มี

ในทัศนะของผู้เขียนมีความเห็นว่า การรู้เท่าทันเทคโนโลยีที่ใช้ในการประมวลผลข้อมูล และผลกระทบหรือความเสี่ยงที่จะเกิดขึ้นจากกระบวนการคุ้มครองข้อมูลส่วนบุคคลมีความสำคัญต่อการวางแผนกำหนดมาตรการความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง เมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการกำกับดูแลผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล จึงเปรียบเสมือนปราการด่านแรกในกระบวนการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด ดังนั้นจึงมีความจำเป็นต้องแก้ไขบทบัญญัติในมาตรา 42

โดยกำหนดเพิ่มเติมหน้าที่ของเจ้าหน้าที่ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการประเมินความเสี่ยง และผลกระทบจากการคุ้มครองข้อมูลส่วนบุคคลก่อนที่ผู้ควบคุม และผู้ประมวลผลจะเริ่มกิจกรรมเกี่ยวกับข้อมูลส่วนบุคคล

4. ปัญหาเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ปัญหาเกี่ยวการแจ้งเหตุข้อมูลส่วนบุคคลถูกละเมิดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยปรากฏอยู่ในมาตรา 37 (4) ให้เป็นหน้าที่ของผู้ควบคุมข้อมูล โดยหลักเกณฑ์วิธีการแจ้งและข้อยกเว้นให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด โดยต้องระบุสาระสำคัญเท่าที่จะสามารถกระทำได้ จะเห็นได้ว่ากฎหมายไม่ได้กำหนดว่าต้องบันทึกรายละเอียดเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นเป็นหลักฐานไว้ที่หน่วยงาน จึงเป็นอุปสรรคต่อการคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐ กล่าวคือ เมื่อมีเหตุร้องเรียน หรือฟ้องร้องเป็นคดีเกี่ยวกับความเสียหายจากผลกระทบของการละเมิดข้อมูลส่วนบุคคล เป็นการยากต่อการพิสูจน์หักล้างข้อกล่าวหา และในกรณีที่เจ้าหน้าที่ผู้ปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลมีส่วนในความเสียหาย เช่น กรณีเจ้าหน้าที่เวชระเบียนไม่ได้ใส่รหัสเพื่อล็อคหน้าจอป้องกันบุคคลอื่นเข้าใช้งานระบบข้อมูลผู้ป่วยนอกขณะพักรับประทานอาหาร เป็นเหตุให้มีบุคคลอื่นเข้าแก้ไขข้อมูลส่วนบุคคลของผู้ป่วยเกี่ยวกับประวัติการแพ้ยา กรณีเจ้าหน้าที่ศูนย์ข้อมูลสารสนเทศที่มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลส่งข้อมูลของผู้ป่วยไปยังศูนย์วิจัยโดยไม่ได้รับความยินยิมจากผู้ป่วย เป็นต้น จะเกิดผลกระทบโดยตรงต่อการกำหนดขอบเขตและแนวทางการสอบสวนทางวินัย และการกำหนดสัดส่วนความรับผิดทางละเมิด

ในขณะที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป (General Data Protection Regulation (GDPR)) มาตรา 33 วางหลักเกณฑ์ให้ผู้ควบคุมข้อมูลต้องบันทึกรายละเอียดเกี่ยวกับการละเมิดรวมทั้งผลกระทบและการเยียวยาที่ได้ดำเนินการ ไว้เป็นหลักฐานเพื่อให้หน่วยงานที่บังคับใช้กฎหมายสามารถตรวจสอบการปฏิบัติหน้าที่ตามกฎหมายได้

ผู้เขียนมีความเห็นว่า เนื่องจากกระบวนการบันทึกหลักฐานและการจัดเก็บหลักฐานรายละเอียดที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลมีความสำคัญในเรื่องการเชื่อมโยงระหว่างข้อเท็จจริงที่เกิดขึ้นกับการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล อีกทั้งยังเป็นประโยชน์ต่อเจ้าของข้อมูลส่วนบุคคลที่ต้องการแสวงหาพยานหลักฐานเกี่ยวกับกรณีที่ถูกละเมิดข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองของหน่วยงานภาครัฐ ดังนั้นจึงเห็นควรแก้ไขเพิ่มเติมบทบัญญัติในมาตรา 37 (4) โดยกำหนดให้มีการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล รวมทั้งผลกระทบ และการเยียวยาที่ได้ดำเนินการไว้เป็นหลักฐานด้วย

สรุป

จากการศึกษาสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 พบว่ามีปัญหาเกี่ยวกับการบังคับใช้กฎหมายในทางปฏิบัติที่ส่งผลกระทบโดยตรงต่อการปฏิบัติงานในโรงพยาบาลของรัฐ จากการที่กฎหมายกำหนดหลักเกณฑ์เอาไว้ไม่ชัดเจน อยู่ 4 ประการ โดยสามารถสรุปได้ดังนี้

ตารางที่ 2 สรุปประเด็นปัญหาและผลกระทบที่เกิดจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ปัญหาการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562		
ประเด็นปัญหาที่เกิดจากการบังคับใช้กฎหมาย	**สาเหตุของปัญหา**	**ผลกระทบที่ได้รับจากบังคับใช้กฎหมาย**
1. ปัญหาการไม่มีบทนิยามความหมายของ “ข้อมูลส่วนบุคคลที่อ่อนไหว” และ “ข้อมูลสุขภาพ”	มาตรา 6 ไม่ได้กำหนดความหมายของข้อมูลส่วนบุคคลที่อ่อนไหว” และ “ข้อมูลสุขภาพ” ไว้เป็นการเฉพาะ	เจ้าหน้าที่เกิดความสับสนในการแยกประเภทของข้อมูลส่วนบุคคล การกำหนดมาตรการความปลอดภัยไม่เหมาะสม ขัดต่อหลักความเป็นสากลด้านการแพทย์และการสาธารณสุข
2. ปัญหาการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา 41 ไม่ได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ไม่มีหลักเกณฑ์ที่ชัดเจนที่ใช้พิจารณาคุณสมบัติในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในระดับโรงพยาบาลเพื่อให้คำแนะนำกับเจ้าหน้าที่
3. ปัญหาการกำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา 42 ไม่ได้กำหนดให้ประเมิน ผลกระทบ หรือความเสี่ยงจากการคุ้มครองข้อมูลส่วนบุคคล	มีผลกระทบต่อการจัดลำดับความร้ายแรง และการวางแผนเพื่อรับสถานการณ์ฉุกเฉิน การป้องกันเหตุไม่พึงประสงค์ เช่น การละเมิดข้อมูล การโจมตีระบบคอมพิวเตอร์ เป็นต้น
4. ปัญหาเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล	มาตรา 37 (4) ไม่ได้กำหนดให้ผู้ควบคุมข้อมูลบันทึกรายละเอียดเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นเป็นหลักฐานไว้ที่หน่วยงาน	ไม่มีพยานหลักฐานในการพิสูจน์หักล้างข้อกล่าวหาเมื่อมีเหตุร้องเรียน หรือฟ้องร้องเป็นคดี การกำหนดขอบเขตการดำเนินการทางวินัย การกำหนดสัดส่วนความรับผิดทางละเมิดของเจ้าหน้าที่ และการตรวจสอบจากหน่วยงานต่างๆ

โดยเมื่อพิจารณาสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยที่นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมาเป็นต้นแบบในการยกร่างกลับพบว่ามีสาระสำคัญบางประการที่แตกต่างกัน และสอดคล้องกับสภาพปัญหาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาลของรัฐที่สมควรได้รับการจะแก้ไขปรับปรุงกฎหมาย เพื่อให้มีมาตรฐานทัดเทียมอารยประเทศ และสร้างความเชื่อมั่นแก่ประชาชนที่เข้ารับบริการในโรงพยาบาลของรัฐ ดังต่อไปนี้

ตารางที่ 3 เปรียบเทียบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยและสหภาพยุโรป

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562					**กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป**			
หลักเกณฑ์ที่กำหนด	**มี**	**ไม่มี**	**มาตรา**	**หมายเหตุ**	**มี**	**ไม่มี**	**มาตรา**	**หมายเหตุ**
1. บทนิยามของข้อมูลส่วนบุคคล ที่อ่อนไหว และ ข้อมูลสุขภาพ	-	√	6	ไม่ได้กำหนด	√	-	4 (15) และ 9	กำหนดให้ข้อมูลสุขภาพเป็นข้อมูลส่วนบุคคลชนิดพิเศษหรือ ข้อมูลอ่อนไหว และกำหนดบทนิยามไว้โดยเฉพาะ
2. คุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	-	√	41	ไม่ได้กำหนด	√	-	37	กำหนดให้พิจารณาจากคุณสมบัติทางวิชาชีพด้านสารสนเทศ และการสื่อสารความรู้ทางกฎหมาย
3. การประเมินความเสี่ยงของผลกระทบที่จะเกิดขึ้น	-	√	42	ไม่ได้กำหนด	√	-	35 (7)	กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลเป็นผู้ประเมินความเสี่ยงต่อผลกระทบที่จะเกิดขึ้นกับข้อมูลก่อนการประมวลผล
4. การบันทึกรายละเอียดเกี่ยวกับการละเมิดผลกระทบ และการเยียวยาไว้เป็นหลักฐาน	-	√	37 (4)	ไม่ได้กำหนด	√	-	33	กำหนดให้มีการบันทึกรายละเอียดของเหตุละเมิดผลกระทบการเยียวยาความเสียหายที่ได้ดำเนินการไว้เป็นหลักฐานให้สามารถตรวจสอบได้

ข้อเสนอแนะ

จากปัญหาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้นกับการคุ้มครองข้อมูลส่วนบุคคลภายในโรงพยาบาลของรัฐที่เกิดขึ้น ผู้เขียนจึงขอเสนอแนะแนวทางในการปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้มีความสอดคล้องกับสภาพสังคม และเพิ่มความมาตรฐานความปลอดภัยในกระบวนการคุ้มครองข้อมูลส่วนบุคคลให้เกิดความชัดเจนยิ่งขึ้น ดังต่อไปนี้

1) ปัญหาการไม่มีบทนิยามความหมายที่ชัดเจน โดยในมาตรา 6 ไม่ได้นิยามความหมายของคำว่า “ข้อมูลส่วนบุคคลที่อ่อนไหว” (Sensitive Personal data) และ “ข้อมูลสุขภาพ” ให้ชัดเจน เพื่อมิให้เกิดปัญหา

ในการตีความทางกฎหมายเกี่ยวกับการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลของกฎหมายนี้ หรือกฎหมายอื่นที่เกี่ยวข้อง ดังนั้นจึงควรเพิ่มเติมบทนิยามดังต่อไปนี้

มาตรา 6 ในพระราชบัญญัตินี้

ฯลฯ

“ข้อมูลส่วนบุคคลที่อ่อนไหวง่าย” หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรมในประการที่น่าจะเกิดความเสียหายต่อเกียรติยศ ชื่อเสียง หรือกระทบสิทธิต่างๆ ของบุคคลผู้เป็นเจ้าของข้อมูล หรือข้อมูลอื่นใดตามที่กำหนดไว้ในมาตรา 26

“ข้อมูลสุขภาพ” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับสุขภาพกาย หรือสุขภาพจิตของบุคคลธรรมดา รวมถึงการจัดการบริการสาธารณสุขที่เปิดเผยข้อมูลเกี่ยวกับสถานะทางสุขภาพของบุคคลนั้น ไม่ว่าจะเป็นการให้บริการด้านสุขภาพในหน่วยงานของรัฐ หรือหน่วยงานเอกชน

2) กรณีปัญหาเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 41 เห็นควรเพิ่มคุณสมบัติของผู้มีสิทธิได้รับการแต่งตั้งให้ดำรงตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยเพิ่มเติมไว้ในมาตรา 41 วรรคหก ดังนี้

มาตรา 41 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่

ฯลฯ

วรรคหก การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้พิจารณาจากคุณสมบัติทางวิชาชีพ และความเชี่ยวชาญเป็นที่ประจักษ์ในด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นสำคัญ หรือผู้มีวิชาชีพ หรือความเชี่ยวชาญด้านอื่นที่เป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

วรรคเจ็ด ทั้งนี้คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ฯลฯ

3) กรณีปัญหาเกี่ยวกับอำนาจหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 42 เห็นควรแก้ไขโดยเพิ่มการประเมินผลกระทบหรือความเสี่ยงจากการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไว้ในมาตรา 42 (1) ดังนี้

มาตรา 42 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีการประเมินความเสี่ยงต่อผลกระทบที่จะเกิดขึ้นในกระบวนการป้องกันข้อมูลส่วนบุคคลก่อนที่ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลจะเริ่มดำเนินการใด ๆ ที่เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

ในการประเมินความเสี่ยงให้คำนึงถึงความจำเป็น ความเหมาะสม และการได้สัดส่วนระหว่างผลกระทบต่อสิทธิเสรีภาพของบุคคลกับกระบวนการป้องกันข้อมูลส่วนบุคคล โดยให้แจ้งถึงผลกระทบที่จะเกิดขึ้น พร้อมให้คำแนะนำแก่บุคคลตามวรรคหนึ่งเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

4) ปัญหาเกี่ยวการแจ้งเหตุข้อมูลส่วนบุคคลถูกละเมิดตามมาตรา 37 (4) การแจ้งเหตุข้อมูลส่วนบุคคลถูกละเมิดเป็นหน้าที่ของผู้ควบคุมข้อมูล โดยที่กฎหมายคุ้มครองข้อมูลของไทยไม่ได้กำหนดให้มีการบันทึกหลักฐาน

และการจัดเก็บหลักฐานรายละเอียดที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลซึ่งเป็นเรื่องสำคัญ จึงเห็นควรแก้ไขดังนี้

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่

ฯลฯ

(4) แจ้งเหตุละเมิดข้อมูลส่วนบุคคล...โดยไม่ชักช้า และให้มีการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลทุกที่เกิดขึ้นทุกกรณี ประกอบด้วยข้อเท็จจริงเกี่ยวกับการละเมิด ผลการดำเนินการที่เกี่ยวข้อง เช่น รายงานผลการสอบสวนทางวินัย รายงานผลการสอบสวนความรับผิดทางละเมิดของเจ้าหน้าที่ เป็นต้น หรือผลการดำเนินการอื่น ๆ ตามมาตรการของหน่วยงาน ไม่ว่าจะเป็นมาตรการด้านบุคลากร มาตรการทางกฎหมาย มาตรการการเยียวยา หรือมาตรการอื่นใดที่แสดงให้เห็นว่าได้มีการดำเนินการตามกฎหมายที่เกี่ยวข้อง พร้อมทั้งเก็บรวบรวมหลักฐานที่เกี่ยวกับการละเมิดข้อมูลนั้นเท่าที่จะสามารถรวบรวมได้ และบันทึกไว้เป็นลายลักษณ์อักษรหรือโดยวิธีการอื่นใด หรือทางอิเล็กทรอนิกส์ เพื่อให้หน่วยงานที่เกี่ยวข้องเข้ากำกับดูแลเหตุละเมิดนั้นสามารถตรวจสอบได้ว่ามีการปฏิบัติตามกฎหมาย...

นอกจากการแก้ไขปรับปรุงกฎหมายดังกล่าวข้างต้นแล้ว การเสริมสร้างความรู้ ความเข้าใจ และแนวทางการปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรเป็นสิ่งที่จำเป็น หน่วยงานที่กำกับดูแลโรงพยาบาลของรัฐจึงควรจัดให้มีการอบรมเชิงปฏิบัติการ และจัดทำคู่มือที่เป็นการปฏิบัติให้โรงพยาบาลของรัฐยึดถือปฏิบัติเป็นมาตรฐานเดียวกัน

เอกสารอ้างอิง

กลุ่มงานนิติการ สำนักอำนวยการ. (1 กรกฎาคม 2565). บทความกฎหมายน่ารู้: ความรู้กฎหมาย PDPA เบื้องต้น. เข้าถึงได้จาก สวสพ. สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) : https://www.hrdi.or.th/InternalRules/Detail/1529

คณาธิป ทองรวีวงศ์. (2564). คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพมหานคร: นิติธรรม.

คำสั่งสำนักงานปลัดกระทรวงสาธารณสุข ที่ 1480/2565. (30 มิถุนายน 2565). เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล. เข้าถึงได้จาก https://ict.moph.go.th/upload_file/files/720aa15f55f44e10de248e63b62583d4.pdf

จุมพต สายสุนทร. (2550). กฎหมายระหว่างประเทศ เล่ม 1. พิมพ์ครั้งที่ 7. กรุงเทพมหานคร: วิญญูชน.

ชาติชาย มิตรกูล. (2558). เวชระเบียนผู้ป่วยภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. เข้าถึงได้จาก กรมการแพทย์:http://www.dms.moph.go.th/dmsweb/dmsweb_v2_2/content/org/webpageJDMS_30/demo/ data/2558/2558-05/original%20article%202558-5-6.pdf

ธัญญานุช ตันติกุล. (2560). บทแนะนำหนังสือ: The New Digital Age และ Mostly Cloudy อนาคตในโลกยุคดิจิทัล โอกาส ความหวัง และความท้าทาย. ดุลพาห, 64(3), 210-227.

บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม. (2558). ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิใน ความเป็นอยู่ส่วนตัว (Right to Privacy). กรุงเทพมหานคร: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

พบประกาศขายข้อมูลคนไข้ของ สธ. ล่าสุดลิงค์หายไปแล้ว. (7 กันยายน 2564). ไทยโพสต์. เข้าถึงได้จาก https://www.thaipost.net/main/detail/115865

พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ. (2560). ราชกิจจานุเบกษา เล่มที่ 134 ตอนที่ 24 ก.

พระราชบัญญัติข้อมูลข่าวสารของทางราชการ. (2540). ราชกิจจานุเบกษา เล่ม114 ตอนที่ 46 ก.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. (2562). ราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 69 ก.

พระราชบัญญัติสุขภาพแห่งชาติ. (2550). ราชกิจจานุเบกษา เล่ม 124 ตอนที่ 16 ก.

รพ.สระบุรีโดนมัลแวร์เรียกค่าไถ่ ระบบคอมฯ พัง ต้องซักประวัติใหม่ทำล่าช้า. (9 กันยายน 2563). ไทยรัฐ. เข้าถึงได้จาก https://www.thairath.co.th/news/local/central/1926639

รัฐธรรมนูญแห่งราชอาณาจักรไทย. (2560). ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 40 ก.

สำนักงานปลัดกระทรวงสาธารณสุข หนังสือที่ สธ 0202.3.6/ว1915. (2563). เรื่อง มอบอำนาจให้ผู้ว่าราชการจังหวัดปฏิบัติราชการแทนปลัดกระทรวงสาธารณสุข.

แสวง บุญเฉลิมวิภาส. (2554). การคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพและความเข้าใจเกี่ยวกับมาตรา 7 พ.ร.บ. สุขภาพแห่งชาติ พ.ศ. 2550. กรุงเทพมหานคร: ศูนย์กฎหมายสุขภาพและจริยศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

อลิซอน, แอล. และคณะ. (2544). พฤติกรรมที่เน้นความซาดิสม์และมาโซคิสม์: ความหลากหลายในการปฏิบัติและความหมาย. อาร์ชเซ็กซ์บีฮาฟ.

American Nurses Association. (2018). ANA Position Statement: Nursing Advocacy for LGBTQ+Population. OJIN: The Online Journal of Issues in Nursing, 24(1).

Bundesministerium fur Gesundheit. (2024). Patient Rights. Retrieved from Gesund.bund de: https://gesund.bund.de/en/topics/patient-rights

European Data Protection Board. (2022). Health Data Breach: Dedalus Biologie Fined 1.5 Million Euros. Retrieved from EDPB: https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en

Lynskey, O. (2016). The Foundations of EU Data Protection Law. Oxford: Oxford University Press.

Rubemfeld, J. (1989). The Right of Privacy. Harvard Law Review, 102(4), 737-807.