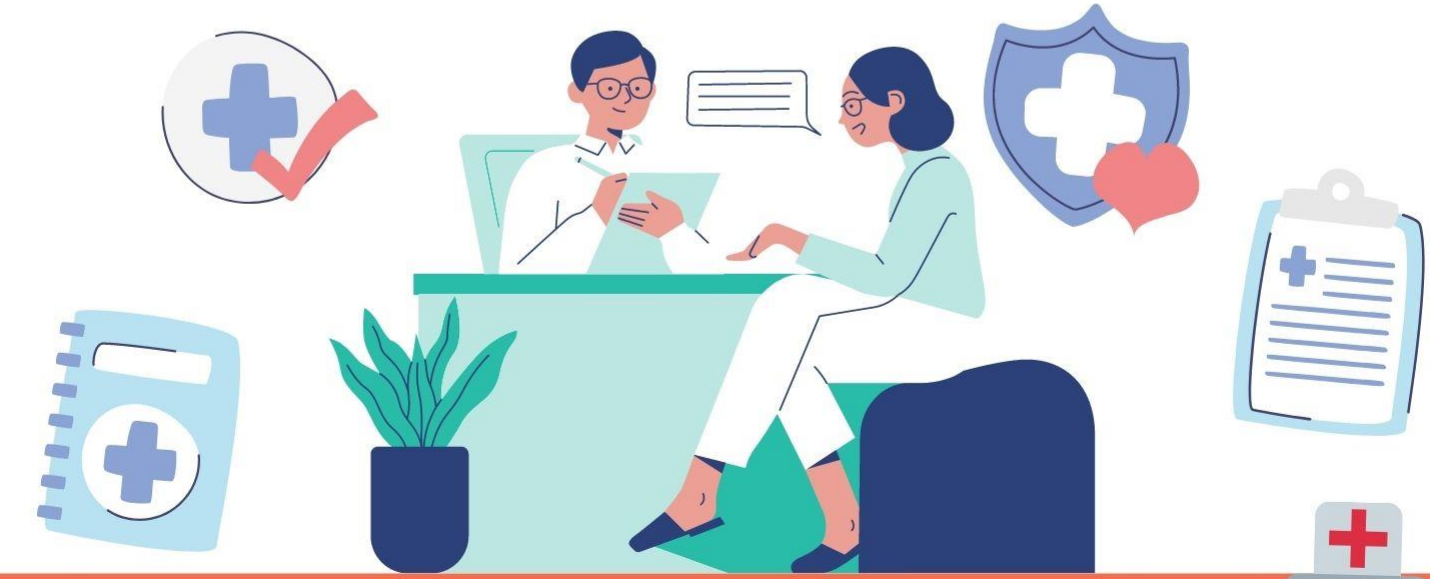
ความรู้เบื้องต้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

สำหรับบุคลากรทางการแพทย์และผู้ปฏิบัติงานในสถานพยาบาล



จัดทำขึ้นเพื่อประกอบการอบรมเชิงปฏิบัติการ "การคุ้มครองข้อมูลส่วนบุคคลในสถานพยาบาลภายใต้ พรบ.คุ้มครองข้อมูลส่วนบุคคล"
ระหว่างเดือนตุลาคม - พฤศจิกายน 2564

คำนำ

ความรู้เบื้องต้นว่าด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับบุคลากรทางการแพทย์และผู้ปฏิบัติงานในสถานพยาบาลฉบับนี้ เป็นเอกสารที่ทางคณะผู้วิจัยได้จัดทำขึ้นภายใต้โครงการวิจัยความโปร่งใสและความมีประสิทธิภาพของความร่วมมือระหว่างรัฐบาลและเอกชนในการบริหารจัดการข้อมูลผู้ได้รับบริการสาธารณสุขในสภาวะวิกฤตการแพร่ระบาดของโรคติดต่อซึ่งได้รับทุนสนับสนุนจากสำนักงานการวิจัยแห่งชาติ (วช.) โดยมีวัตถุประสงค์ คือ เป็นเอกสารเผยแพร่ความรู้ความเข้าใจเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยผู้วิจัยได้สรุปย่อสาระสำคัญของกฎหมายและกรณีศึกษาต่างๆ เพื่อใช้เป็นเอกสารประกอบการบรรยายและกิจกรรมสัมมนาเชิงปฏิบัติการสำหรับบุคลากรทางการแพทย์และผู้ปฏิบัติงานในสถานพยาบาลที่เกี่ยวข้องในด้านการแพทย์และสาธารณสุข ซึ่งจัดขึ้นในช่วงระหว่างเดือนตุลาคม และพฤศจิกายน 2564

เนื้อหาตามเอกสารฉบับนี้ ผู้จัดทำได้เรียบเรียงขึ้นจากการศึกษาเอกสาร ตำรา หนังสือ บทความวิชาการทั้งภาษาไทยและภาษาอังกฤษที่เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสิทธิในความเป็นส่วนตัว ตลอดจนแนวปฏิบัติต่าง ๆ เช่น แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 3.0 (THAILAND DATA PROTECTION GUIDELINES 3.0 – TDPG 3.0) EXTENSION ฉบับพิมพ์ครั้งที่ 3 เมษายน 2564 ซึ่งจัดทำโดยศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เป็นต้น โดยการเรียบเรียงเนื้อหานี้มุ่งสื่อสารเพื่อให้บุคลากรทางการแพทย์และผู้ปฏิบัติงานที่มิใช่นักกฎหมายสามารถเข้าใจและเข้าถึงหลักสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยหวังว่าเนื้อหาจะเป็นพื้นฐานและเป็นแนวทางในการพัฒนา ปรับปรุง และปฏิบัติงานในการเตรียมความพร้อมหน่วยงานและบุคลากรเพื่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยต่อไป

คุณค่าและประโยชน์ใด ๆ อันเกิดจากเอกสารฉบับนี้ ผู้วิจัยขอมอบเป็นกตเวทิตาแก่ครูบาอาจารย์และผู้ที่เกี่ยวข้องที่มีส่วนช่วยเหลือและผลักดันการวางรากฐานกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ความผิดพลาดใด ๆ อันเกิดจากเอกสารฉบับนี้ ผู้วิจัยขอน้อมรับคำแนะนำเพื่อปรับปรุงต่อไป.

คณะผู้วิจัย

PROJECT.PDPA2021@GMAIL.COM

สารบัญ

เนื้อหาส่วนที่ 1 สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล หน้า

สารบัญ(ต่อ)

เนื้อหาส่วนที่ 2 กรณีศึกษาน่ารู้ หน้า

เนื้อหาส่วนที่ 1

สาระสำคัญของ กฎหมายคุ้มครองข้อมูลส่วนบุคคล

คำศัพท์ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลธรรมดาที่ยังมีชีวิตอยู่ที่ถูกระบุหรือสามารถถูกระบุตัวได้ด้วยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้น

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

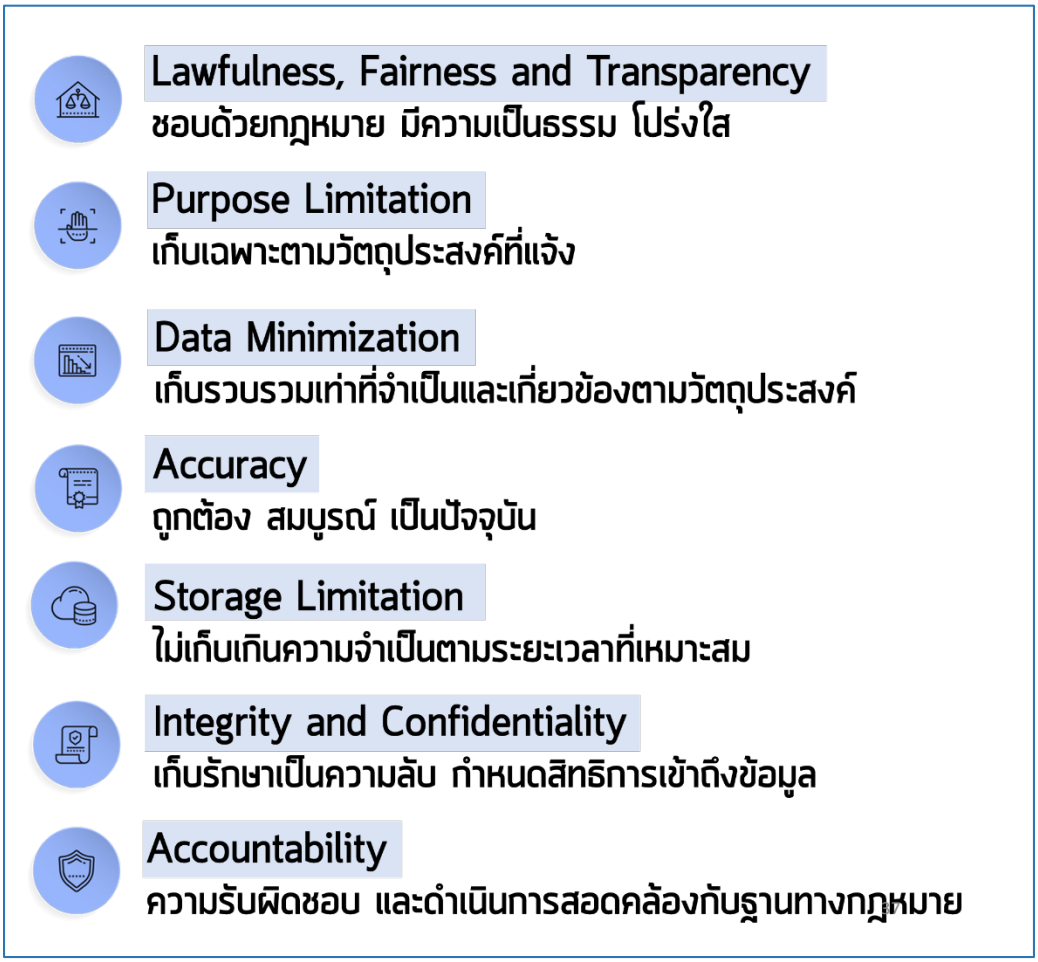
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หมายความว่า บุคคลหรือคณะบุคคลที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในการให้ความรู้คำแนะนำกับองค์กรเกี่ยวกับการปฏิบัติให้ถูกต้องตามตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data / Personally Identifiable Information (PII) หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ประมวลผล (Processing) หมายถึง การดำเนินการหรือชุดการดำเนินการใด ๆ ซึ่งกระทำต่อส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก จัดโครงสร้าง การจัดเก็บ ประยุกต์หรือแก้ไข การกู้คืน การใช้ การเปิดเผยด้วยการส่ง การเปิดเผยด้วยการเผยแพร่หรือทำให้สามารถเข้าถึงได้โดยวิธีอื่นใด การรวมข้อมูล การจำกัด การลบหรือทำลาย (GDPR Article 4 (2))

หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล



หลัก ความชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส (Lawfulness, Fairness and Transparency) กล่าวคือ ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องอยู่ภายใต้เงื่อนไขที่กฎหมายกำหนด มีฐานหรือเหตุทางกฎหมาย (Lawful Basis) รองรับ ใช้วิธีการที่เป็นธรรมและเหมาะสมในการจัดเก็บรวบรวมข้อมูลดังกล่าว การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องให้เจ้าของข้อมูลส่วนบุคคลรับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน จึงจะดำเนินการได้

หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องเป็นไปตามกรอบวัตถุประสงค์ที่กำหนดไว้ ว่าเราจะเก็บรวบรวมข้อมูลส่วนบุคคลมาใช้ทำอะไร และการใช้ จะต้องเป็นไปตามวัตถุประสงค์ดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลส่วนบุคคลทราบ ไม่ว่าผู้ควบคุมข้อมูลจะอาศัยฐานทางกฎหมายใดในการเก็บรวบรวมข้อมูลส่วนบุคคลก็ตาม การเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ จะกระทำไม่ได้

หลักการประมวลผลข้อมูลเท่าที่จำเป็น (Data Minimization) กล่าวคือ การประมวลผลข้อมูลส่วนบุคคล จะกระทำเท่าที่จำเป็น เท่าที่เกี่ยวข้องกับการดำเนินการตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้นเท่านั้น องค์กรไม่ควรเก็บข้อมูลส่วนบุคคลแบบเผื่อ หรือเกินกว่าความจำเป็นที่ต้องใช้เพราะจะทำให้เกิดภาระในการจัดเก็บ รักษาข้อมูลส่วนบุคคลดังกล่าว

หลักความถูกต้อง (Accuracy) กล่าวคือ การเก็บรวบรวมข้อมูล จะต้องมีการความถูกต้องและเป็นปัจจุบัน ตามความจำเป็นในการใช้ข้อมูลส่วนบุคคลดังกล่าว โดยจะต้องมีขั้นตอนที่สมเหตุสมผลเพื่อทำให้มั่นใจว่า ข้อมูลส่วนบุคคลที่ได้มีการเก็บรวบรวมไว้นั้น ถูกต้องตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลดังกล่าว

หลักการเก็บรักษาข้อมูลอย่างจำกัด (Storage Limitation) กล่าวคือ การเก็บรวบรวมข้อมูล มิให้เก็บข้อมูลไว้นานเกินกว่าความจำเป็นตามวัตถุประสงค์ของข้อมูลนั้น

หลักความชอบด้วยกฎหมายและเป็นความลับ (Integrity and Confidentiality) กล่าวคือ ผู้ควบคุมข้อมูลจะต้องมีการจัดเตรียมมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูล

หลักความรับผิดชอบ (Accountability) กล่าวคือ การกำหนดตัวบุคคลที่มีหน้าที่ความรับผิดชอบในการดำเนินการเพื่อให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คืออะไร ?

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลฯ ได้ให้นิยามของคำว่า “ข้อมูลส่วนบุคคล” ว่า หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม”

จากนิยามดังกล่าว ข้อมูลส่วนบุคคล มีองค์ประกอบหลัก ๆ อยู่ 3 ส่วน คือ

หลักการที่หนึ่ง : ข้อมูลต้องเป็นข้อมูลของบุคคลธรรมดา หมายความว่า ใครก็ตาม ที่เป็นบุคคลธรรมดา ล้วนแล้วแต่เป็นเจ้าของข้อมูลส่วนบุคคลได้ แต่ถ้าเป็น นิติบุคคล เช่น ห้างหุ้นส่วนจำกัด บริษัทจำกัด ไม่ใช่บุคคลธรรมดา

ทั้งนี้ ในส่วนของข้อมูลของนิติบุคคล อาจต้องพิจารณาว่า ในข้อมูลดังกล่าว มีข้อมูลของบุคคลธรรมดาอยู่ในนั้นหรือไม่ ซึ่งหากมีข้อมูลดังกล่าว ก็อาจพิจารณาได้ว่า ข้อมูลเหล่านั้น เป็นข้อมูลส่วนบุคคลได้เช่นกัน เช่น ข้อมูลในหนังสือรับรองบริษัท มีข้อมูลเกี่ยวกับ กรรมการบริษัท ซึ่งปรากฏชื่อของกรรมการ ข้อมูลในส่วนของบุคคลธรรมดานั้น ถือเป็นข้อมูลส่วนบุคคล เป็นต้น

หลักการที่สอง : บุคคลดังกล่าว จะต้องเป็นบุคคลที่ยังมีชีวิตอยู่ ยกตัวอย่างเช่น นาย A เป็นบุคคลธรรมดา เป็นเจ้าของข้อมูลส่วนบุคคลได้ ต่อมา นาย A เกิดอุบัติเหตุ เสียชีวิต นาย A จะไม่ถือว่าเป็น “เจ้าของข้อมูลส่วนบุคตคล” อีกต่อไป เพราะเสียชีวิตแล้ว

หลักการที่สาม : ข้อมูลส่วนบุคคลนั้น จะต้องสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม หมายความว่า หากข้อมูลใดๆ ก็ตาม หากสามารถสื่อไปถึงตัวบุคคลคนนั้นได้ ถือว่าเป็นข้อมูลส่วนบุคคลทั้งสิ้น

การสามารถระบุไปถึงเจ้าของข้อมูลได้ มี 3 ลักษณะ คือ[1]

- Distinguishabiliy การแยกแยะ หมายถึง การที่ข้อมูลสามารถระบุแยกแยะตัวบุคคลออกจากกันได้ เช่น ชื่อ นามสกุล หรือ เลขบัตรประจำตัวประชาชน

[1] ศูนย์วิจัยและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, “Thailand Data Protection Guideline 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล”, 2564, หน้า 26-27.

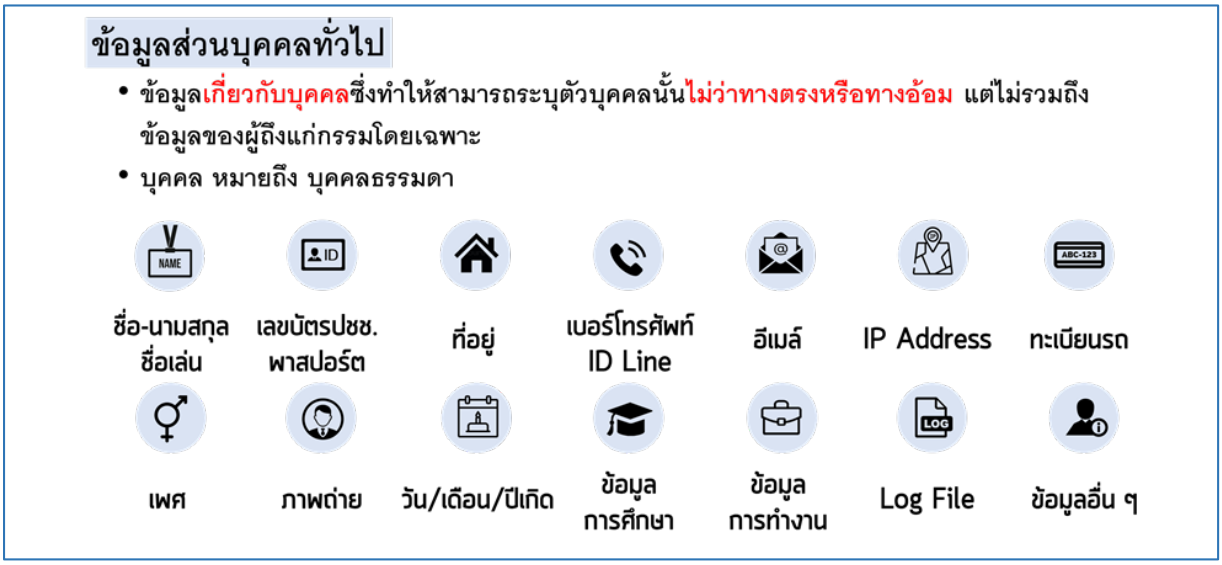
- Tracability การติดตาม หมายถึง การที่ข้อมูลามารถถูกใช้ในการติดตามพฤติกรรมหรือกิจกรรมที่บุคคลนั้นทำได้ เช่น Log File

- Linkability การเชื่อมโยง หมายถึง การที่ข้อมูลสามารถถูกใช้เชื่อมโยงกันเพื่อระบุไปถึงตัวบุคคลได้ โดยแบ่งออกเป็น 2 กรณี คือ

- ข้อมูลที่ถูกเชื่อมโยงแล้ว (Linked) เป็นกรณีหากมีข้อมูลที่เกี่ยวข้องกับข้อมูลที่เมื่อใช้ด้วยกันแล้วสามารถระบุถึงตัวบุคคล เช่น ชุดข้อมูล 2 ชุด แต่ละชุดมีข้อมูลแยกกัน แต่หากมีบุคคลที่สามารถเข้าถึงข้อมูลทั้ง 2 ชุดนั้นได้ ก็จะสามารถเชื่อมโยงและระบุไปถึงตัวบุคคลได้

- ข้อมูลที่อาจถูกเชื่อมโยง (Linkable) เป็นกรณีหากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูลอื่นแล้วก็จะสามารถระบุตัวบุคคลได้ แต่โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมนั้นไม่อยู่ในระบบ หรืออยู่ในอินเตอร์เน็ต หรืออยู่ที่อื่นใด

ตัวอย่างของข้อมูลส่วนบุคคล ได้แก่



ทั้งนี้ ข้อมูลส่วนบุคคลดังกล่าว จะต้องเป็น ข้อมูลที่สื่อไปถึง “บุคคลคนนั้น” ถ้าเป็นข้อมูลที่สื่อไปยังบุคคลอื่น ไม่ถือว่าเป็นข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลรายนั้น

เช่น นาย B เป็นหมออายุรกรรม ประจำโรงพยาบาล XXX

ข้อมูลว่า หมออายุรกรรมท่านนี้ ชื่อ “นาย B” ทำงานอยู่ที่ “โรงพยาบาล XXX” เป็นข้อมูลส่วนบุคคล คุณหมอท่านนี้ ไม่ใช่ข้อมูลส่วนบุคคลของคนอื่น เป็นต้น

ข้อมูลที่ไม่ถือว่าเป็นข้อมูลส่วนบุคคล เช่น ชื่อลูกค้าที่เป็นนิติบุคคล, เลขทะเบียนนิติบุคคล ข้อมูลที่ไม่ปรากฏรายละเอียดของข้อมูลส่วนบุคคล เช่น อีเมลแอดเดรส info@hotmail.com , admin@hotmail.com เป็นต้น

ที่กล่าวมา เป็นข้อมูลส่วนบุคคลทั่ว ๆ ไป แต่ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล มีกล่าวถึงข้อมูลอีกประเภทหนึ่ง ที่เรียกว่า “ข้อมูลส่วนบุคคลประเภทอ่อนไหว” หรือ “Sensitive Data” ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนกว่าข้อมูลส่วนบุคคลทั่วไป เป็นเรื่องส่วนตัวโดยแท้ของบุคคล และมีความสุ่มเสี่ยงต่อการถูกนำไปใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม อันอาจทำให้ผู้ที่ได้รับข้อมูลดังกล่าว เกิดความรู้สึกบางอย่างกับเจ้าของข้อมูลส่วนบุคคล เวลาต้องเข้าไปเก็บรวบรวม ใช้ข้อมูลดังกล่าว จึงต้องใช้ความระมัดระวังมากยิ่งขึ้น เช่น

ตัวอย่างเช่น

- ประวัติการติดเชื้อไวรัสโคโรน่า-2019 ซึ่งจัดเป็น “ข้อมูลสุขภาพ” ที่บางคนหากทราบข้อมูลดังกล่าว อาจรู้สึกไม่สบายใจ ไม่กล้าเข้าใจ เพราะกลัวการแพร่ระบาดของเชื้อไวรัส

- ประวัติอาชญากรรม ที่หลาย ๆ องค์กร ใช้เป็นหนึ่งปัจจัยในการพิจารณาว่าจ้างให้เข้ามาทำงานให้กับบริษัทฯ เป็นต้น

ขอบเขตการบังคับใช้ตามกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้บังคับกับการ เก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ของบุคคลธรรมดา เท่านั้น หากไม่ใช่การเก็บรวบรวม ใช้ เปิดเผย แล้ว ไม่อยู่ในขอบข่ายของการปฏิบัติตามกฎหมายฉบับนี้

ขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล จะใช้บังคับแก่กรณี ดังต่อไปนี้

- ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรไทย
- มีผลใช้บังคับถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมีกิจกรรม ดังนี้

  (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่

  (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร

ทั้งนี้ กฎหมายฉบับนี้ ไม่ใช้บังคับแก่กรณีดังต่อไปนี้

1) การเก็บรวบรวม ใช้ หรือเปิดเผย เพื่อประโยชน์ส่วนตน หรือ เพื่อกิจกรรมในครอบครัวของบุคคลนั้น

2) การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ความมั่นคงทางการคลังของรัฐ การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์

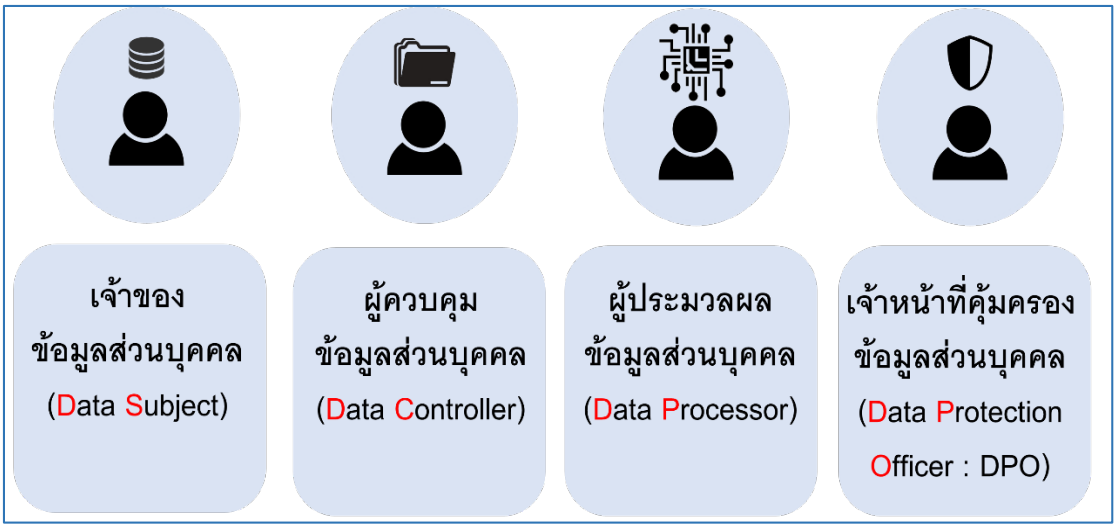
3) การเก็บรวบรวมเพื่อกิจการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

4) สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมาธิการ ตามอำนาจและหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมาธิการ

5) การพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ การดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ทั้งนี้ ในส่วนของบุคคลที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล จะมีอยู่ 4 กลุ่มหลัก ๆ คือ เจ้าของข้อมูลส่วนบุคคล, ผู้ควบคุมข้อมูลส่วนบุคคล, ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจะแยกพิจารณาเป็นแต่ละกรณี



เจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลที่กฎหมายให้การรับรองและคุ้มครองถึงสิทธิเกี่ยวกับข้อมูลส่วนบุคคล ไม่ให้ใครทำการประมวลผลข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมายรองรับ

คนทุกคน สามารถเป็นเจ้าของข้อมูลส่วนบุคคลได้ ไม่ได้จำกัดว่า คนที่จะเป็นเจ้าของข้อมูลส่วนบุคคลจะต้องเป็น “ลูกค้า” หรือ “คนไข้” ที่เข้ามารับบริการกับเราเท่านั้น เพราะ การคุ้มครองข้อมูลส่วนบุคคล มุ่งคุ้มครอง “บุคคลธรรมดา” ทุกคน เสมอกัน ไม่ได้จำกัดว่า เขาเหล่านั้น จะอยู่ในสถานะทางกฎหมายใด

เขาอาจจะเป็น “ลูกค้า” ก็ได้

เขาอาจจะเป็น “พนักงาน” หรือ “ลูกจ้าง” ในองค์กรก็ได้

เขาอาจจะเป็นคนที่ไม่ได้มีความผูกพันใด ๆ ตามกฎหมายกับเราเลยก็ได้ เช่น คนที่เดินผ่านไปผ่านมาในบริเวณพื้นที่ของเรา หากเรามีการติดตั้งกล้อง CCTV เอาไว้ในพื้นที่ เราก็อาจมีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้อื่นได้เช่นกัน

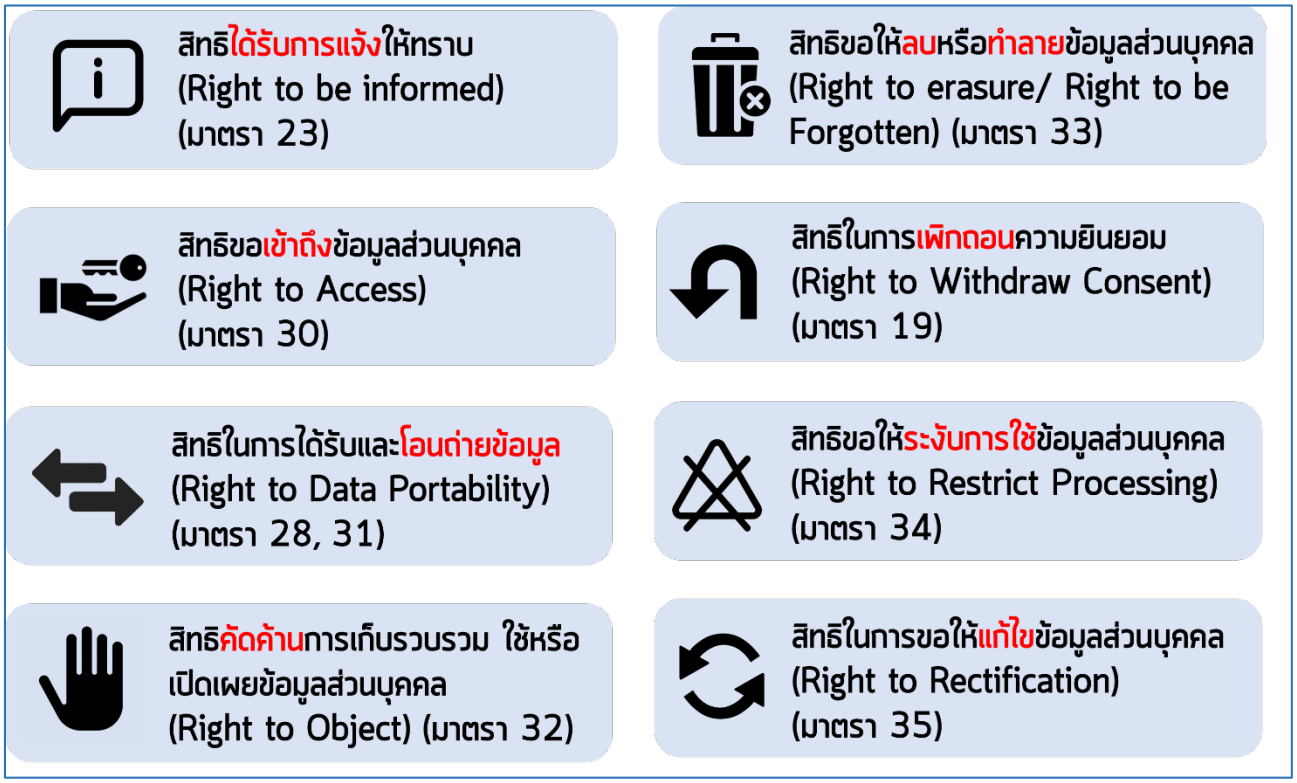
ที่เราต้องรู้ว่า ใครเป็นเจ้าของข้อมูลส่วนบุคคล ก็เพราะว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคล มุ่งเน้นให้ความสำคัญกับ “เจ้าของข้อมูลส่วนบุคคล” ที่กฎหมายฉบับนี้ ออกมาคุ้มครองไม่ให้ “สิทธิในข้อมูลส่วนบุคคล” ถูกบุคคลหนึ่งบุคคลใดล่วงละเมิด หรือ นำข้อมูลส่วนบุคคลเอาไปใช้โดยไม่ชอบ

เมื่อรู้แล้วว่า ใครเป็น “เจ้าของข้อมูลส่วนบุคคล” แล้ว เรามาทำความเข้าใจกันต่อ ว่า เราในฐานะที่เป็น “เจ้าของข้อมูลส่วนบุคคล” มี “สิทธิ” อะไรที่กฎหมายให้การรับรองและคุ้มครองบ้าง

จะได้รู้ว่า เมื่อวันหนึ่ง มีคนเข้ามาล่วงละเมิดสิทธิของเรา เราสามารถใช้สิทธิอะไร ในการปกป้องรักษาสิทธิของเราได้

สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล ที่ได้รับความคุ้มครองตามกฎหมาย ควรรู้ถึง “สิทธิของเจ้าของข้อมูลส่วนบุคคล” ว่ามีสิทธิในการดำเนินการอย่างไร กับบุคคลที่เข้ามาเกี่ยวกับข้อมูลส่วนบุคคลของตน โดยกฎหมายให้การรับรองสิทธิพื้นฐานของเจ้าของข้อมูลส่วนบุคคล ดังนี้



1. สิทธิได้รับการแจ้ง (Right to Be Informed)

การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งรายละเอียดในการเก็บข้อมูลตลอดจนการนำไปใช้ หรือเผยแพร่ให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูล (ยกเว้นกรณีที่เจ้าของข้อมูลทราบรายละเอียดนั้นอยู่แล้ว เช่น เพื่อนำไปเปิดบัญชี หรือสมัครใช้ผลิตภัณฑ์และบริการต่างๆ) โดยเจ้าของข้อมูลมีสิทธิที่จะทราบวัตถุประสงค์ของการเก็บข้อมูล, การนำไปใช้ หรือเผยแพร่, สิ่งที่ต้องการจัดเก็บ, ระยะเวลาในการเก็บข้อมูล ตลอดจนรายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคล เช่น สถานที่ติดต่อและวิธีการติดต่อ รวมถึงผลกระทบที่อาจเกิดขึ้นจากการไม่ให้ข้อมูล

2. **สิทธิขอเข้าถึงข้อมูลส่วนบุคคล** (Right to Access) ได้มีการกำหนดหลักเกณฑ์เอาไว้ในมาตรา 30 โดยเจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน ซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล

ในการติดต่อขอใช้สิทธิดังกล่าว ตามกฎหมายไม่ได้กำหนดว่า จะต้องเป็นเจ้าของข้อมูลส่วนบุคคลคนนั้นเท่านั้น ที่จะขอใช้สิทธิได้ การดำเนินการใช้สิทธิขอเข้าถึง จึงสามารถมอบอำนาจให้ดำเนินการแทนเจ้าของข้อมูลส่วนบุคคลได้ โดยจะต้องมีการทำหลักฐานการมอบอำนาจให้ถูกต้อง

ในการขอเข้าถึงข้อมูลส่วนบุคคล ในต่างประเทศ จะเรียกว่า Data Subject Access Request หรือ DSAR ที่ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องกำหนดวิธีในการที่เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิในการเข้าถึงข้อมูลของตน และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการอย่างไร ภายในกำหนดระยะเวลาเท่าไหร่

กรณีที่ เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคล โดยข้อมูลดังกล่าว มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลท่านอื่น การถ่ายสำเนาหรือการส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลส่วนบุคคลผู้ใช้สิทธิ จะต้องพิจารณาดำเนินการให้โดยไม่กระทบกระเทือนถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลอื่นด้วย

ในการใช้สิทธิขอเข้าถึงข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลได้รับแล้ว อาจปฏิเสธการใช้สิทธิดังกล่าวได้ หากมีเหตุที่กฎหมายกำหนดไว้ ดังนี้

1) เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล

2) เป็นการเขาถึงและขอรับสำเนาข้อมูลส่วนบุคคลดังกล่าวจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

3. **สิทธิในการได้รับหรือโอนถ่ายข้อมูล** (Right to Data Portability)

เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ และเจ้าของข้อมูลส่วนบุคคล สามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ส่งหรือโอนข้อมูลส่วนบุคคลของตนไปยังบุคคลอื่นได้ หากข้อมูลดังกล่าวอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ

4. **สิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล** (Right to Object)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ โดยเมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้าน ผู้ควบคุมข้อมูลส่วนบุคคล ไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ โดยผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแยกส่วนข้อมูลส่วนบุคคลดังกล่าวกับข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

แต่ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการคัดค้าน เนื่องจาก มีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือ เมื่อการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลนั้น เป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

5. **สิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล** (Right to Erasure / Right to be Forgotten)

เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอลบข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมเอาไว้ อย่างไรก็ตาม แม้เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิดังกล่าวได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธการใช้สิทธิดังกล่าวได้ หากมีเหตุทางกฎหมายรองรับในการปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

6. **สิทธิในการเพิกถอนความยินยอม** (Right to Withdraw Consent)

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดยอาศัยฐานความยินยอม เจ้าของข้อมูลส่วนบุคคลสามารถเพิกถอนความยินยอมดังกล่าวได้โดยอิสระ และภายหลังจากที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมแล้ว ผู้ควบคุมข้อมูลส่วนบุคคล ไม่สามารถประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ หากปราศจากฐานทางกฎหมายอื่นรองรับ

7. **สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล** (Right to Restrict Processing)

เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล เมื่อเข้าเหตุหรือเงื่อนไข กรณีหนึ่งกรณีใดดังต่อไปนี้

7.1 เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา 36

7.2 เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา 33 (4) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน

7.3 เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

8. **สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล** (Right to Rectification)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลที่เกี่ยวกับตนให้ถูกต้อง พร้อมใช้ และเป็นปัจจุบันได้ ตัวอย่างเช่น คนไข้เคยขึ้นทะเบียนผู้ป่วยและมีประวัติการรักษาอยู่ที่โรงพยาบาล ต่อมา คนไข้ได้แต่งงาน เปลี่ยนชื่อ เปลี่ยนนามสกุล คนไข้ ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลสามารถแจ้งโรงพยาบาลให้เปลี่ยนชื่อและนามสกุลของตนที่อยู่ในฐานข้อมูลคนไข้ของโรงพยาบาลให้ถูกต้องตามความเป็นจริงและเป็นปัจจุบันได้

ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น กฎหมายให้ความคุ้มครองเอาไว้ว่า “ห้ามประมวลผลข้อมูลส่วนบุคคล เว้นแต่ จะมีฐานหรือเหตุแห่งการประมวลผลให้ทำได้ตามกฎหมาย”

โดยฐานทางกฎหมาย ในการประมวลผลข้อมูลส่วนบุคคล ตามกฎหมายไทย ได้กำหนดเอาไว้ในมาตรา 24 และมาตรา 26

LAWFUL BASIS	GDPR	PDPA
ฐานความยินยอม (Consent)	Article 6 (1)(a)	มาตรา 19 มาตรา 24
ฐานการปฏิบัติตามสัญญา (Contract)	Article 6 (1)(b)	มาตรา 24 (3)
ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal Obligation)	Article 6 (1)(c)	มาตรา 24 (6)
ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)	Article 6 (1)(d)	มาตรา 24 (2)
ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)	Article 6 (1)(e)	มาตรา 24 (4)
ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)	Article 6 (1)(f)	มาตรา 24 (5)
ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Historical & Statistic Research)	Article 89	มาตรา 24 (1)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้วางหลักเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล ไว้ในมาตรา 24 และ มาตรา 26 โดยมาตรา 24 เป็นกรณีเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไป ส่วนมาตรา 26 เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) โดยมีรายละเอียด ดังนี้

มาตรา 24

หลัก ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

ข้อยกเว้น

1. จัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือเกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
2. ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
6. เพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 26

หลัก ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

ข้อยกเว้น

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
2. ดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไร
3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
4. เป็นการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกม.
5. เป็นการจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับ
   (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์
   (ข) ประโยชน์สาธารณะด้านการสาธารณสุข
   (ค) การคุ้มครองแรงงาน
   (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่น
   (จ) ประโยชน์สาธารณะที่สำคัญ

ฐานทางกฎหมาย (Lawful Basis) ตามกฎหมาย มี 7 ฐาน ซึ่งหากเข้าหลักเกณฑ์ฐานใดฐานหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคล จะสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ โดยแต่ละฐาน มีรายละเอียด ดังนี้

ฐานความยินยอม (Consent)

ฐานความยินยอม เป็นหนึ่งฐานที่หลายคนให้ความสนใจ เพราะเข้าใจว่า การจะเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลของผู้อื่น จะต้องได้รับความยินยอมเสมอ

หลักเกณฑ์เกี่ยวกับความยินยอม มีรายละเอียดเบื้องต้น ดังนี้

- ต้องได้รับความยินยอม "ก่อน" หรือ "ขณะ" เก็บรวบรวมข้อมูล >> หากมีการเก็บรวบรวมข้อมูลก่อนแล้วมาขอความยินยอมภายหลัง ไม่ได้

- ความยินยอม จะต้องชัดแจ้ง >> การนิ่ง ไม่นับว่าเป็นการให้ความยินยอม

- ความยินยอม จะต้องทำเป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์ >> เพื่อให้การให้ความยินยอม มีความชัดเจน และมีหลักฐานยืนยัน ป้องกันการโต้แย้งกันในภายหลัง

- ในการขอความยินยอมจะต้องแจ้งวัตถุประสงค์ที่มีความชัดแจ้ง เฉพาะเจาะจง ให้เจ้าของข้อมูลส่วนบุคคลรับรู้รับทราบ

- ข้อความในการขอความยินยอม จะต้องแยกส่วนจากข้อความอื่น ๆ >> การขอความยินยอมอาจระบุอยู่ในนโยบายความคุ้มครองข้อมูลส่วนบุคคล หรือเอกสารอื่นใดก็ได้ หรือจะขัดทำเป็นหนังสือขอความยินยอมเป็นเอกสารอีกฉบับหนึ่งแยกต่างหากก็ได้

- การขอความยินยอม ต้องใช้ภาษาที่เข้าถึงง่าย เข้าใจง่าย อ่านง่าย >> ไม่ได้จำเป็นจะต้องทำเป็นภาษากฎหมาย

- การไม่ให้ความยินยอม จะต้องไม่เป็นเงื่อนไขการให้บริการ >> ผู้ควบคุมข้อมูลส่วนบุคคล จะกำหนดเงื่อนไขในการใช้บริการว่า เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมก่อน จึงจะเข้าใช้บริการได้ ลักษณะนี้ทำไม่ได้

- การขอความยินยอมจะต้องไม่เป็นการหลวงลวงหรือทำให้สำคัญผิด >> ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งขอความยินยอมแก่เจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้ง โดยจะไม่หลอกลวงให้เขาสำคัญผิดในการให้ความยินยอม

- ความยินยอม จะต้องเป็นอิสระ >> เจ้าของข้อมูลส่วนบุคคล มีอิสระในการตัดสินใจว่า จะให้หรือไม่ให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวมข้อมูลส่วนบุคคลของตนได้

- ความยินยอมจะต้องไม่มีเงื่อนไขในการให้ความยินยอม >> จะต้องเป็นการให้ความยินยอมโดยชัดแจ้ง โดยไม่มีการกำหนดเงื่อนไข เช่น ให้ความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคลก็ได้ หากผู้ควบคุมข้อมูลส่วนบุคคล อนุญาตให้เข้ารับบริการทางการแพทย์โดยลดค่าบริการ 30 เปอร์เซ็นต์ ลักษณะนี้ ทำไม่ได้

- การขอความยินยอมจะต้องกระทำเท่าที่จำเป็น และชอบด้วยกฎหมาย

- การเก็บรวบรวมข้อมูลโดยใช้ฐานความยินยอม เจ้าของข้อมูลสามารถถอนความยินยอมเมื่อไหร่ก็ได้

- การถอนความยินยอมจะต้องง่ายเหมือนตอนให้ความยินยอม >> หากตอนขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล ดำเนินการในลักษณะใด การถอนความยินยอม ก็จะต้องดำเนินการในลักษณะเดียวกัน เช่น ตอนให้ความยินยอม เพียงแค่กดคลิก “ให้ความยินยอม” ตอนถอนความยินยอม จะกำหนดว่าหากจะถอนความยินยอม จะต้องชำระค่าบริการเพิ่ม 5,000 บาท ลักษณะนี้ ทำไม่ได้

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งผลกระทบที่อาจเกิดขึ้นจากการถอนความยินยอม >> ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่า หากถอนความยินยอมแล้ว จะทำให้ไม่สามารถให้บริการได้ตามปกติในลักษณะเช่นเดียวกันตอนให้ความยินยอม เป็นต้น

- เมื่อได้รับความยินยอมให้เก็บรวบรวมข้อมูลแล้ว จะนำข้อมูลที่เก็บรวบรวมดังกล่าวมาใช้แตกต่างจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูล หรือนอกกรอบความยินยอม ไม่ได้

ฐานการปฏิบัติตามสัญญา (Contract)

จะต้องเป็นกรณีเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หากบุคคลอื่นเป็นคู่สัญญาไม่สามารถอ้างหลักการปฏิบัติตามสัญญาได้ และการปฏิบัติตามสัญญา ครอบคลุมไปถึง การดำเนินการก่อนเข้าทำสัญญาด้วย

ตัวอย่างเช่น การสมัครงาน ผู้สมัครงาน กรอกข้อมูลเกี่ยวกับประวัติส่วนตัว ซึ่งเป็นข้อมูลส่วนบุคคลให้แก่ บริษัท แม้ในขณะยื่นใบสมัคร ความสัมพันธ์ระหว่างผู้สมัครกับบริษัท จะยังไม่มีฐานะเป็นนายจ้าง-ลูกจ้าง ตามสัญญาจ้างแรงงาน แต่เป็นกรณีที่ บริษัท สามารถเก็บรวบรวมข้อมูลส่วนบุคคลของผู้สมัครงานได้ โดยอาศัยฐานการปฏิบัติตามสัญญา (Contract)

- ในสัญญาหนึ่งอาจประกอบด้วยกิจกรรมย่อย ๆ หลายอย่าง เกี่ยวกับข้อมูลส่วนบุคคล กิจกรรมบางอย่างจำเป็นในการปฏิบัติตามสัญญา จึงไม่ต้องขอความยินยอม แต่กิจกรรมบางอย่าง ไม่เกี่ยวข้องกับการปฏิบัติตามสัญญา จึงต้องอาศัยฐานหรือเหตุอื่น ซึ่งหากใช้ฐานความยินยอม ก็จะต้องแยกการขอความยินยอมสำหรับกิจกรรมเหล่านั้นออกมาเป็นการเฉพาะโดยไม่นำไปรวมกับกิจกรรมที่จำเป็นตามสัญญา

ฐานสัญญาใช้ได้เฉพาะแต่การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลทั่วไปของเจ้าของข้อมูลส่วนบุคคล เท่านั้น ไม่สามารถใช้กับข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ได้

ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)

ฐานนี้เป็นฐานที่กฎหมายกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการอันเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ตัวอย่างเช่น พนักงานของบริษัท กฎหมายแรงงาน กำหนดให้นายจ้างต้องจัดทำทะเบียนลูกจ้าง กฎหมายประกันสังคม กำหนดให้นายจ้างขึ้นทะเบียนผู้ประกันตนต่อสำนักงานประกันสังคม ซึ่งเป็นหน้าที่ที่กฎหมายกำหนด นายจ้างจึงสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานได้ โดยอาศัยฐานการปฏิบัติหน้าที่ตามกฎหมาย เป็นต้น

ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)

เป็นกรณีการประมวลผลข้อมูลส่วนบุคคลที่มีความจำเป็นสำคัญเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล โดยเฉพาะกรณีฉุกเฉินเกี่ยวกับการแพทย์ โดยจำกัดเฉพาะกรณีที่มีเหตุฉุกเฉินซึ่งไม่อาจขอความยินยอมได้ ทั้งนี้

ฐานนี้ ไม่ได้จำกัดเฉพาะการกระทำต่อข้อมูลเพื่อป้องกันประโยชน์ของเจ้าของข้อมูล แต่รวมถึงการกระทำต่อข้อมูลของบุคคลเพื่อประโยชน์ต่อชีวิตของบุคคลอื่นด้วย โดยเป็นกรณีไม่สามารถอาศัยเหตุหรือฐานอื่นในการประมวลผลได้

ฐานนี้ ใช้ได้แต่เฉพาะกับข้อมูลส่วนบุคคลทั่วไปเท่านั้น

ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)

ฐานนี้ แยกเป็น 2 กรณี คือ

(1) ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐหรือเจ้าหน้าที่รัฐ ซึ่งเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลในการใช้อำนาจรัฐ หรือดำเนินภารกิจเพื่อประโยชน์สาธารณะ

(2) ผู้ควบคุมข้อมูลส่วนบุคคล ที่เป็นผู้ประกอบธุรกิจหรือหน่วยงานเอกชนซึ่งเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลในการใช้อำนาจที่รัฐมอบให้หรือดำเนินภารกิจเพื่อประโยชน์สาธารณะ

ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)

ฐานนี้เป็นฐานหนึ่งที่มีขอบเขตการใช้ค่อนข้างกว้าง โดยการจะนำฐานนี้มาใช้ จะต้องเป็นกรณีที่ไม่มีวิธีอื่นใด หรือไม่มีฐานทางกฎหมายอื่นใด ในการบรรลุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว หากสามารถใช้ฐานทางกฎหมายฐานอื่นได้ ให้เลือกพิจารณาใช้ฐานทางกฎหมายฐานอื่นก่อน แต่หากไม่มีฐานทางกฎหมายใดรองรับ จึงนำฐานนี้มาพิจารณา

โดยบุคคลหรือหน่วยงานที่อาจอ้างเหตุหรือฐานนี้ได้ ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าหน้าที่ของรัฐ และรวมถึงบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล

ในการอ้างฐานทางกฎหมายนี้ จะต้องประเมินชั่งน้ำหนักระหว่างประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคลว่าสิทธิใด

ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุหรือเพื่อประโยชน์สาธารณะหรือการศึกษาวิจัยหรือสถิติ (Historical & Statistic Research)

ฐานนี้ ปัจจุบัน ยังไม่ได้มีการกำหนดไว้โดยชัดเจน ต้องรอคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนดรายละเอียดและเงื่อนไขให้ชัดเจน

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- ผู้ควบคุมข้อมูลส่วนบุคคล อาจเป็นบุคคลธรรมดา หรือ นิติบุคคล ก็ได้
- กฎหมายไม่ได้จำกัดว่าจะต้องเป็นนิติบุคคลที่จัดขึ้นตามกฎหมายใด
- ผู้ควบคุมข้อมูลส่วนบุคคล คือ ผู้ที่มีอำนาจตัดสินใจเกี่ยวกับ วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- พิจารณาในลักษณะของ “องค์กร” พนักงานหรือลูกจ้างในองค์กร ไม่ถือว่าเป็น ผู้ควบคุมข้อมูลส่วนบุคคล
- แม้มีการแบ่งเป็นแผนก ฝ่าย หรือ ส่วนงานย่อย หากเป็นไปตามนโยบายหรือข้อกำหนดขององค์กร หน่วยงานย่อยมีสถานะเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล แต่หน่วยงานย่อยนั้น ไม่ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล

คำถามสำหรับบุคคลหรือนิติบุคคลเพื่อประเมินตนเองในเบื้องต้นว่าเข้าข่ายเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่[2]

- ☐ เราเป็นผู้ตัดสินใจเก็บรวบรวมหรือประเมิลผลข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้ตัดสินใจเกี่ยวกับวัตถุประสงค์และผลที่จะได้รับจากการประมลผลข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดบ้าง
- ☐ เราเป็นผู้ตัดสินใจว่าจะเก็บข้อมูลส่วนบุคคลของบุคคลใด
- ☐ เราเป็นผู้ได้รับประโยชน์เชิงพาณิชย์หรือประโยชน์อื่นใดจากการประมวลผล
- ☐ เราประมวลผลข้อมูลส่วนบุคคลเนื่องจากผลของสัญญากับเจ้าของข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้ตัดสินใจเกี่ยวกับบุคคลโดยอาศัยผลจากการประมวลผลข้อมูลส่วนบุคคล

[2] คณาธิป ทองรวีวงศ์, “คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล”, สำนักพิมพ์นิติธรรม, 2564, หน้า 106-107,

- ☐ เจ้าของข้อมูลส่วนบุคคลเป็นลูกจ้างของเรา
- ☐ เราเป็นผู้ตัดสินใจเกี่ยวกับบุคคลโดยอาศัยผลจากการประมวลผลข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้ใช้อำนาจตัดสินใจทางวิชาชีพในการประมวลผลข้อมูลส่วนบุคคล
- ☐ เรามีความสัมพันธ์โดยตรงกับเจ้าของข้อมูลส่วนบุคคล
- ☐ เราสามารถดำเนินการโดยอิสระในการกำหนดว่าจะประมวลผลข้อมูลส่วนบุคคลอย่างไร
- ☐ เราเป็นผู้แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อประมวลผลข้อมูลส่วนบุคคลในนามของเรา

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวให้ทันสมัยตามเทคโนโลยี และเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะกำหนดต่อไป

2. จัดให้มีมาตรการป้องการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ

3. จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้เมื่อข้อมูลนั้นหมดความจำเป็นที่จะใช้ เกินจำเป็น หรือเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศกำหนดหลักเกณฑ์ในการลบ หรือ ทำลายข้อมูลส่วนบุคคลได้ในอนาคต

4. แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมงนับแต่เมื่อทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

5. แต่งตั้งตัวแทนในราชอาณาจักร หากผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกประเทศไทย ผู้ควบคุมส่วนบุคคลต้องแต่งตั้งตัวแทนของตนในประเทศไทย โดยต้องแต่งตั้งเป็นหนังสือ

6. จัดทำบันทึกรายการ (มาตรา 39) โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำรายการในรูปแบบหนังสือหรือรูปแบบอิเล็กทรอนิกส์เพื่อให้เจ้าของข้อมูลส่วนบุคคลหรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยต้องจดบันทึกรายการเกี่ยวกับข้อมูลที่เก็บรวบรวม, วัตถุประสงค์ของการเก็บรวบรวม, ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล, ระยะเวลาเก็บรักษาข้อมูล, สิทธิและวิธีการเข้าถึงข้อมูล, เงื่อนไขของผู้มีสิทธิเข้าถึงข้อมูลและการเข้าถึงข้อมูล, การเก็บรวมรวบ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมตามข้อยกเว้นที่กฎหมายกำหนด, การปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล, และ คำอธิบายมาตรการรักษาความปลอดภัยของข้อมูล

7. จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer): หากผู้ควบคุมข้อมูลส่วนบุคคล เป็นบุคคลดังกรณีต่อไปนี้

- เป็นหน่วยงานของรัฐ
- ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเป็นจำนวนมากโดยดำเนินการอย่างสม่ำเสมอ หรือ
- กิจกรรมธุรกิจหลักของผู้ควบคุมข้อมูลส่วนบุคคลเป็นกิจกรรมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data)

ทั้งนี้ เป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

8. ดำเนินการให้ข้อมูลส่วนบุคคลนั้น ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

9. บันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เมื่อผู้ควบคุมข้อมูลส่วนบุคคล ปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมเหตุผลไว้ในรายการบันทึกรายการตามมาตรา 39

10. จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ซึ่งเป็นสัญญาที่กำหนดสิทธิและหน้าที่ในการปฏิบัติหน้าที่ให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- ผู้ประมวลผลข้อมูลส่วนบุคคล อาจเป็นบุคคลธรรมดา หรือ นิติบุคคล ก็ได้
- การประมวลผล ไม่ได้จำกัดแค่ การนำข้อมูลมาวิเคราะห์ เท่านั้น แต่รวมถึง การเก็บรวบรวม ใช้ เปิดเผย ด้วย
- ผู้ประมวลผลเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล “ในนามหรือตามคำสั่ง” ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ได้เป็นผู้ตัดสินใจในการดำเนินการดังกล่าวด้วยตนเอง
- ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล จึงไม่มีหน้าที่และความรับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เช่น ไม่มีหน้าที่เกี่ยวกับเหตุหรือฐานทางกฎหมาย (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคล เป็นต้น
- หากดำเนินการเกินขอบเขตของการกระทำ “ในนามหรือตามคำสั่ง” ผู้ประมวลผลข้อมูลส่วนบุคคล จะมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ในส่วนของการที่กระทำเกินขอบเขตนั้น

คำถามสำหรับบุคคลหรือนิติบุคคลเพื่อประเมินตนเองในเบื้องต้นว่าเข้าข่ายเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่[3]

- ☐ เราดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของบุคคลอื่น
- ☐ เราได้รับข้อมูลส่วนบุคคลจากลูกค้าหรือบุคคลที่สามหรือได้รับคำสั่งให้เก็บรวบรวมข้อมูลส่วนบุคคล
- ☐ เราไม่ได้ตัดสินใจเก็บรวบรวมข้อมูลส่วนบุคคลของผู้อื่น
- ☐ เราไม่ได้ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลใด
- ☐ เราไม่ได้ตัดสินใจเกี่ยวกับเหตุหรือฐานทางกฎหมาย (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคล
- ☐ เราไม่ได้ตัดสินใจเกี่ยวกับวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคล

[3] เพิ่งอ้าง, หน้า 111-112.

- เราไม่ได้ตัดสินใจว่าจะเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ใด
- เราอาจทำการตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคลอย่างไร แต่การตัดสินใจนั้นอยู่ภายใต้สัญญาที่ทำกับบุคคลอื่น
- เราไม่คำนึงถึงผลสุดท้ายของการประมวลผลข้อมูลส่วนบุคคล

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมาย ดังนี้

1. ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยต้องกระทำภายในขอบเขตคำสั่งที่ได้รับมาจากผู้ควบคุมข้อมูลส่วนบุคคล หากกระทำเกินกว่าขอบเขตคำสั่ง หรือ กระทำโดยไม่มีคำสั่ง จะถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม โดยหน้าที่นี้ มีลักษณะเช่นเดียวกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล แต่หากเกิดกรณีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดดังกล่าวด้วย

3. จัดทำและเก็บรักษาบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities (ROPA)) โดยหน้าที่การจัดทำบันทึกตามข้อนี้มิใช่กรณีตามมาตรา 39 ซึ่งเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลที่ตนได้ทำไป โดยหลักเกณฑ์และวิธีการทำจะถูกกำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต่อไป

4. หน้าที่ในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกันกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หากผู้ประมวลผลข้อมูลส่วนบุคคลเข้าเกณฑ์ที่ระบุไว้ ก็จะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกันกับผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ กฎหมายไม่ได้กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่และความรับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เช่น ไม่มีหน้าที่เกี่ยวกับเหตุหรือฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจึงไม่มีหน้าที่ขอความยินยอมหรือหาเหตุตามกฎหมาย รวมทั้งไม่มีหน้าที่แจ้งรายละเอียด (Privacy Notice) แก่เจ้าของข้อมูลส่วนบุคคล แต่หากเป็นกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลเข้าไปเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ผู้ประมวลผลข้อมูลส่วนบุคคล อาจมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในกรณีดังกล่าว

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) คือ บุคลากรที่องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลแต่งตั้งขึ้น เพื่อปฏิบัติหน้าที่ตามกฎหมาย บุคคลดังกล่าว ไม่ใช่เจ้าหน้าที่รัฐ

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจแต่งตั้งจากบุคลากรภายในองค์กรก็ได้ (Insource DPO) เช่น พนักงาน ลูกจ้าง หรือแต่งตั้งบุคคลภายนอก (outsource DPO) เข้ามาดำรงตำแหน่งดังกล่าวก็ได้ ขึ้นอยู่กับนโยบายและแนวทางในการบริหารขององค์กร

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กฎหมายไม่ได้กำหนดว่า องค์กรจะต้องแต่งตั้งใครคนหนึ่งมาดำรงตำแหน่งดังกล่าว และไม่ได้จำกัดจำนวนของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเอาไว้ ในทางปฏิบัติจึงสามารถแต่งตั้งเป็นคณะทำงานขึ้นมาดำรงตำแหน่งดังกล่าวได้

คุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ปัจจุบัน ยังไม่ได้มีการกำหนดไว้โดยชัดเจน ต้องรอคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยคำนึงถึงความรู้ ความเชี่ยวชาญ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (ทั้งนี้ ความรู้ความเชี่ยวชาญที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ความรู้ด้านกฎหมาย ความรู้เกี่ยวกับการประกอบธุรกิจ ความรู้เกี่ยวกับการบริหารจัดการทรัพยากรบุคคล ความรู้เกี่ยวกับการตลาด เป็นต้น)

องค์กรใดบ้างที่จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

องค์กรที่อยู่ในสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้ มีน้าที่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1) หน่วยงานของรัฐ ตามที่ประกาศกำหนด

2) การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด

ตัวอย่างเช่น บริษัทประกัน, ธุรกิจ E-Market Place เป็นต้น

3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)

ตัวอย่างเช่น โรงพยาบาล สถานพยาบาล เป็นต้น

มาตรา 41 ***อยู่ระหว่างรอคณะกรรมการประกาศกำหนดรายละเอียด

ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

1.  หน่วยงานของรัฐ

2.  การดำเนินการต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่**มีข้อมูลส่วนบุคคลเป็นจำนวนมาก**

3.  **กิจกรรมหลัก**เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม**มาตรา 26**

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ตามกฎหมาย ดังนี้

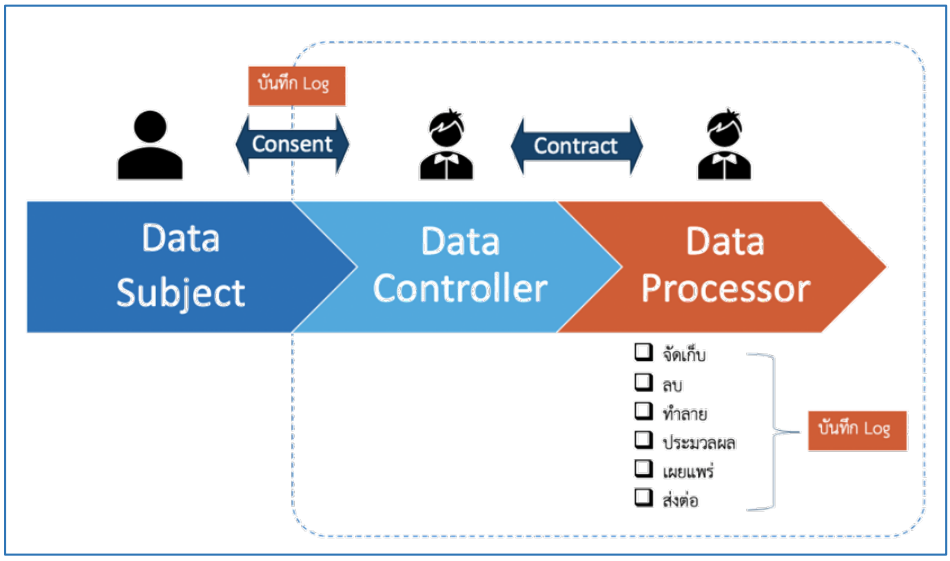
1. ให้คำแนะนำ เกี่ยวกับการประกอบกิจการให้สอดคล้องกับหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม ใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล โดยดูแลการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมาย และนโยบายคุ้มครองข้อมูลส่วนบุคคลที่องค์กรได้ประกาศใช้

3. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย โดยหากเจ้าของข้อมูลส่วนบุคคลได้ร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ปฏิบัติหน้าที่ไม่ถูกต้องตามกฎหมาย เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการประสานงานกับบุคคลที่เกี่ยวข้อง และให้คำแนะนำแก่องค์กรเกี่ยวกับการปฏิบัติให้สอดคล้องต่อกฎหมาย

4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

สรุปความสัมพันธ์ระหว่าง เจ้าของข้อมูลส่วนบุคคล / ผู้ควบคุมข้อมูลส่วนบุคคล / ผู้ประมวลผลข้อมูลส่วนบุคคล และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีลักษณะดังนี้



โทษตามกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดความผิดและโทษตามกฎหมายกรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้กระทำการฝ่าฝืนกฎหมายไว้เป็น 3 ส่วน คือ

- ความรับผิดทางแพ่ง (มาตรา 77-78)

- ความรับผิดทางอาญา (มาตรา 79-81)

- มาตรการทางปกครอง (มาตรา 82-90)

มาตรการลงโทษ	อัตราโทษ	มาตรา
มาตรการทางแพ่ง	ค่าเสียหายตามจริง สินไหมทดแทน สูงสุด 2 เท่า ของค่าเสียหายตามจริง <อายุความ 3 ปี นับแต่รู้เรื่อง + รู้ตัว หรือ 10 ปี นับแต่ละเมิด>	มาตรา 77,78
มาตรการทางอาญา	อัตราโทษจำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ <ความผิดอันยอมความได้>	มาตรา 79,80
มาตรการทางปกครอง	ปรับไม่เกิน 5,000,000 บาท	มาตรา 82-90

ถ้าผู้กระทำผิดเป็นนิติบุคคล
กรรมการ / ผู้จัดการ / ผู้สั่ง / บุคคลที่รับผิดชอบในการดำเนินงาน / บุคคลที่มีหน้าที่สั่งการ ต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนที่พระราชบัญญัตินี้มีผลใช้บังคับ

การเก็บรวบรวม และใช้ข้อมูลส่วนบุคคล ที่มีการเก็บรวบรวมไว้ก่อนวันที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ (ตาม พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (ฉบับที่ 2) พ.ศ.2564 ได้เลื่อนการบังคับใช้กฎหมายฉบับนี้ออกไป โดยจะมีผลใช้บังคับแบบเต็มรูปแบบในวันที่ 1 มิถุนายน 2565)

การจะพิจารณาว่า ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไว้ก่อนที่กฎหมายใช้บังคับ จะต้องดำเนินการอย่างไรต่อไป มี 3 เรื่อง ที่จะต้องทำความเข้าใจในเบื้องต้น

เรื่องที่หนึ่ง : ข้อมูลดังกล่าว เป็นข้อมูลส่วนบุคคลหรือไม่ และเป็นข้อมูลเกี่ยวกับอะไรบ้าง

หากข้อมูลที่มีการเก็บรวบรวม ไม่ใช่ข้อมูลส่วนบุคคล ไม่จำเป็นต้องกังวลว่าจะต้องปฏิบัติตามกฎหมายฉบับนี้หรือไม่ แต่ถ้าข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคล เราจะต้องพิจารณาให้รอบคอบว่า ข้อมูลส่วนบุคคลที่เก็บมานั้น เป็นข้อมูลอะไร เป็นข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data) เสียก่อน เพื่อให้รับรู้รับทราบว่าจะต้องดำเนินการกับข้อมูลดังกล่าวเช่นไร

เรื่องที่สอง : ข้อมูลส่วนบุคคลนั้น เป็นข้อมูลของบุคคลใด

การพิจารณาว่าในหน่วยงานมีการจัดเก็บข้อมูลส่วนบุคคลเอาไว้หรือไม่ และใครเป็นเจ้าของข้อมูลส่วนบุคคลชุดดังกล่าว เพราะ เจ้าของข้อมูลส่วนบุคคล แม้จะเป็นบุคคลที่ได้รับความคุ้มครองตามกฎหมายเช่นเดียวกัน แต่ในความเป็นจริง สถานะทางกฎหมายของบุคคลแต่ละประเภท เกี่ยวข้องกับฐานทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลที่แตกต่างกัน

เรื่องที่สาม : วัตถุประสงค์ในการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดหลักเกณฑ์เอาไว้ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ ให้เจ้าของข้อมูลส่วนบุคคลรับทราบ ซึ่งหากวัตถุประสงค์เดิมที่เก็บรวบรวมข้อมูลส่วนบุคคลเอาไว้ เป็นอย่างไร ก็ให้ประมวลผลได้ตามนั้น หากจะใช้ข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์เดิมที่เก็บรวบรวมข้อมูลส่วนบุคคลไว้ จะต้องอาศัยฐานทางกฎหมายอื่นในการเก็บรวบรวมข้อมูลส่วนบุคคลเพิ่มเติม

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคล สามารถ เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวนั้นได้ต่อไป โดยมีเงื่อนไข 3 ประการ คือ

เงื่อนไขข้อที่หนึ่ง : การเก็บรวบรวม และใช้ จะต้องเป็นไปตามวัตถุประสงค์เดิม

นาย A เป็นพ่อค้าออนไลน์ ขายสินค้าให้ นาง B ในการส่งสินค้าให้กับนาง B นาย A จำเป็นต้องขอข้อมูลส่วนบุคคล อาทิ ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เพื่อใช้ในการส่งสินค้าให้กับนาง B

หากการซื้อขายสินค้าออนไลน์ดังกล่าว เกิดขึ้นก่อนที่ กฎหมายคุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับ ต่อมา นาง B มาซื้อสินค้าจากนาย A ก็สามารถใช้ข้อมูลส่วนบุคคล ตามวัตถุประสงค์เดิม คือ การซื้อขายสินค้า-ส่งสินค้า นาย A จะเอาข้อมูลส่วนบุคคลของนาง B มาใช้ในการทำการตลาด หรือ ส่งรายละเอียดเกี่ยวกับโปรโมชั่นสินค้าใหม่ให้แก่นาง B ไม่ได้ เนื่องจาก เป็นการนำข้อมูลส่วนบุคคลของผู้อื่นมาใช้ นอกกรอบวัตถุประสงค์เดิม

เงื่อนไขข้อที่สอง : กำหนดวิธีการยกเลิกความยินยอม

ก่อนที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล จะประกาศใช้บังคับ เดิมผู้ควบคุมข้อมูลส่วนบุคคล อาจไม่เคยขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลมาก่อน แต่เมื่อกฎหมายมีผลใช้บังคับ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายในการกำหนดวิธีการยกเลิกความยินยอม

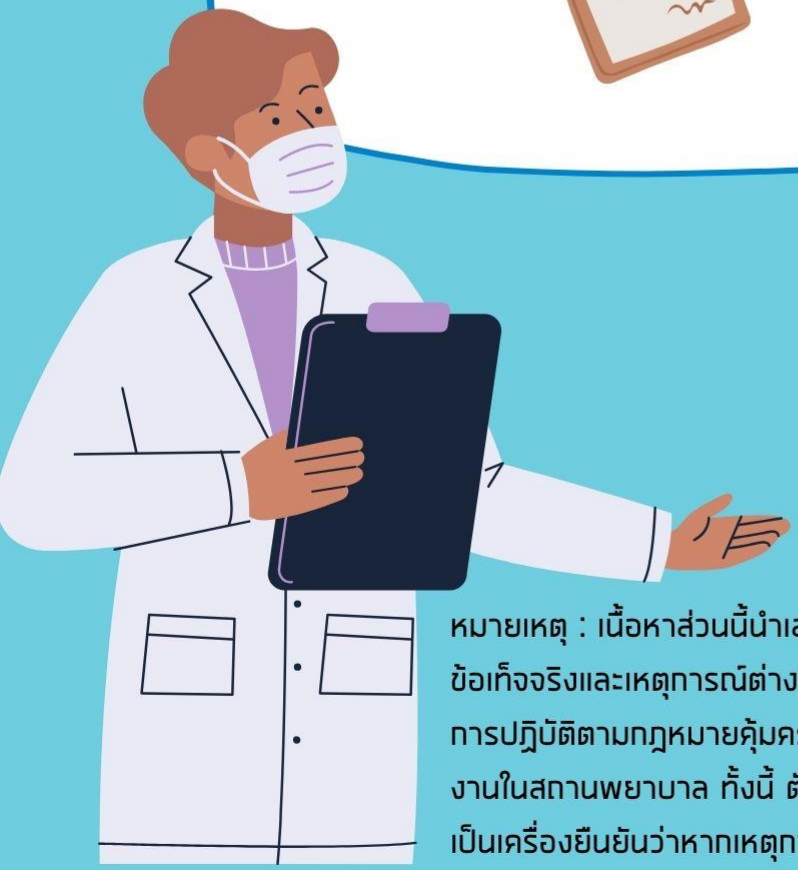
ทั้งนี้ ณ ขณะจัดทำหนังสือนี้ (วันที่..... ตุลาคม 2564) ยังไม่มีการออกข้อกำหนดใด ๆ ว่า การกำหนดวิธีการยกเลิกความยินยอม จะต้องดำเนินการด้วยวิธีใด ในกรณีทั่วไป หากเดิม ผู้ควบคุมข้อมูลส่วนบุคคลเคยติดต่อกับเจ้าของข้อมูลส่วนบุคคลในช่องทางไหน ก็ใช้ช่องทางดังกล่าวได้ เช่น เมื่อก่อนติดต่อกันทางโทรศัพท์ การแจ้งวิธีในการถอนความยินยอม ก็สามารถดำเนินการผ่านทางโทรศัพท์ได้ เป็นต้น

หมายเหตุ: รอความชัดเจนของกฎหมายและรายละเอียดของขั้นตอนในการดำเนินการต่าง ๆ ตามกฎหมายต่อไป

เงื่อนไขข้อที่สาม : ต้องเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม และใช้ข้อมูลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

เนื้อหาส่วนที่ 2

กรณีศึกษาน่ารู้



หมายเหตุ : เนื้อหาส่วนนี้นำเสนอกรณีศึกษาน่ารู้ที่เกิดขึ้นในต่างประเทศ โดยการสรุปย่อข้อเท็จจริงและเหตุการณ์ต่าง ๆ เพื่อใช้เป็นตัวอย่างทำความเข้าใจแสดงมุมมองเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับโรงพยาบาลและผู้ปฏิบัติงานในสถานพยาบาล ทั้งนี้ ตัวอย่างต่าง ๆ มิได้มุ่งหมายถึงกรณีในประเทศไทย และมิได้เป็นเครื่องยืนยันว่าหากเหตุการณ์ตามกรณีศึกษาเกิดขึ้นในประเทศไทย คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของไทย หรือหน่วยงานอื่นที่เกี่ยวข้องจะมีความเห็นในลักษณะทำนองเดียวกัน

กรณีศึกษา 1 คดีแรกของการสั่งปรับโรงพยาบาล ตามกฎหมาย GDPR

(GDPR: Centro Hospitalar Barreiro Montijo Ankita Sharma)

สาระสำคัญ

สถานประกอบการโรงพยาบาลของรัฐในโปรตุเกส Centro Hospitalar Barreiro Montijo (CHBM) ถูกสั่งปรับเป็นเงินจำนวน 400,000 ยูโร เนื่องจากมีการกระทำที่ละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ซึ่งเป็นกรณีศึกษาแรกในประเทศโปรตุเกส นับแต่กฎหมาย GDPR มีผลใช้บังคับ โดยตามข้อเท็จจริง CHBM มีความบกพร่องในเรื่องแนวปฏิบัติในการบริหารจัดการข้อมูลของโรงพยาบาล ซึ่งมีการเปิดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และไม่จำกัดให้แก่บุคคลภายนอก ทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลอ่อนไหว ซึ่งนำไปสู่การตรวจสอบ โดยทางโรงพยาบาลได้ต่อสู้ว่า ตนใช้บริการการประมวลผลข้อมูลภายนอก อย่างไรก็ตาม คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของโปรตุเกส วินิจฉัยว่า โรงพยาบาลมีความรับผิดชอบที่จะต้องทำให้แน่ใจว่า ระบบการใช้งานสอดคล้องและปฏิบัติตามแนวทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป[4]

First GDPR fine in Portugal issued against hospital for three violations by Ana Monteiro (Jan 3 2019)

Centro Hospitalar Barreiro Montijo has been fined 400,000 euros for violating the General Data Protection Regulation. The country's supervisory authority, Comissão Nacional de Protecção de Dados, found that there were three violations of the GDPR. First was a violation of Article 5(1)(c), a minimization principle, by allowing indiscriminate access to an excessive number of users, and a

[4] GDPR Case Study: Centro Hospitalar Barreiro Montijo
http://cs.brown.edu/courses/csci2390/2019/assign/gdpr/asharma7-hospital-barreiro.pdf

violation of Article 83(5)(a) a violation of the processing basic principles. For those, the fine was 150,000 euros.

The second, a violation of integrity and confidentiality as a result of non-application of technical and organizational measures to prevent unlawful access to personal data under Article 5(1)(f), and also of Article 83(5)(a), a violation of the processing basic principles. There, the fine was 150,000 euros.

Both of the above were punishable with a fine of up to 20 million euros or 4 percent of the total annual turnover.

Finally, the CNPD fined under Article 32(1)(b), the incapacity of the defendant to ensure the continued confidentiality, integrity, availability and resilience of treatment systems and services as well as the non-implementation of the technical and organizational measures to ensure a level of security adequate to the risk, including a process to regularly testing, assessing and evaluating the technical and organizational measures to ensure the security of the processing. There the fine was for 100,000 euros, though the maximum fine was 10 million euros to 2 percent of the total annual turnover.

The defense submitted by the hospital referred that the CNPD could not be considered as the supervisory authority as per Article 51 because it had not yet been appointed formally. To this, CNPD responded that it is, for all purposes, the national authority which has the power to control and supervise the compliance in terms of data protection in accordance with the current Portuguese Data Protection Law. Also, among its arguments was that the hospital used the IT system provided to public hospitals by the Portuguese Health Ministry and not its own systems.

Some facts considered proven by the CNPD:

- There was no document containing the correspondence between the functional competences of the users and the profiles for access to the information (including to clinical information).
- There was also no document defining the rules for creating users of the hospital's information system.
- Nine technical employees enjoyed the level of access reserved for the medical group, which resulted in the indiscriminate possibility of such employees consulting the clinical processes of all hospital users.
- Existence of access credentials which allowed any doctor, regardless of his/her specialty, to access at any time the data of the clients of a hospital. This was considered as violating the principle of "need to know" and the principle of "minimization of data."
- There were 985 users associated with the profile "doctor," but in the official hospital human resources charts there are only 296 doctors in that hospital.
- Maintenance of useless profiles for doctors who no longer provide services to the hospital.
- There were only 18 user accounts that were inactive and the last one was deactivated in November 2016.
- The defendant acted in a free and voluntary way and consciously knowing that its acts are prohibited by law.

When determining the amount of the fine, which was relatively low considering what it could have been, the CNPD considered the following, in accordance with Article 83(1)(a-k):

- The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing as well as the number of data subjects affected. It was also considered as relevant the fact that the personal data involved were special categories of data, including health data which increased significantly the risk of damages to the data subjects.

- Possible fraud: the defendant represented the practice of misconduct as a possible consequence of the conduct and conformed to it.

- The defendant's initiative to mitigate the damages suffered by the data subjects.

- The degree of responsibility of the defendant, taking into account the technical and organizational measures implemented.

- There were no previous infractions.

- Degree of cooperation with the CNPD in order to remedy the infringement and mitigate its possible negative effects.

- How the CNPD learned of the infraction, in that it was not communicated by the hospital but rather was known through the media and later confirmed by the CNPD inspection.

When determining the amount of the penalty the CNPD also considered the fact that the defendant took measures to regularize the situation.

The striking fact about this fine is that the CNPD acted upon a newspaper article and not on a complaint. From this we consider that it was particularly relevant to the CNPD that there were no documented procedures for access to the data, but also that the data involved were special categories of data.

It is also worth mentioning that in the first draft of the proposed new data protection law, there were no penalties applicable to the public entities. This was referred to by the CNPD: That it was not in line with the Portuguese legislative tradition. This fine is in line with that opinion. In fact, according to the CNPD, to exempt public entities from the application of the fines violates the principle of equality and weakens the protection of citizens' fundamental rights.

The decision was not published in the CNPD site, which obviously does not contribute to promote public awareness and understanding of the risks, rules, safeguards in relation to the processing, as provided for in Article 57 of the GDPR.

Source https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/

กรณีศึกษา 2 ความเสี่ยงจากการเข้าถึงข้อมูลเวชระเบียน

บริบท

งานสำคัญประการหนึ่งในการตรวจสอบการั่วไหลข้อมูลส่วนบุคคลของคนไข้ในโรงพยาบาล คือ การตรวจสอบระบบการจัดเก็บข้อมูลเวชระเบียน หรือห้องสมุดเวชระเบียนของโรงพยาบาล การรักษาความปลอดภัยเวชระเบียนของคนไข้เป็นเรื่องที่สำคัญมาก โดยปกติที่จัดเก็บข้อมูลเวชระเบียนจะตั้งอยู่ในส่วนหนึ่งของสถานพยาบาลที่ผู้ป่วย หรือสมาชิกคนอื่นๆ หรือประชาชนไม่สามารถเข้าถึงได้ โดยห้องสมุดเวชระเบียนมักจะมีพนักงานประจำในช่วงเวลาทำการ และขึ้นอยู่กับขนาดของโรงพยาบาล จำนวนเจ้าหน้าที่อาจมีตั้งแต่สี่หรือห้าคน และอาจมากถึงยี่สิบคน ในโรงพยาบาลขนาดใหญ่บางแห่ง โดยมีเจ้าหน้าที่ประจำห้องสมุดเวชระเบียนตลอดเวลา รวมทั้งวันหยุดสุดสัปดาห์และข้ามคืน โดยขนาดพื้นที่จัดเก็บข้อมูลเวชระเบียนทางกายภาพอาจแตกต่างกันไป อย่างไรก็ตาม แม้แต่โรงพยาบาลที่มีพื้นที่จัดเก็บจำกัด ก็มักจะมีแผนภูมิผู้ป่วยหลายพันรายในห้องสมุดเวชระเบียน และมีบ้างที่พบว่า โรงพยาบาลบางแห่งจัดเก็บข้อมูลเวชระเบียนนอกสถานที่สำหรับเวชระเบียนที่ไม่ได้ใช้งานในช่วงระยะเวลาหนึ่ง

โดยผลจากการตรวจสอบพบว่า ปัญหาหนึ่งที่เกิดการละเมิดข้อมูลส่วนบุคคลของผู้ป่วย มักเกิดจากความประมาทและความหละหลวมในการควบคุมความปลอดภัยของเวชระเบียน กล่าวคือ

ความเสี่ยง 1 ความไม่เข้มงวดในการควบคุมและจำกัดการเข้าถึงห้องสมุดเวชระเบียนโดยเจ้าหน้าที่ของโรงพยาบาลที่ทำงานในส่วนอื่น ๆ ของโรงพยาบาล กล่าวคือ ในโรงพยาบาลแห่งหนึ่ง พบว่า ห้องไปรษณีย์ภายในอยู่ในพื้นที่บริเวณเดียวกับหอสมุดเวชระเบียน ในกรณีดังกล่าว เจ้าหน้าที่ของโรงพยาบาลที่มีสิทธิเข้าใช้ห้องบริการไปรษณีย์ ก็สามารถเข้าถึงห้องสมุดเวชระเบียนได้เช่นกัน และอีกกรณีหนึ่ง พนักงานทุกคนในโรงพยาบาลแห่งหนึ่งที่มีบัตรรูดประตู จะสามารถเข้าถึงทุกพื้นที่ของโรงพยาบาลได้ ซึ่งรวมถึงการเข้าถึงห้องสมุดเวชระเบียนด้วย

ผู้ตรวจพบสถานการณ์ในโรงพยาบาลสองแห่งซึ่งมีพนักงานมากถึงสามพันคนเข้าถึงพื้นที่เวชระเบียนของโรงพยาบาลในครั้งเดียว และพนักงานอีกกว่าหกร้อยคนได้เข้าถึงพื้นที่เวชระเบียนในตัวอย่างอื่น ข้อเท็จจริงนี้แสดงให้เห็นว่า ขาดการจำกัดบุคคลที่สามารถเข้าถึงห้องเก็บเอกสารเวชระเบียน เจ้าหน้าที่ที่ไม่จำเป็นต้อง

เกี่ยวข้อง สามารถเข้าถึงพื้นที่เก็บเวชระเบียนได้ ก่อให้เกิดความเสี่ยงที่ร้ายแรง หากเจ้าหน้าที่สามารถเข้าถึงข้อมูล อาจเกิดการสอดแนม อ่านข้อมูลทางการแพทย์ของสมาชิกในครอบครัว เพื่อน หรือผู้อื่น

คำแนะนำ

- ควรมีการควบคุมที่มีประสิทธิภาพเพื่อจำกัดการเข้าถึงห้องสมุดเวชระเบียนของเจ้าหน้าที่ไว้เฉพาะเจ้าหน้าที่ของโรงพยาบาลที่มีหน้าที่ในการเข้าถึงดังกล่าว จำเป็นอย่างยิ่งที่โรงพยาบาลทุกแห่งต้องทบทวนการควบคุมความปลอดภัยในปัจจุบันเพื่อระบุจุดอ่อนที่อาจเกิดขึ้น และดำเนินการแก้ไขเพื่อให้การควบคุมการเข้าออกเป็นไปอย่างเข้มงวดสูงสุด
- ควรจำกัดจำนวนเจ้าหน้าที่ที่สามารถเข้าถึงห้องสมุดเวชระเบียนให้น้อยที่สุด เจ้าหน้าที่หน่วยอื่นหรือแผนกอื่น ๆ ของโรงพยาบาลไม่ควรตั้งอยู่ในพื้นที่เดียวกัน เว้นแต่จะมีมาตรการควบคุมการเข้าออกที่เข้มงวดเพื่อจำกัดการเข้าถึงบริการทางการแพทย์ของพนักงานเจ้าหน้าที่ห้องเวชระเบียน

ความเสี่ยง 2 จากการตรวจสอบ พบว่า มีโรงพยาบาลเพียงไม่กี่แห่งเท่านั้นที่มีการบันทึกการเข้าใช้ห้องสมุดเวชระเบียนของเจ้าหน้าที่ได้ ส่วนที่เหลือไม่มีวิธีการตรวจสอบการเข้าถึงของพนักงานที่ไม่ได้รับอนุญาต การเข้าถึงพื้นที่ห้องเก็บเวชระเบียนของโรงพยาบาล โดยไม่ได้รับการตรวจสอบซึ่งมีข้อมูลส่วนบุคคลที่ละเอียดอ่อนที่สุดของผู้ป่วยหลายพันรายทำให้มีความเสี่ยงสูงในการเข้าถึงโดยไม่ได้รับอนุญาตโดยพนักงานที่ไม่มีเหตุสมควรในการเข้าพื้นที่ เจ้าหน้าที่ทราบดีว่าการเข้าถึงห้องเวชระเบียนโดยไม่มีการตรวจสอบการเข้าถึงพื้นที่นั้น ผู้เข้าถึงอาจเข้าถึงด้วยจุดประสงค์ที่ชั่วร้าย

คำแนะนำ

- ควรมีขั้นตอนการทำงานเพื่อสร้างรายงานการเข้าถึงเป็นประจำในส่วนที่เกี่ยวกับการเข้าถึงห้องเวชระเบียนของเจ้าหน้าที่ โดยรายงานการเข้าถึงเหล่านี้ต้องได้รับการตรวจสอบเป็นประจำเพื่อตรวจสอบว่ารูปแบบการเข้าถึงที่น่าสงสัยเกิดขึ้นหรือไม่
- จำเป็นอย่างยิ่งที่เจ้าหน้าที่โรงพยาบาลจะต้องทราบว่าห้องสมุดเวชระเบียนโดยทั่วไปอยู่นอกขอบเขตสำหรับเจ้าหน้าที่ทุกคน ยกเว้นผู้ที่มีหน้าที่และได้รับอนุญาตให้เข้าถึงเท่านั้น เพื่อยับยั้งการเข้าถึงโดยไม่จำกัด พนักงานทุกคนจะต้องรับทราบว่ามีการตรวจสอบการเข้าถึงห้องสมุดเวชระเบียนเป็นประจำ

● เพื่อขัดขวางไม่ให้เจ้าหน้าที่เข้าถึงข้อมูลเวชระเบียนผู้ป่วยโดยไม่มีเหตุผล โรงพยาบาลควรกำหนดนโยบายที่ถือว่าการเข้าถึงโดยไม่ได้รับอนุญาตนั้นเป็นเรื่องทางวินัย

ความเสี่ยง 3 พบว่า มีแนวทางปฏิบัติที่หลากหลายในโรงพยาบาลที่อนุญาตให้เจ้าหน้าที่เข้าถึงข้อมูลเวชระเบียน 'นอกเวลาทำการ' โดยไม่มีการเก็บบันทึกเพื่อบันทึกรายละเอียดของผู้ที่เข้ามาในห้องสมุดหรือรายละเอียดว่าเอาแผนภูมิเวชระเบียนใดออกไป หรือมีหลักฐานเพียงเล็กน้อยที่บ่งชี้ถึงข้อจำกัดใดๆ เกี่ยวกับเจ้าหน้าที่ที่สามารถเข้าถึงห้องสมุด "หลังเวลาทำการ"

คำแนะนำ

● สำหรับการเข้าถึงห้องสมุดเวชระเบียน "หลังเวลาทำการ" ควรใช้สมุดบันทึกหรือสิ่งที่คล้ายกันซึ่งเจ้าหน้าที่ที่เข้าถึงห้องสมุดต้องลงชื่อเข้าใช้และออกจากระบบ ในสมุดบันทึกเล่มนี้ ควรบันทึกตามหมายเลขแผนภูมิเวชระเบียน วันที่ และเวลา รายละเอียดของแผนภูมิเวชระเบียนที่ลบออกจากห้องสมุด

● พนักงานที่ได้รับอนุญาตให้เข้าถึงห้องสมุดเวชระเบียนไม่ควรนำเจ้าหน้าที่ที่ไม่ได้รับอนุญาตเข้ามาในห้องสมุดเวชระเบียนด้วย

ความเสี่ยง 4 ห้องสมุดเวชระเบียนในโรงพยาบาลส่วนใหญ่ที่ตรวจสอบ พบว่า ไม่มีระบบแจ้งเตือนที่จะแจ้งไปยังผู้เกี่ยวข้อง หากพบว่ามีการเข้าถึงเอกสาร แก้ไข หรือลบข้อมูลเวชระเบียนในระบบ หรือไม่ได้ส่งคืนข้อมูลเวชระเบียน

คำแนะนำ

● ควรกำหนดขั้นตอนระบบการจัดการผู้ป่วยแบบอิเล็กทรอนิกส์เพื่อสร้างรายงานเป็นประจำเกี่ยวกับแผนภูมิทางการแพทย์ที่ยังไม่ได้ส่งกลับไปยังห้องสมุดเวชระเบียนภายในช่วงระยะเวลาหนึ่ง

● จำเป็นอย่างยิ่งที่รายงานเหล่านี้ต้องได้รับการตรวจสอบเพื่อพยายามกำหนดตำแหน่งปัจจุบันของแผนภูมิทางการแพทย์ที่เกี่ยวข้อง และเพื่อให้สามารถอัปเดตระบบการดูแลผู้ป่วยแบบอิเล็กทรอนิกส์เพื่อสะท้อนตำแหน่งปัจจุบันของแผนภูมิผู้ป่วย

ความเสี่ยง 5

รถเข็นแบบเปิดด้านบน (สี่ล้อ) มักใช้ในการขนส่งแผนภูมิผู้ป่วยจากห้องสมุดเวชระเบียนไปยังแผนกต่าง ๆ ของโรงพยาบาลตามที่ต้องการ โรงพยาบาลส่วนใหญ่รายงานว่า แนวปฏิบัติทั่วไปในสถานการณ์นี้คือพนักงานที่ควบคุมรถเข็นคว่ำหน้าแผนภูมิลงเพื่อให้แน่ใจว่าข้อมูลส่วนตัวบนปกด้านหน้าจะอ่านไม่ได้ แม้จะมีการปฏิบัติเช่นนี้ แผนภูมิผู้ป่วยที่ขนส่งในรถเข็นแบบเปิดโล่งจากห้องเวชระเบียนไปยังตำแหน่งอื่นของโรงพยาบาล ผ่านทางเดิน ลิฟต์ และหอผู้ป่วยมีความเสี่ยงเป็นพิเศษต่อการสัมผัส ในพื้นที่สาธารณะที่มีผู้คนพลุกพล่านในโรงพยาบาล มีความเสี่ยงสูงที่เจ้าหน้าที่ที่ควบคุมรถเข็นจะเสียสมาธิหรือมีส่วนร่วมอื่น ๆ ดังนั้นจึงทำให้เกิดคำถามเกี่ยวกับความปลอดภัยของแผนภูมิผู้ป่วย

คำแนะนำ

- รถเข็นที่ใช้ในการขนส่งแผนภูมิทางการแพทย์ทั่วทั้งสถานพยาบาลควรได้รับการคุ้มครองอย่างปลอดภัยเพื่อปกป้องข้อมูลผู้ป่วยที่ถืออยู่ในแผนภูมิทางการแพทย์จากการถูกมองเห็นหรือเข้าถึงโดยบุคคลที่สาม
- ไม่ควรเก็บแผนภูมิทางการแพทย์ บันทึกเวชระเบียนไว้นอกช่องเก็บสัมภาระของรถเข็นในขณะที่รถเข็นอยู่ระหว่างการขนส่ง
- ในระดับทั่วไปควรมีขั้นตอนที่เข้มงวดเกี่ยวกับการเคลื่อนไหวของแผนภูมิเวชระเบียนทั่วทั้งโรงพยาบาล เพื่อให้แน่ใจว่าเจ้าหน้าที่จะปกป้องข้อมูลส่วนบุคคลในแผนภูมิทางการแพทย์ไม่ให้บุคคลอื่นเห็น

ความเสี่ยง 6 พบว่า มีโรงพยาบาลบางแห่ง ไม่มีการติดตามการเคลื่อนไหวของแผนภูมิทางอิเล็กทรอนิกส์ ในทางกลับกัน การตรวจสอบการเคลื่อนไหวของแผนภูมิใช้ระบบแมนนวลในการอัปเดตการ์ดติดตามในห้องสมุดเวชระเบียนเท่านั้น ในกรณีหนึ่ง การอัปเดตการ์ดติดตามถูกกระตุ้นโดยการโทรศัพท์ไปยังห้องสมุดเวชระเบียนจากเจ้าหน้าที่ที่เกี่ยวข้องในการเคลื่อนไหวของแผนภูมิในแผนกต่างๆ ของโรงพยาบาล ระบบที่ดำเนินการด้วยตนเองดังกล่าวนี้ มีความเสี่ยงอย่างมากที่การติดตามแผนภูมิอาจไม่ทันสมัย พร้อมความเสี่ยงเพิ่มเติมที่หากจำเป็นต้องใช้แผนภูมิอย่างเร่งด่วน ตำแหน่งปัจจุบันอาจไม่สามารถระบุได้อย่างรวดเร็ว

คำแนะนำ

- ระบบแบบแมนนวลสำหรับการติดตามแผนภูมิผู้ป่วยควรแทนที่ด้วยระบบติดตามอิเล็กทรอนิกส์ ซึ่งรวมคุณลักษณะต่างๆ เช่น บาร์โค้ด ที่มีความสามารถในการระบุตำแหน่งของแผนภูมิเวชระเบียนผู้ป่วยทั้งหมดได้อย่างถูกต้องตลอดเวลา

กรณีศึกษา 3 ความปลอดภัยของข้อมูลและการรั่วไหลของข้อมูล

บริบท

โรงพยาบาลมักมีการควบคุมที่เข้มงวดเพื่อจำกัดการเข้าถึงของสาธารณะในบางส่วนของสถานพยาบาล อย่างไรก็ตาม มีโรงพยาลบางแห่งอาจไม่ได้เข้มงวดมากพอ เช่น ในพื้นที่ทำงาน (work station) ที่มีคอมพิวเตอร์ อาจขาดขั้นตอนการรักษาความปลอดภัยที่เหมาะสม หรือขาดมาตรการในการปกป้องข้อมูลส่วนบุคคลจำนวนมาก และส่งผลให้ข้อมูลส่วนบุคคลอ่อนไหวรั่วไหล

พบว่า ในโรงพยาบาลแห่งหนึ่งบนทางเดินของหอผู้ป่วยสาธารณะ แผนภูมิผู้ป่วยของผู้ป่วยปัจจุบันถูกเก็บไว้ในตู้กระจกที่มีการติดล็อก อย่างไรก็ดี พบว่าแผนภูมิทางการแพทย์ของผู้ป่วยของผู้ป่วยที่ออกจากโรงพยาบาลถูกละเลยที่ด้านบนของตู้กระจก ในวอร์ดเดียวกัน โดยผู้ตรวจสอบได้สังเกตพบกล่องกระดาษแข็งสองกล่องที่มีแผนภูมิผู้ป่วยของผู้ป่วยที่ออกจากโรงพยาบาล แผนภูมิเหล่านี้อยู่ระหว่างกำลังรอการส่งต่อไปยังห้องสมุดเวชระเบียน และผู้ตรวจสอบได้รับแจ้งว่าเป็นวิธีปฏิบัติที่แผนภูมิของผู้ป่วยที่ออกจากโรงพยาบาลจะถูกจัดเก็บในลักษณะนี้ในวอร์ดนานถึงหนึ่งสัปดาห์ ตัวอย่างเหล่านี้แสดงให้เห็นว่า แผนภูมิผู้ป่วยสามารถเข้าถึงได้ง่ายโดยผู้ป่วย ผู้เยี่ยมชม หรือสมาชิกคนอื่นๆ ในที่สาธารณะ

ความเสี่ยง 1 จากการตรวจสอบ พบว่า การตรวจสอบบางรายการระบุจุดอ่อนที่เกี่ยวข้องกับการควบคุมการเข้าถึงประตูบางบานที่นำไปสู่พื้นที่จำกัด ในบางกรณีพบว่า บันทึกการเข้าออกประตูได้รับการตรวจสอบไม่เพียงพอ และพบว่า พนักงานทุกคนในโรงพยาบาลแห่งหนึ่งที่ถือบัตรรูดประตูเข้าถึงทุกพื้นที่ของโรงพยาบาลนั้นได้ จึงเป็นที่สงสัยว่าทำไมเจ้าหน้าที่แผนกฉุกเฉินสามารถเข้าถึงแผนกผู้ป่วยนอก หรือแผนกผู้ป่วยนอกได้)

ความเสี่ยงนี้เกี่ยวข้องกับความปลอดภัยของประตูและการเข้าถึงบัตรรูดในระดับกว้าง อาจส่งผลอันตรายต่อการรักษาความปลอดภัยของแผนภูมิผู้ป่วยที่อาจถูกจัดเก็บไว้ในพื้นที่ที่ได้รับผลกระทบ และทำให้ข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่ละเอียดอ่อนมีความเสี่ยงที่จะไม่ได้รับอนุญาตให้เข้าถึง

คำแนะนำ

● ประตูทางเข้าทุกพื้นที่ของโรงพยาบาลที่ผู้ป่วยหรือประชาชนทั่วไปไม่มีทางเข้า ควรได้รับการรักษาความปลอดภัยอย่างเหมาะสมตลอดเวลา เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึง

● การเข้าใช้ด้วยบัตรรูด (Swipe card access) ต้องมีการวางแผนอย่างเหมาะสมและตรวจสอบทั่วทั้งโรงพยาบาล เพื่อให้แน่ใจว่าพนักงานถูกจำกัดตามบทบาทหน้าที่การงาน จากการเข้าไปในพื้นที่ที่ไม่จำเป็นต้องเข้าถึงธุรกิจ

● ในกรณีที่มีการใช้ระบบควบคุมการเข้าออกด้วยบัตรรูด ควรมีการตรวจสอบสิ่งเหล่านี้เป็นประจำ (อย่างน้อยทุก ๆ หกเดือน) เพื่อให้แน่ใจว่ามีเพียงเจ้าหน้าที่ที่มีความจำเป็นต้องเข้าถึงพื้นที่ของโรงพยาบาลที่เกี่ยวข้องเท่านั้นที่สามารถทำเช่นนั้นได้

● ควรมีการดำเนินการตามขั้นตอนด้านความปลอดภัยเพื่อสร้างบันทึกการเข้าใช้ที่เกี่ยวข้องกับประตูที่นำไปสู่พื้นที่จำกัด บันทึกการเข้าถึงเหล่านี้ควรได้รับการตรวจสอบเป็นประจำเพื่อตรวจหารูปแบบของการเข้าถึงที่ผิดปกติหรือไม่ได้รับอนุญาต

● เมื่อมีการใช้ระบบควบคุมการเข้าออกด้วยคีย์แพด ควรเปลี่ยนรหัสคีย์เป็นระยะๆ

● กลไกการเข้าถึงความปลอดภัยบนประตูควรได้รับการทดสอบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าทำงานได้อย่างถูกต้อง

● ประตูห้องปรึกษาควรปิดตลอดเวลาในขณะที่ผู้ป่วยกำลังเข้ารับการปรึกษาทางการแพทย์ เพื่อปกป้องสิทธิ์ในการปกป้องข้อมูลของตน

● กุญแจของสำนักงานที่ถูกล็อกควรเก็บไว้ในที่ปลอดภัย และห้ามมิให้พนักงานนำกุญแจกลับบ้านเมื่อสิ้นสุดกะ

ความเสี่ยง 2 ความเสี่ยงของคอมพิวเตอร์บางเครื่องจากพื้นที่ทำงาน ในหลายกรณี ข้อมูลส่วนบุคคลบนหน้าจอคอมพิวเตอร์สามารถดูได้โดยผู้สัญจรไปมา เนื่องจากตำแหน่งหลักในการวางตำแหน่งทางกายภาพของหน้าจอคอมพิวเตอร์

คำแนะนำ

- ข้อมูลส่วนบุคคลบนหน้าจอคอมพิวเตอร์ควรถูกซ่อนจากมุมมองของผู้ที่สัญจรไปมาตลอดเวลา

ความเสี่ยง 3 พบว่า มีการขาดการป้องกันทางเทคนิคที่เหมาะสม ส่งผลให้หน้าจอคอมพิวเตอร์แบบไม่ต้องใส่ข้อมูลถูกเปิดทิ้งไว้เป็นระยะเวลานานช่วงที่ไม่มีการใช้งาน ในสถานการณ์เหล่านี้ เจ้าหน้าที่คนอื่น ๆ และประชาชนทั่วไปที่อาจอยู่ในบริเวณใกล้เคียงในขณะนั้น (เช่น ผู้ที่มากับผู้ป่วยในแผนกฉุกเฉิน) อาจสามารถดูข้อมูลส่วนบุคคลบนหน้าจอที่เปิดอยู่ได้ นอกจากนี้ พนักงานที่ไม่ออกจากระบบหลังการใช้งานอาจส่งผลให้ผู้ใช้รายต่อไปป้อนข้อมูลโดยใช้บัญชีผู้ใช้ก่อนหน้า

คำแนะนำ

- ควรใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อให้แน่ใจว่าหน้าจอคอมพิวเตอร์ได้รับการตั้งค่าให้ล็อก และล็อกผู้ใช้โดยอัตโนมัติหลังจากไม่มีการใช้งานเป็นระยะเวลาสั้นๆ ทั้งนี้ ควรพิจารณาถึงความต้องการทางธุรกิจของพื้นที่ทำงานต่าง ๆ ภายในโรงพยาบาลในการกำหนดระยะเวลาการหยุดทำงานสูงสุดที่เหมาะสม ตัวอย่างเช่น ช่วงเวลาหมดเวลาของสถานพยาบาลในสถานพยาบาลอาจแตกต่างกันระหว่าง 1 นาทีในพื้นที่หนึ่งและ 10 นาทีในอีกพื้นที่หนึ่ง ทั้งนี้ขึ้นอยู่กับความต้องการทางธุรกิจของแต่ละพื้นที่
- โปรแกรมรักษาหน้าจอควรปรากฏบนหน้าจอล็อกเพื่อให้แน่ใจว่าไม่มีข้อมูลส่วนบุคคลของผู้ป่วยยังคงปรากฏให้เห็น
- พนักงานควรไม่ได้รับอนุญาตให้เข้าถึงหรือแก้ไขบันทึกข้อมูลส่วนบุคคลในระบบคอมพิวเตอร์ของโรงพยาบาลผ่านบัญชีผู้ใช้อื่น

ความเสี่ยง 4 พบว่า มีการระบุประเด็นที่น่ากังวลหลายประการเกี่ยวกับการจัดการและการจัดเก็บข้อมูลผู้ป่วย ซึ่งรวมถึงการจัดเก็บแผนภูมิผู้ป่วยในตู้เก็บเอกสารที่ไม่ปลอดภัย การจัดเก็บบัตรแผนกฉุกเฉิน (บัตร 'ED') ในแผนกฉุกเฉินโดยไม่มีกำหนดระยะเวลา การจัดเก็บกุญแจของตู้เก็บเอกสารที่ใช้สำหรับการจัดเก็บแผนภูมิผู้ป่วยหรือไฟล์ในสถานที่ที่ไม่ปลอดภัย การใช้ตัวยึดพลาสติกแบบซีทรูติดผนังเพื่อเก็บข้อมูลผู้ป่วย การทิ้งแผนภูมิผู้ป่วยไว้บนชั้นวางหรือโต๊ะนอกห้องให้คำปรึกษาในแผนกผู้ป่วยนอก การทิ้งแผนภูมิ

ผู้ป่วยไว้บนเคาน์เตอร์ในบริเวณแผนกต้อนรับของโรงพยาบาลต่าง ๆ และการทิ้งจดหมายลับไว้ในพื้นที่ที่ไม่มีผู้ดูแล

คำแนะนำ

● ตู้เก็บเอกสารทั้งหมดที่ใช้เก็บแผนภูมิผู้ป่วยหรือข้อมูลส่วนบุคคลอื่น ๆ ของผู้ป่วยควรถูกล็อกอย่างปลอดภัยเพื่อห้ามการเข้าถึงโดยไม่ได้รับอนุญาต

● กุญแจตู้เก็บเอกสารที่ล็อกไว้ควรเก็บไว้ในที่ปลอดภัย และห้ามพนักงานนำกุญแจกลับบ้านเมื่อเลิกกะ

● การ์ด 'ED' ที่สร้างขึ้นเป็นประจำในแผนกฉุกเฉินของโรงพยาบาลเพื่อบันทึกรายละเอียดการเข้าร่วมของผู้ป่วยควรเก็บไว้ในแผนกฉุกเฉินเป็นระยะเวลาที่จำกัด ก่อนส่งไปยังห้องสมุดเวชระเบียนหรือสภาพแวดล้อมที่ปลอดภัยอื่น ๆ เพื่อการจัดเก็บ

● ควรหยุดการจัดเก็บแผนภูมิผู้ป่วยในลักษณะที่ไม่เป็นทางการ หรือในลักษณะที่ไม่มีการป้องกันบนชั้นวางหรือโต๊ะนอกห้องให้คำปรึกษาในขณะที่ผู้ป่วยกำลังรอการเรียกจากทีมแพทย์ ควรมีแนวทางการจัดเก็บไว้ในสภาพแวดล้อมที่ปลอดภัยยิ่งขึ้น ซึ่งไม่เสี่ยงต่อการถูกเข้าถึงโดยบุคคลที่สาม [เป็นตัวอย่างของแนวปฏิบัติที่ดี ในโรงพยาบาลแห่งหนึ่ง ผู้ตรวจประเมินสังเกตว่า แผนภูมิผู้ป่วยถูกเก็บไว้นอกห้องให้คำปรึกษาในถังรถเข็นที่ปลอดภัย ปิดฝาถังรถเข็นไม่ได้ แผนภูมิไม่ถูกเก็บไว้นอกหน่วยซ่องรถเข็น และ ถังขยะอยู่ในระยะที่ปลอดภัยจากผู้ป่วยที่รออยู่ นอกจากนี้ เจ้าหน้าที่ได้ปฏิบัติหน้าที่ในพื้นที่นี้ ซึ่งมีหน้าที่อำนวยความสะดวกในการเคลื่อนย้ายผู้ป่วยไปยังห้องให้คำปรึกษาที่เกี่ยวข้องอย่างเป็นระเบียบ และกำกับดูแลการรักษาความปลอดภัยของแผนภูมิผู้ป่วย]

● ข้อมูลที่เป็นความลับเกี่ยวกับผู้ป่วยจะต้องได้รับการปกป้องอย่างปลอดภัยตลอดเวลา และต้องใช้มาตรการรักษาความปลอดภัยเพื่อให้แน่ใจว่าการติดต่อดังกล่าวจะไม่ถูกทิ้งไว้ในสภาพแวดล้อมที่ผู้คนสามารถเข้าถึงได้ง่าย

● ในสถานพยาบาลหลายแห่ง แผนภูมิทางการแพทย์ของผู้ป่วยถูกจัดเก็บไว้ในตู้ล็อกเกอร์หรือชั้นวางของแบบเปิดในพื้นที่ต่าง ๆ เช่น Admissions Office แผนกผู้ป่วยนอก หรือบริเวณทางเดินหรือสำนักงานย่อยภายในห้องสมุดเวชระเบียน ยุติการจัดเก็บแผนภูมิทางการแพทย์ของผู้ป่วยในพื้นที่ที่ไม่ปลอดภัย และ

ตรวจสอบให้แน่ใจว่าแผนภูมิทางการแพทย์ทั้งหมดที่จัดอยู่ในสภาพแวดล้อมที่ไม่ปลอดภัยในปัจจุบันถูกย้ายไปยังพื้นที่ที่ปลอดภัย

ความเสี่ยง 5

แนวปฏิบัติในการกำหนดให้ผู้ป่วยที่เช็คอินที่โรงพยาบาลผ่าน Admissions Office นำแผนภูมิทางการแพทย์ไปยังวอร์ดที่ได้รับมอบหมายนั้นพบได้บ่อยในโรงพยาบาลหลายแห่งที่ได้รับการตรวจ ด้วยลักษณะที่ละเอียดอ่อนของข้อมูลที่อาจมีอยู่ในแผนภูมิทางการแพทย์ของผู้ป่วยควบคู่ไปกับความวิตกกังวลตามธรรมชาติของผู้ป่วยเกี่ยวกับการเข้ารับการรักษาในโรงพยาบาลเพื่อทำหัตถการหรือการรักษา การปฏิบัตินี้จึงมีความเสี่ยงอย่างแท้จริงต่อความปลอดภัยของข้อมูลในขณะที่อยู่ในการดูแลผู้ป่วย ความเสี่ยงนี้ยังคงมีอยู่โดยที่โรงพยาบาลจัดหาถุงปิดผนึกซึ่งวางแผนภูมิผู้ป่วยไว้ก่อนที่จะถูกส่งไปยังผู้ป่วยเพื่อดำเนินการไปยังหอผู้ป่วยที่เกี่ยวข้อง

คำแนะนำ

- ควรมีการแนะนำขั้นตอนในโรงพยาบาลเพื่อให้แน่ใจว่าผู้ป่วยไม่จำเป็นต้องพกแผนภูมิทางการแพทย์ ประวัติเวชระเบียนจากส่วนหนึ่งของโรงพยาบาลไปยังอีกส่วน เจ้าหน้าที่ของโรงพยาบาลควรทำหน้าที่นี้ในทุกสถานการณ์

ความเสี่ยง 6

เมื่อ GDPR มีผลบังคับใช้ในวันที่ 25 พฤษภาคม 2018 จะมีภาระผูกพันทางกฎหมายภายใต้มาตรา 33 สำหรับผู้ควบคุมข้อมูลเพื่อแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลทราบถึงการละเมิดข้อมูลส่วนบุคคล การแจ้งเตือนการละเมิดที่บังคับจะทำให้เกิดการรายงานการละเมิดทั้งหมดต่อคณะกรรมาธิการคุ้มครองข้อมูล โดยปกติภายในเจ็ดสิบสองชั่วโมง เว้นแต่ผู้ควบคุมข้อมูลสามารถแสดงให้เห็นตามหลักการความรับผิดชอบว่าการละเมิดข้อมูลส่วนบุคคลไม่น่าจะส่งผลให้เกิดความเสี่ยงต่อสิทธิ และเสรีภาพของบุคคล นอกจากนี้ ภายใต้มาตรา 34 ของ GDPR เมื่อการละเมิดข้อมูลส่วนบุคคลมีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงการละเมิดโดยไม่ชักช้า

ความรับผิดชอบเหล่านี้ต้องการให้ผู้ควบคุมข้อมูลมีโปรโตคอลที่มีประสิทธิภาพเพื่อให้แน่ใจว่าปฏิบัติตามข้อกำหนดการแจ้งเตือนการละเมิด GDPR อย่างสมบูรณ์ จากหลักฐานของการตรวจสอบบางส่วน มีความเสี่ยงที่อาจเกิดขึ้นที่โรงพยาบาลบางแห่งอาจไม่มีโปรโตคอลการละเมิดดังกล่าวในสถานที่และตรงเวลา จึงจำเป็นต้องพัฒนาและดำเนินการตามโปรโตคอลการแจ้งเตือนการละเมิดในแต่ละโรงพยาบาลและฝึกอบรมและแจ้งเจ้าหน้าที่เกี่ยวกับข้อกำหนดต่อไป

(หมายเหตุ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย มีการกล่าวถึงหน้าที่ของผู้ควบคุมข้อมูลและระบบการแจ้งเตือน ภายในระยะเวลา 72 ชั่วโมง เมื่อเกิดการรั่วไหลของข้อมูลเช่นกัน)

คำแนะนำ

- ควรมีโปรโตคอลสำหรับจัดการกับการละเมิดข้อมูลส่วนบุคคลในทุกโรงพยาบาลภายในวันที่ 25 พฤษภาคม 2018
- เจ้าหน้าที่โรงพยาบาลควรได้รับการฝึกอบรมอย่างเต็มที่เกี่ยวกับการดำเนินการตามโปรโตคอลการละเมิดข้อมูล ควรได้รับการศึกษาเกี่ยวกับวิธีรับรู้การละเมิดความปลอดภัยของข้อมูล และควรได้รับคำแนะนำที่เข้าใจง่ายและชัดเจนเกี่ยวกับสิ่งที่ต้องทำในกรณีที่มีการละเมิดความปลอดภัยของข้อมูล

ความเสี่ยง 7 ในการตรวจสอบของโรงพยาบาลแห่งหนึ่ง มีความกังวลเกี่ยวกับรายการจดหมายขาเข้าและขาออกที่ตามหลักปฏิบัติแล้ว ถูกทิ้งไว้ในถาดลวดที่สภาพแวดล้อมไม่มีการป้องกันขณะรอรับจากพนักงานยกกระเป๋าของโรงพยาบาล กรณีดังกล่าวมีความเสี่ยงสูงที่ข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่ละเอียดอ่อนของผู้ป่วยที่อยู่ในจดหมายโต้ตอบทางไปรษณีย์อาจเข้าถึงได้ง่ายโดยผู้ป่วยหรือผู้มาเยี่ยม ในอีกกรณีหนึ่ง จดหมายทางไปรษณีย์ถูกทิ้งไว้ในถาดเปิดที่ไม่มีหลักประกันบนเคาน์เตอร์ในวอร์ดสาธารณะที่ผู้สัญจรไปมาสามารถเข้าถึงได้ง่าย

คำแนะนำ

- จดหมายโต้ตอบทางไปรษณีย์ เช่น จดหมายขาเข้าและขาออก ที่รอการรวบรวมหรือแจกจ่ายต่อไปภายในสถานพยาบาล ควรจัดในสภาพแวดล้อมที่ปลอดภัยให้พ้นมือผู้ป่วยหรือสมาชิกที่มาเยี่ยมเยียนประชาชน

ความเสี่ยง 8 พบว่า โรงพยาบาลมีการทำสัญญาใช้ผู้ให้บริการบุคคลที่สามในการจัดเก็บแผนภูมิทางการแพทย์ที่มีอายุครบกำหนด ในการตรวจโรงพยาบาลแห่งหนึ่ง เกิดความสับสนว่ามีการทำสัญญากับผู้ให้บริการพื้นที่จัดเก็บนอกสถานที่หรือไม่

คำแนะนำ

- การจัดการประมวลผลข้อมูลทั้งหมดกับผู้ให้บริการบุคคลที่สามควรได้รับการตรวจสอบเพื่อให้แน่ใจว่าสัญญาเป็นไปตามข้อกำหนดของมาตรา 2C(3) ของกฎหมายคุ้มครองข้อมูลปี 1988 และ 2003 และจะเป็นไปตามข้อกำหนดของ GDPR ตั้งแต่วันที่ 25 พฤษภาคม 2018 .

กรณีศึกษา 4 การจัดเก็บบันทึกการดูแลผู้ป่วยในวอร์ดของโรงพยาบาล (Patient Observation Charts)

บริบท

แผนภูมิบันทึกการดูแลผู้ป่วยใช้กันอย่างแพร่หลายในโรงพยาบาลทั่วโลก เอกสารเหล่านี้เป็นเอกสารสำคัญที่ช่วยให้สามารถบันทึกการสังเกตทางสรีรวิทยาของผู้ป่วยระหว่างพักรักษาตัวในโรงพยาบาลได้ โดยอาจมีการบันทึกรายละเอียดทางสรีรวิทยาในระดับต่างๆ ลงในแผนภูมิการสังเกต ทั้งนี้ขึ้นอยู่กับประเภทของแผนภูมิที่ใช้ แผนภูมิการสังเกตส่วนใหญ่จะใช้เพื่อตรวจสอบสัญญาณชีพของผู้ป่วย เช่น อุณหภูมิร่างกาย อัตราการเต้นของหัวใจหรือชีพจร อัตราการหายใจ และความดันโลหิต โดยปกติชื่อและวันเกิดของผู้ป่วยจะถูกบันทึกไว้ในบันทึกการดูแลผู้ป่วย

รายละเอียดทางสรีรวิทยาที่บันทึกไว้ในบันทึกการดูแลผู้ป่วยเกี่ยวกับผู้ป่วยที่สามารถระบุตัวตนได้ทำให้เนื้อหาของแผนภูมิจัดอยู่ในหมวดหมู่ของ 'ข้อมูลส่วนบุคคลที่ละเอียดอ่อน' ตามความหมาย GDPR รายละเอียดทางสรีรวิทยาดังกล่าวอยู่ในคำจำกัดความของ 'ข้อมูลเกี่ยวกับสุขภาพ'

ความเสี่ยง 1 ในสถานพยาบาลบางแห่งที่ได้รับการตรวจสอบตามหลักปฏิบัติ แผนภูมิการสังเกตผู้ป่วยในส่วนที่เกี่ยวกับผู้ป่วยที่เข้ารับการรักษาจะถูกตัดไปที่ปลายเตียงของผู้ป่วยแต่ละราย ในกรณีที่ผู้ป่วยเข้ารับการรักษาในหอผู้ป่วยแยก โดยโรงพยาบาลบางแห่งจะปฏิบัติตามแนวทางปฏิบัติมาตรฐานในการแขวนแผนภูมิการสังเกตผู้ป่วยไว้บนราวแขวนผนังทันทีนอกหอผู้ป่วยแยกผู้ป่วย โดยปกติแล้วจะอยู่บริเวณทางเดิน ในทั้งสองกรณีนี้ เช่น แผนภูมิการสังเกตไม่มีการป้องกันและไม่มีหลักประกัน มีความเสี่ยงสูงที่บุคคลภายนอกจะดู หรือเข้าถึงแผนภูมิการสังเกตของผู้ป่วยอย่างไม่เหมาะสมได้ เช่น ผู้ป่วยรายอื่น ผู้มาเยี่ยม หรือสมาชิกสาธารณะอื่นๆ

ในฐานะผู้ควบคุมข้อมูล โรงพยาบาลมีหน้าที่ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมกับการเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต แนวทางปฏิบัติที่ระบุไว้ข้างต้นเป็นแนวทางที่สืบทอดมาจากกฎหมายว่าด้วยการคุ้มครองข้อมูล ทั้งนี้ แนวทางปฏิบัติเหล่านี้ใช้กับสถานการณ์ที่ข้อมูลส่วนบุคคลของผู้ป่วยถูกเปิดเผยโดยบุคคลที่สาม เช่น ผู้เยี่ยมชมโดยเฉพาะ ผู้ป่วยมีสิทธิ์ที่จะมีข้อมูลส่วนบุคคลของ

ที่บันทึกไว้ในแผนภูมิการสังเกตที่ได้รับการคุ้มครองอย่างเต็มที่และความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคลนั้นขึ้นอยู่กับโรงพยาบาลที่เกี่ยวข้อง ดังนั้น จึงเป็นเรื่องของโรงพยาบาลแต่ละแห่งที่มีส่วนร่วมในแนวปฏิบัติที่กล่าวไว้ข้างต้นหรือคล้ายกันในการค้นหา และกำหนดแนวทางการปกป้องข้อมูลส่วนบุคคลของผู้ป่วยอย่างเต็มที่ ในขณะเดียวกันก็ตอบสนองความต้องการของโรงพยาบาลในแง่ของการเข้าถึงข้อมูล แผนภูมิการสังเกตสำหรับพยาบาลและแพทย์

อย่างไรก็ตาม มีบางกรณีที่น่าเป็นห่วง เช่น การวางกระดาษเปล่าไว้บนแผนภูมิการสังเกตผู้ป่วย หรือโดยการวางแผนภูมิการสังเกตผู้ป่วยในโฟลเดอร์ที่ไม่ปลอดภัยหรือรูปแบบอื่น ๆ ของอุปกรณ์ที่ไม่ปลอดภัย แนวทางแนะนำ คือ การรักษาความปลอดภัยแผนภูมิการสังเกตผู้ป่วยทั้งหมดในลักษณะที่ปกป้องจากการถูกเข้าถึงโดยผู้ป่วยรายอื่น ผู้มาเยือน ผู้สัญจรไปมา หรือบุคคลที่สามอื่น ๆ

คำแนะนำ [หมายเหตุ: การนำคำแนะนำเหล่านี้ไปใช้โดยโรงพยาบาลควรคำนึงถึงประเด็นที่เกี่ยวข้องกับความปลอดภัยของผู้ป่วยในการตั้งค่าวอร์ด เพื่อให้แน่ใจว่ามีความสมดุลที่เหมาะสมระหว่างการลดความเสี่ยงในการปกป้องข้อมูลที่ระบุไว้ข้างต้นและการลดความเสี่ยงต่อความปลอดภัยของผู้ป่วย]

- ในกรณีที่แผนภูมิการสังเกตผู้ป่วยถูกตัดหรือทิ้งไว้ที่ปลายเตียงผู้ป่วย ในอนาคตควรจัดเก็บแผนภูมิเหล่านี้อย่างปลอดภัยในสภาพแวดล้อมที่มีการป้องกัน ในบริเวณใกล้เคียงกับเตียงของผู้ป่วยหากจำเป็น ซึ่งสามารถเข้าถึงได้โดยเจ้าหน้าที่ของโรงพยาบาลเท่านั้น ที่มีความต้องการระดับมืออาชีพในการเข้าถึง

- ในกรณีที่แผนภูมิการสังเกตผู้ป่วยจัดเก็บไว้บนราวแขวนผนังหรือที่คล้ายกันนอกหอผู้ป่วยแยกหรือห้องแยก ในอนาคตควรจัดเก็บแผนภูมิเหล่านี้อย่างปลอดภัยในสภาพแวดล้อมที่มีการป้องกัน ในบริเวณใกล้เคียงกับหอผู้ป่วยหรือห้องของผู้ป่วย หากจำเป็น ซึ่งสามารถเข้าถึงได้เท่านั้น ให้กับเจ้าหน้าที่ของโรงพยาบาลที่มีความต้องการระดับมืออาชีพในการเข้าถึง

กรณีศึกษา 5 การจัดเก็บข้อมูลผู้ป่วยในรถเข็นถังขยะในวอร์ดต่าง ๆ

บริบท

บันทึกการดูแลสุขภาพหรือที่เรียกกันทั่วไปว่าแผนภูมิผู้ป่วย (Patient charts) จะถูกสร้างขึ้นสำหรับผู้ป่วยที่เข้ารับการรักษาทุกรายในโรงพยาบาล ผู้ป่วยที่เกี่ยวข้องกับแผนภูมิมักจะระบุโดยใช้ฉลากที่ติดอยู่กับปกด้านหน้า ฉลากแสดงรายละเอียดชื่อของผู้ป่วย ที่อยู่ วันเกิด และหมายเลขบันทึกการรักษาพยาบาล โดยปกติ โฟลเดอร์ประกอบด้วยข้อมูลผู้ป่วยที่อยู่ในส่วนที่เกี่ยวข้องภายในโฟลเดอร์ ตัวอย่างเช่น ส่วนของแผนภูมิอาจเรียงลำดับตามบรรทัดต่อไปนี้ แผนกธุรการ ส่วนโต้ตอบ ส่วนบันทึกทางคลินิก บันทึกพยาบาล ขั้นตอนการยินยอม การวัดทางคลินิก ผลการตรวจทางห้องปฏิบัติการ ผลการถ่ายภาพรังสีวิทยาและการวินิจฉัย ยาตามใบสั่งแพทย์ และสุขภาพ & ส่วนผู้เชี่ยวชาญด้านการดูแลสังคม

รายละเอียดที่บันทึกไว้ในแผนภูมิผู้ป่วยเกี่ยวกับผู้ป่วยที่สามารถระบุตัวตนได้ทำให้เนื้อหาของแผนภูมิจัดอยู่ในหมวดหมู่ของ 'ข้อมูลส่วนบุคคลที่ละเอียดอ่อน' อย่างชัดเจนตามความหมายของพระราชบัญญัติสำหรับวัตถุประสงค์ของ GDPR รายละเอียดดังกล่าวจะอยู่ในคำจำกัดความของ "ข้อมูลเกี่ยวกับสุขภาพ"

ความเสี่ยง 1 ในการตั้งวอร์ดของโรงพยาบาลบางแห่ง พบว่า แผนภูมิผู้ป่วยของผู้ป่วยที่เข้ารับการรักษาในปัจจุบันจะถูกจัดเก็บไว้ในสิ่งที่เรียกว่ารถเข็นถังขยะ (Trolley bins) ถังขยะรถเข็นมาในรูปทรงและขนาดต่างๆ ถังขยะรถเข็นส่วนใหญ่เป็นแบบเคลื่อนย้ายได้ (มีสี่ล้อ) และมีฝาปิดแบบล็อกได้ บางแห่งมีชั้นวางของแบบเปิดด้านล่างใต้ตู้เก็บของแบบปิด

ในขณะที่แผนภูมิผู้ป่วยที่จัดเก็บไว้ในถังรถเข็นสามารถป้องกันได้อย่างปลอดภัยจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยการปิดและล็อกฝาถังรถเข็น ผู้ตรวจสอบพบหลักฐานเพียงเล็กน้อยในโรงพยาบาลบางแห่งว่าฝาถังรถเข็นเคยถูกใช้เพื่อการนี้ โดยทั่วไปแล้ว ผู้เชี่ยวชาญทางการแพทย์ใช้ฝาปิดถังขยะแบบรถเข็นเพื่อช่วยเปิดแผนภูมิของผู้ป่วยเมื่อเขียนเคสบนแผนภูมิ สิ่งที่น่ากังวลเป็นพิเศษ คือ สถานการณ์ที่ถังรถเข็นที่ปลดล็อกแล้วจอดอยู่นอกสถานีพยาบาล ซึ่งแผนภูมิผู้ป่วยในนั้นอาจเข้าถึงได้โดยผู้สัญจรไปมา เช่น ผู้ป่วย ผู้มาเยี่ยม หรือสมาชิกคนอื่นๆ ของประชาชน

คำแนะนำ

● รถเข็นทั้งหมดที่ใช้ในการตั้งค่าวอร์ดเพื่อจัดเก็บแผนภูมิผู้ป่วยของผู้ป่วยปัจจุบัน ควรเก็บไว้ในพื้นที่ปลอดภัยและห่างไกลจากผู้สัญจรไปมา เช่น ด้านหลังโต๊ะในสถานีพยาบาลหรือในพื้นที่สำนักงานที่ล็อกไว้

● ในช่วงเวลาการเยี่ยมชมสาธารณะ ควรปิดฝาถังรถเข็นทั้งหมดที่มีแผนภูมิผู้ป่วยปิดและล็อก

ความเสี่ยง 2 ในโรงพยาบาลบางแห่ง ผู้ตรวจสอบตั้งข้อสังเกตถึงกรณีที่แผนภูมิผู้ป่วยและ/หรือข้อมูลผู้ป่วยหรือบันทึกการพยาบาลถูกจัดเก็บไว้ในสภาพแวดล้อมที่ไม่ได้รับการปกป้อง ไม่ว่าจะอยู่ในพื้นที่เปิดโล่งที่ด้านล่างของรถเข็นหรือในอุปกรณ์แขวนที่ด้านข้างของรถเข็น

คำแนะนำ

● แผนภูมิผู้ป่วย ข้อมูลผู้ป่วย หรือบันทึกการพยาบาลไม่ควรเก็บไว้ในชั้นวางแบบเปิดบนถังรถเข็น

กรณีศึกษา 6 การจัดเก็บกระดาษเสียที่เป็นความลับภายในสถานพยาบาล

บริบท

ในสภาพแวดล้อมการทำงานหลายๆ แห่ง การจัดเก็บและกำจัดเศษกระดาษที่เป็นความลับเป็นเรื่องสำคัญ ในสถานพยาบาล ขยะที่เป็นความลับถูกสร้างขึ้นในเกือบทุกพื้นที่ของสถานพยาบาลทุกวัน ด้วยลักษณะของงานที่ทำในสภาพแวดล้อมของโรงพยาบาล ขยะที่เป็นความลับส่วนใหญ่เกี่ยวข้องกับผู้ป่วยในแง่ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสภาพทางการแพทย์ การรักษา ประกันสุขภาพ การนัดหมายแพทย์ ฯลฯ

ความเสี่ยง 1 โรงพยาบาลหลายแห่งที่ได้รับการตรวจสอบใช้ถังกระดาษ กระเป๋า หรือถาดที่ไม่ปลอดภัยในสำนักงาน ส่วนต่างๆ และหอผู้ป่วยทั่วอาคาร ในสถานการณ์เหล่านี้ ผู้อื่นสามารถนำเศษกระดาษที่วางอยู่ในถังขยะ ถุงหรือถาดเหล่านี้ออกได้ โดยพบว่าในโรงพยาบาลแห่งหนึ่ง พนักงานคนหนึ่งนำเอกสารที่เป็นความลับทิ้งขยะซึ่งมีข้อมูลผู้ป่วย ซึ่งก่อนหน้านี้พนักงานคนอื่นใส่ลงในถังขยะนั้น

ดังนั้น ผู้ควบคุมข้อมูลมีหน้าที่กำหนดมาตรการการทิ้งขยะกระดาษที่มีข้อมูลอ่อนไหว และความลับของผู้ป่วยเพื่อปกป้องข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการรั่วไหลและการเข้าถึงข้อมูลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

คำแนะนำ

- เปลี่ยนถังขยะ ถุงและถาดที่ไม่ปลอดภัยทั้งหมดที่ใช้เก็บกระดาษเสียที่เป็นความลับด้วยถังขยะที่เป็นความลับแบบล็อกได้ซึ่งมีฝาปิดหรือช่องสำหรับทิ้งขยะที่เป็นความลับแต่ไม่สามารถดึงออกมาได้ คำแนะนำนี้ใช้กับทุกพื้นที่ของสถานพยาบาลรวมถึงพื้นที่สำนักงานที่จำกัดการเข้าถึงสำหรับเจ้าหน้าที่

กรณีศึกษา 7 การกำจัดรายการส่งมอบและรายการผู้ป่วย

บริบท

ในการตั้งค่าวอร์ดของโรงพยาบาลหลายแห่ง พบว่า เจ้าหน้าที่พยาบาลจะพกรายการเอกสารจริงไว้ในกระเป๋าเครื่องแบบตลอดช่วงกะทำงาน โรงพยาบาลบางแห่งใช้คำว่า 'รายการส่งมอบ' เพื่ออธิบายรายการเหล่านี้ในขณะที่รวบรวมไว้เมื่อกะการพยาบาลหนึ่งกะถูกส่งมอบให้กับกะการพยาบาลครั้งต่อไป ในระหว่างการบรรยายสรุปการส่งมอบนั้น เจ้าหน้าที่พยาบาลที่เข้ากะที่เข้ากะจะบันทึกเป็นลายลักษณ์อักษรเกี่ยวกับแง่มุมต่างๆ ของการพยาบาลผู้ป่วยแต่ละรายในวอร์ดของตน โรงพยาบาลอื่นๆ ใช้คำว่า "รายชื่อผู้ป่วย" เนื่องจากในกรณีดังกล่าวจะมีข้อมูลทั่วไปของผู้ป่วย เช่น ชื่อและหมายเลขเตียงของผู้ป่วยแต่ละราย

ความเสี่ยง 1 โรงพยาบาลทุกแห่งที่เจ้าหน้าที่พยาบาลใช้รายการส่งมอบหรือรายชื่อผู้ป่วยในวอร์ดรายงานต่อผู้ตรวจว่าเป็นขั้นตอนมาตรฐานที่เมื่อสิ้นสุดกะแต่ละกะ พยาบาลจะใส่รายการลงในเครื่องทำลายเอกสารหรือในถังขยะที่เป็นความลับ อย่างไรก็ตาม ผู้ตรวจไม่พบหลักฐานว่าโรงพยาบาลที่เกี่ยวข้องติดตามการปฏิบัติตามขั้นตอนมาตรฐาน ดังนั้น หากไม่มีขั้นตอนสิ้นสุดกะเพื่อบัญชีสำหรับการกำจัดรายการดังกล่าวอย่างปลอดภัย จึงมีความเสี่ยงที่สำคัญที่เจ้าหน้าที่พยาบาลอาจนำรายการออกจากการตั้งค่าของโรงพยาบาลโดยไม่ได้ตั้งใจเมื่อสิ้นสุดกะและกำจัดข้อมูลในเวลาต่อมาในที่อื่น เนื่องจากรายการลักษณะนี้มีข้อมูลส่วนบุคคลเกี่ยวกับผู้ป่วยที่อาจมีความละเอียดอ่อนเป็นพิเศษ จึงจำเป็นต้องกำจัดทิ้งอย่างปลอดภัยในสภาพแวดล้อมของโรงพยาบาล ด้วยเหตุผลดังกล่าว โรงพยาบาลจะต้องมีวิธีการบัญชีสำหรับการรวบรวมรายชื่อแต่ละรายการเมื่อสิ้นสุดกะแต่ละกะ และการกำจัดอย่างปลอดภัยในเครื่องทำลายเอกสารหรือในถังขยะที่เป็นความลับแบบล็อกได้

[เป็นที่น่าสังเกตว่าในโรงพยาบาลจำนวนน้อยที่ตรวจสอบรายการส่งมอบหรือรายชื่อผู้ป่วยจะไม่สร้างหรือใช้ในทุกวอร์ดและวอร์ดเหล่านั้นทำงานได้อย่างมีประสิทธิภาพ]

คำแนะนำ

● ใช้ขั้นตอนที่เข้มงวดในการตั้งค่าวอร์ดเพื่อให้แน่ใจว่ารายการส่งมอบที่ใช้และรายชื่อผู้ป่วยทั้งหมดจะถูกนำมาพิจารณาเมื่อสิ้นสุดกะแต่ละกะและกำจัดทิ้งอย่างปลอดภัยในเครื่องทำลายเอกสารหรือในถังขยะที่เป็นความลับแบบล็อกได้ ซึ่งสามารถทำได้ ตัวอย่างเช่น โดยการจัดเตรียมใบลงนามที่เครื่องทำลายเอกสาร/ถังเก็บความลับ โดยที่เจ้าหน้าที่จะลงนามว่าได้เสร็จสิ้นการกำจัดรายการอย่างปลอดภัยแล้ว

● ให้ยุติการปฏิบัติที่เจ้าหน้าที่พยาบาลพกรายการส่งเอกสารจริงหรือรายชื่อผู้ป่วยไว้ในกระเป๋าเครื่องแบบ

กรณีศึกษา 8 การใช้เครื่องแฟกซ์ในการส่งข้อมูล

บริบท

การใช้เครื่องแฟกซ์สำหรับการส่งข้อความที่เป็นลายลักษณ์อักษรในโรงพยาบาลเป็นเรื่องปกติ โดยพบว่า มีการใช้เครื่องแฟกซ์ในแผนกต่างๆ ของโรงพยาบาล เช่น แผนกฉุกเฉิน ผู้ป่วยนอก การรับเข้า และในสถานีพยาบาลของหอผู้ป่วยในหลายแห่ง เครื่องแฟกซ์ จึงถือเป็นเครื่องมือสื่อสารที่จำเป็นในโรงพยาบาลหลายแห่งในการส่งข้อมูลผู้ป่วยไปและรับข้อมูลผู้ป่วยจากผู้ปฏิบัติงานทั่วไป สถานพยาบาล และสถานพยาบาลอื่นๆ ระดับการใช้เครื่องแฟกซ์ยังคงสูง แม้ว่าจะมีอีเมลที่เข้ารหัสไว้ซึ่งเป็นวิธีที่ปลอดภัยกว่าในการสื่อสารทางอิเล็กทรอนิกส์

ความเสี่ยง 1 ความเสี่ยงของการใช้เครื่องแฟกซ์คือความผิดพลาดของมนุษย์ เมื่อกดหมายเลขเพื่อส่งข้อความแฟกซ์ขาออก มีการรายงานการละเมิดความปลอดภัยของข้อมูลหลายครั้งต่อคณะกรรมการคุ้มครองข้อมูลอันเป็นผลมาจากข้อผิดพลาดดังกล่าว รวมถึงเหตุการณ์ที่เกี่ยวข้องกับการส่งข้อมูลผู้ป่วยระหว่างโรงพยาบาลและผู้ปฏิบัติงานทางการแพทย์ โดยเฉพาะอย่างยิ่งความเสี่ยงเกิดขึ้นจากการกดหมายเลขตามลำดับที่ถูกต้อง รวมถึงการละเว้นการโทรออก หรือกดรหัสพื้นที่ของหมายเลขแฟกซ์ที่รับไม่ถูกต้อง

คำแนะนำ

- หากเป็นไปได้ ควรตั้งโปรแกรมหมายเลขแฟกซ์ที่โทรออกเป็นประจำในเครื่องแฟกซ์ล่วงหน้าเพื่อลดความเสี่ยงที่จะเกิดข้อผิดพลาดในการโทรผิด ในกรณีที่เป็นไปไม่ได้ ควรวางไดเร็กทอรีของหมายเลขแฟกซ์ที่โทรออกเป็นประจำซึ่งพิมพ์ในรูปแบบที่ชัดเจนและอ่านง่าย ในตำแหน่งที่โดดเด่นข้างเครื่องแฟกซ์แต่ละเครื่อง

ความเสี่ยง 2 พบข้อเท็จจริงว่า ไม่มีคำแนะนำสำหรับผู้ใช้เครื่องแฟกซ์ในโรงพยาบาลหลายแห่งในการแจ้งให้ทราบถึงแนวทางปฏิบัติที่ดีที่สุดเกี่ยวกับการส่งหรือรับข้อความแฟกซ์ที่มีข้อมูลส่วนบุคคลที่ละเอียดอ่อน

คำแนะนำ

- เครื่องแฟกซ์ทุกเครื่องควรมีบันทึกคำแนะนำในบริเวณใกล้เคียงเพื่อให้คำแนะนำแก่ผู้ใช้ในสถานการณ์ที่เหมาะสมที่จะใช้เครื่องแฟกซ์เพื่อส่งข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่ละเอียดอ่อน และ

เพื่อเตือนผู้ใช้ถึงความเสี่ยงในการส่งข้อความไปยังผู้รับผิด หมายเลขแฟกซ์ บันทึกคำแนะนำควรให้แนวทางปฏิบัติเกี่ยวกับวิธีใช้เครื่องแฟกซ์ด้วย ควรร่างขั้นตอนที่ต้องปฏิบัติตามในกรณีที่ข้อความโทรสารส่งออกไปผิดทิศทาง

กรณีศึกษา 9 ความเป็นส่วนตัวกับการรั่วไหลของข้อมูลจากการพูด

บริบท

ความเป็นส่วนตัวของคำพูดมักถูกกำหนดให้ไม่สามารถเข้าใจการสนทนาได้ แม้ว่าคำบางคำอาจยังได้ยินอยู่ก็ตาม ความเป็นส่วนตัวของคำพูดเกิดขึ้นเมื่อคำพูดหรือการสนทนาระหว่างสองฝ่ายขึ้นไป ไม่สามารถเข้าใจได้โดยบุคคลอื่นที่อาจอยู่ใกล้ ๆ ปัญหาที่พบบ่อยที่สุดประการหนึ่งที่ คือ การขาดความเป็นส่วนตัวในการพูดในพื้นที่ต่างๆ ของสถานพยาบาล ปัญหานี้เกิดขึ้นในหลายพื้นที่ของโรงพยาบาลที่ผู้ป่วยมีปฏิสัมพันธ์กับเจ้าหน้าที่ของโรงพยาบาล เช่น ที่แผนกต้อนรับในแผนกฉุกเฉิน โต๊ะต้อนรับในแผนกผู้ป่วยนอก ห้องรักษาในแผนกฉุกเฉิน ที่เตียงของโรงพยาบาลในหอผู้ป่วย ในหลายกรณี การขาดความเป็นส่วนตัวในการพูดอาจเนื่องมาจากรูปแบบทั่วไปของพื้นที่ที่เกี่ยวข้องหรือพื้นที่จำกัดที่มีอยู่ในพื้นที่ที่เกี่ยวข้อง

ทั้งนี้ ผู้ป่วยควรได้รับความเป็นส่วนตัวเพื่อหารือเกี่ยวกับสภาพทางการแพทย์ การรักษาพยาบาล การจัดการทางการเงินกับโรงพยาบาล สถานะประกันสุขภาพส่วนตัวหรือสถานะบัตรแพทย์ และเรื่องส่วนตัวอื่น ๆ ทั้งหมดกับเจ้าหน้าที่ของโรงพยาบาลโดยไม่เสี่ยงต่อการถูกได้ยิน

ความเสี่ยง 1 ในพื้นที่ต่าง ๆ ของโรงพยาบาลที่ขาดความเป็นส่วนตัวในการพูด มีโอกาสที่บุคคลที่สามสามารถเข้าถึงข้อมูล เช่น ผู้ป่วยรายอื่นและผู้มาเยี่ยมในโรงพยาบาลที่จะได้ยินการสนทนาส่วนตัวระหว่างผู้ป่วยและเจ้าหน้าที่ของโรงพยาบาล ยกตัวอย่างสถานการณ์ของแผนกต้อนรับ ผู้ป่วยที่มาถึงมักจะร้องขอโดยพนักงานต้อนรับของโรงพยาบาลให้ระบุองค์ประกอบหลายอย่างของข้อมูลส่วนบุคคลด้วยวาจา เช่น ชื่อ ที่อยู่ วันเดือนปีเกิด รายละเอียดการติดต่อ รายละเอียดเครือญาติ รายละเอียดบัตรแพทย์ ฯลฯ จากนั้นพนักงานต้อนรับจะป้อนรายละเอียดที่ได้รับจากผู้ป่วยเข้าระบบคอมพิวเตอร์ของโรงพยาบาล เห็นได้ชัดว่า การมีส่วนร่วมที่แผนกต้อนรับของโรงพยาบาลถือเป็นรูปแบบหนึ่งของการประมวลผลข้อมูล โรงพยาบาลซึ่งเป็นผู้ควบคุมข้อมูลมีหน้าที่ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมกับการเปิดเผยข้อมูลส่วนบุคคล ในสถานการณ์สมมติของแผนกต้อนรับที่อธิบายข้างต้น โรงพยาบาลต้องตรวจสอบให้แน่ใจว่าการมีส่วนร่วมของผู้ป่วยกับพนักงานต้อนรับและการรวบรวมข้อมูลส่วนบุคคลที่เกิดขึ้นระหว่างการมีส่วนร่วมนั้นดำเนินการใน

สภาพแวดล้อมที่ช่วยให้ผู้ป่วยมีความเป็นส่วนตัวในการพูดเพียงพอและป้องกันการเปิดเผย ของข้อมูลส่วนบุคคลแก่บุคคลอื่นที่อยู่ใกล้เคียง

คำแนะนำ

● ในบริเวณแผนกต้อนรับ ผู้ป่วยควรมีพื้นที่เพียงพอและเป็นส่วนตัวเพื่อให้สามารถให้รายละเอียดข้อมูลส่วนบุคคลแก่เจ้าหน้าที่ของโรงพยาบาลได้โดยไม่เสี่ยงต่อการถูกมองข้ามโดยคนที่ยืนอยู่ข้างๆ หรือคนที่เดินผ่านไปมา

● ควรพิจารณาวิธีแก้ปัญหาต่าง ๆ ในบริเวณแผนกต้อนรับเพื่อทำให้ผู้ฟังทั่วไปไม่สามารถเข้าใจคำพูดได้ เช่น การทบทวนแผนผังทั่วไปของพื้นที่ที่เกี่ยวข้อง การโพสต์ประกาศเกี่ยวกับความเป็นส่วนตัวบนผนังที่อยู่ติดกัน การทาสีเครื่องหมายเส้นบนพื้น การแนะนำเทคโนโลยีเสียงอะคูสติกที่เหมาะสมและการใช้ระบบตั๋ว ซึ่งจะช่วยลดความเป็นไปได้ที่ผู้อื่นจะยืนอยู่ข้างหลังผู้ป่วยที่กำลังเช็คอินทันที

● เมื่อพื้นที่เช็คอินอยู่บนทางเดินสาธารณะ ควรมีมาตรการหลายอย่าง เช่น การวางช่องแบ่งระหว่างช่องที่โต๊ะเช็คอิน เครื่องหมายเส้นบนพื้น หากจำเป็นตำแหน่งของโต๊ะเช็คอินควรเปลี่ยนแปลงเพื่อให้มีสภาพแวดล้อมที่เป็นมิตรต่อความเป็นส่วนตัวมากขึ้น หรือควรพิจารณาให้ย้ายไปอยู่ที่ส่วนอื่นของโรงพยาบาลซึ่งจะไม่เกิดความเสี่ยงด้านความเป็นส่วนตัวในการพูด

ความเสี่ยง 2 พบว่า เกิดขึ้นในห้องบำบัดของแผนกฉุกเฉินบางแห่ง โดยในห้อง มีพื้นที่และม่านที่มีขนาดจำกัดพร้อมฉากกั้นทั้งสองข้างเป็นห้องกั้นการสนทนาส่วนตัวที่เกิดขึ้นในห้องเล็ก ๆ ทำให้ระหว่างการพูดคุย เจ้าหน้าที่ทางการแพทย์และผู้ป่วยสามารถได้ยินกันได้ง่าย ๆ ในห้องเล็กที่อยู่ติดกันทั้งสองข้าง การสนทนาในลักษณะที่ละเอียดอ่อนที่สุดเกิดขึ้นระหว่างเจ้าหน้าที่ทางการแพทย์และผู้ป่วยในห้องบำบัดของแผนกฉุกเฉินในเรื่องต่างๆ เช่น อาการ ประวัติการรักษาก่อนหน้า แผนการรักษา ฯลฯ และในอีกตัวอย่างหนึ่งพบว่า ได้ยินการสนทนาเกี่ยวกับภาวะทางการแพทย์ของผู้ป่วยและแผนการรักษาที่เกิดขึ้นระหว่างแพทย์กับผู้ป่วยบนบริเวณทางเดินของหอผู้ป่วยใน จึงเป็นหน้าที่ของโรงพยาบาลที่จะต้องทำให้แน่ใจว่าการนัดหมายในลักษณะนี้ระหว่างผู้ป่วยและเจ้าหน้าที่ทางการแพทย์จะดำเนินการในสภาพแวดล้อมที่เป็นมิตรกับความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่ละเอียดอ่อนของผู้ป่วยได้อย่างเพียงพอ

คำแนะนำ

● ในพื้นที่การรักษา หอผู้ป่วย และพื้นที่อื่น ๆ ของโรงพยาบาล ควรตระหนักและเคารพสิทธิของผู้ป่วยและข้อมูลส่วนบุคคลของผู้ป่วยในระหว่างการเข้ารับบริการทางการแพทย์ ปรึกษากับแพทย์หรือเจ้าหน้าที่โรงพยาบาลอื่น ๆ เกี่ยวกับสภาพทางการแพทย์ การดูแลทางการแพทย์ หรือการรักษา

● ควรพิจารณาวิธีแก้ปัญหาต่างๆ เพื่อทำให้ผู้ฟังทั่วไปไม่สามารถเข้าใจคำพูดได้ เช่น การทบทวนแผนผังทั่วไปของพื้นที่ที่เกี่ยวข้อง การติดประกาศเกี่ยวกับความเป็นส่วนตัวบนผนังที่อยู่ติดกัน การทาสีเครื่องหมายเส้นบนพื้น เทคโนโลยีเสียงอะคูสติกและการใช้ม่านความเป็นส่วนตัวที่ได้รับการปรับปรุง เหนือสิ่งอื่นใด การแก้ปัญหาเหล่านี้ควรนำมาใช้เป็นแพ็คเกจเพื่อให้เกิดประโยชน์สูงสุด การเลือกและการนำโซลูชันหนึ่งไปใช้โดยแยกกันไม่น่าจะได้รับประโยชน์สูงสุด

● ผู้ป่วยที่อยู่ในพื้นที่ส่วนกลางของโรงพยาบาล (เช่น หอผู้ป่วยหลายเตียง) มีสิทธิที่จะได้รับความเป็นส่วนตัว และควรได้รับโอกาสเมื่อพูดคุยกับเจ้าหน้าที่ของโรงพยาบาลเพื่อย้ายไปยังพื้นที่ส่วนตัวมากขึ้น ควรมีห้องให้คำปรึกษาส่วนตัวในทุกกรณีเพื่อให้ผู้ป่วยมีระดับความเป็นส่วนตัวในการพูดที่เพียงพอ

กรณีศึกษา 10 การตรวจสอบเส้นทางข้อมูลที่มีประสิทธิภาพ

บริบท

ทุกปีผู้ป่วยหลายแสนคนเข้ารับการรักษาในโรงพยาบาล และจะมีการบันทึกรายละเอียดทางประชากรศาสตร์พื้นฐานไว้บนระบบการจัดการผู้ป่วยแบบอิเล็กทรอนิกส์ของโรงพยาบาลที่เกี่ยวข้อง โดยทางโรงพยาบาลจะสร้างบันทึกอิเล็กทรอนิกส์ของผู้ป่วยหลายพันรายต่อปี การรักษาความปลอดภัยข้อมูลส่วนบุคคลที่มีอยู่ในบันทึกเหล่านี้จำเป็นต้องมีมาตรการ เช่น ร่องรอยการตรวจสอบที่ใช้งานได้ ตลอดจนการตรวจสอบเส้นทางการตรวจสอบที่มีประสิทธิภาพ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยโรงพยาบาลทุกแห่งที่ตรวจสอบใช้ระบบฐานข้อมูลอิเล็กทรอนิกส์ต่างๆ สำหรับการบริหารผู้ป่วยและเพื่อวัตถุประสงค์อื่นๆ เช่น การจัดการเวชระเบียนเกี่ยวกับรังสีวิทยา การสแกน ฯลฯ ระบบการจัดการฐานข้อมูลจำนวนมากที่ทำงานในโลกของเทคโนโลยีสมัยใหม่รวมถึงเส้นทางการตรวจสอบ (หรือบันทึกการตรวจสอบ) เส้นทางการตรวจสอบคือ บันทึกที่แสดงว่าใครเข้าถึงระบบคอมพิวเตอร์และดำเนินการใด ๆ ที่ได้ดำเนินการในช่วงเวลาที่กำหนด ฟังก์ชันเส้นทางการตรวจสอบที่มีประสิทธิภาพควรมีความสามารถในการบันทึกการเข้าถึงแบบ 'อ่านอย่างเดียว' (โดยที่ผู้ใช้เข้าถึงบันทึกแต่ไม่ได้แก้ไขหรือเพิ่มเติมใดๆ) เช่นเดียวกับการเข้าถึง 'แก้ไข' (ที่ผู้ใช้แก้ไขหรือเพิ่มข้อมูลลงใน บันทึก) ด้วยเหตุนี้ การตรวจสอบจึงเป็นเครื่องมือที่จำเป็นและมีประโยชน์มากสำหรับการรักษาความปลอดภัยและความสมบูรณ์ของระบบฐานข้อมูลอิเล็กทรอนิกส์

ความเสี่ยง 1 ความเสี่ยงหลักที่สามารถระบุได้ในกรณีที่ไม่มีการตรวจสอบที่ทำงานได้อย่างสมบูรณ์ (เช่น การเข้าถึงแบบ 'อ่านอย่างเดียว') รวมถึงการเข้าถึงโดยเจ้าหน้าที่สอดแนมและการเข้าถึงที่เกิดจากการ 'หมิ่นประมาท' การเข้าถึงดังกล่าวถือเป็นการละเมิดความปลอดภัยของข้อมูล

คำแนะนำ

- ควรมีระบบเส้นทางการตรวจสอบที่มีประสิทธิภาพซึ่งรวบรวมการเข้าถึงทั้งแบบ "อ่านอย่างเดียว" และ "แก้ไข" ในฐานข้อมูลบันทึกผู้ป่วยอิเล็กทรอนิกส์ทั้งหมด และกำหนดแนวทางการแก้ไขโดยไม่ชักช้า

- ควรมีการตรวจสอบผลลัพธ์ของเส้นทางการตรวจสอบเป็นประจำเพื่อตรวจสอบว่ามีการเข้าถึงโดยไม่ได้รับอนุญาตหรือการพยายามเข้าสู่ระบบบันทึกผู้ป่วยที่ล้มเหลวหรือไม่
- ควรดำเนินการตามขั้นตอนที่เข้มงวดเพื่อให้แน่ใจว่าสิทธิในการเข้าถึงบันทึกผู้ป่วยแบบอิเล็กทรอนิกส์นั้นจำกัดเฉพาะพนักงานที่ต้องการเข้าถึงบนพื้นฐาน 'จำเป็นต้องรู้' ในบันทึกผู้ป่วยเฉพาะตามบทบาทงาน การดูแลและการรักษาผู้ป่วย ควรมีการควบคุมที่เหมาะสมเพื่อให้แน่ใจว่ามีการปฏิบัติตามขั้นตอนและไม่ควรให้เจ้าหน้าที่ทางการแพทย์ คลินิก หรือพยาบาลใด ๆ เข้าถึงบันทึกผู้ป่วยทางอิเล็กทรอนิกส์ทั้งหมดได้อย่างไม่จำกัด ไม่ว่าจะมีความจำเป็นใดหรือไม่ก็ตาม
- จำกัดไม่ให้เจ้าหน้าที่เข้าถึงบันทึกผู้ป่วยทางอิเล็กทรอนิกส์โดยไม่มีเหตุผล โรงพยาบาลควรกำหนดนโยบายที่ถือว่าการเข้าถึงโดยไม่ได้รับอนุญาตนั้นเป็นเรื่องทางวินัย

กรณีศึกษา 11 การสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคลในโรงพยาบาล

บริบท

โรงพยาบาลควรปลูกฝังและสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคลในหมู่เจ้าหน้าที่ของโรงพยาบาลอย่างต่อเนื่อง จากการตรวจสอบ พบว่า โรงพยาบาลหลายแห่งมีประกาศข้อมูลขนาดต่างๆ และเนื้อหาต่างๆ ที่จัดแสดงในพื้นที่ส่วนกลางบางแห่ง เช่น แผนกต้อนรับและโซนพักรอ มีประกาศบางฉบับกล่าวถึงความมุ่งมั่นของโรงพยาบาลในเรื่องความเป็นส่วนตัวหรือการปกป้องข้อมูลโดยสังเขป หรือโรงพยาบาลบางแห่งยังจัดเตรียมแผ่นพับข้อมูลหรือหนังสือเล่มเล็ก ๆ ที่ครอบคลุมหัวข้อที่น่าสนใจมากมายสำหรับผู้ป่วยที่เข้ารับการรักษา รวมถึงความเป็นส่วนตัวและการปกป้องข้อมูล และพบโรงพยาบาลจำนวนน้อยที่มีการแสดงประกาศในพื้นที่พนักงาน เพื่อเตือนพนักงานถึงภาระหน้าที่เกี่ยวกับการรักษาความลับของผู้ป่วยและการปกป้องข้อมูล ด้วยเหตุนี้ จึงจำเป็นต้องมีการสร้างการตระหนักรู้ การฝึกอบรมด้านการปกป้องคุ้มครองข้อมูล

ความเสี่ยง 1 นับตั้งแต่เวลาที่ผู้ป่วยมาถึงโรงพยาบาล จนถึงจุดที่ออกจากโรงพยาบาล จะเกี่ยวข้องกับการดำเนินการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนทั้งหมด กล่าวได้ว่าการเข้าโรงพยาบาลจะเกี่ยวข้องกับการสร้างและการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่แบบฟอร์มการลงทะเบียนผู้ป่วย แผนภูมิ การสแกน และเอกสารอื่น ๆ ที่มีข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่ละเอียดอ่อนในโรงพยาบาล ในฐานะผู้ควบคุมข้อมูล จึงมีหน้าที่แจ้งให้ผู้ป่วยทราบว่าจะใช้ข้อมูลของตนอย่างไร และเพื่อวัตถุประสงค์ใด ความล้มเหลวในการแจ้งผู้ป่วยเป็นการละเมิดหลักการพื้นฐานของการประมวลผลข้อมูลโดยชอบว่าด้วยหลักความเป็นธรรมและความโปร่งใส

คำแนะนำ

- จัดทำนโยบายความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล โดยแสดงข้อมูลแก่ผู้ที่มาติดต่อทางโรงพยาบาลให้เข้าใจด้วยภาษาง่ายๆ ว่าโรงพยาบาลจะประมวลผลข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่ละเอียดอ่อนอย่างไร และจะดำเนินการเพื่อวัตถุประสงค์ใด ข้อมูลนี้อาจอยู่ในรูปแบบแผ่นพับข้อมูล โปสเตอร์ข้อมูลที่แสดงในพื้นที่สำคัญ เว็บไซต์ของโรงพยาบาล ฯลฯ ประกาศข้อมูลดังกล่าวทั้งหมดควรมีชื่อ และ

รายละเอียดการติดต่อของเจ้าหน้าที่โรงพยาบาลที่ได้รับมอบหมายให้รับผิดชอบในการจัดการการปกป้องข้อมูล ความกังวลที่ผู้ป่วยหรือผู้อื่นอาจต้องการแจ้ง

ความเสี่ยง 2 สร้างวัฒนธรรมองค์กรของโรงพยาบาลในการคุ้มครองข้อมูลส่วนบุคคล ความล้มเหลวในการสร้างความตระหนักของพนักงาน ก่อให้เกิดความเสี่ยงที่สำคัญที่พนักงานอาจละเลยการรักษาความปลอดภัยและเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลที่ละเอียดอ่อนต่อบุคคลที่สามไม่ว่าจะโดยไม่ได้ตั้งใจหรือโดยเจตนา

คำแนะนำ

- ควรมีโปรแกรมฝึกอบรมพนักงานเกี่ยวกับการปกป้องข้อมูลควรได้รับการตรวจสอบเพื่อให้แน่ใจว่ามีการฝึกอบรมทบทวนเป็นระยะสำหรับพนักงานทุกคนเพื่อเตือนถึงภาระหน้าที่เกี่ยวกับการเคารพสิทธิในการปกป้องคุ้มครองข้อมูลของผู้ป่วย

- ควรมีโปรแกรมฝึกอบรมสำหรับพนักงานต้อนรับ ควรมีเป็นประจำเพื่อให้แน่ใจว่ามีการปฏิบัติตามแนวทางปฏิบัติที่ดีที่สุดสำหรับการบันทึกข้อมูลส่วนบุคคลและดำเนินการตลอดเวลา

- ควรแสดงประกาศนโยบายความเป็นส่วนตัวอย่างชัดเจนในพื้นที่พนักงาน เช่น สำนักงาน ห้องประชุม โรงอาหารของพนักงาน ฯลฯ เพื่อเน้นย้ำถึงภาระหน้าที่ของตนต่อเจ้าหน้าที่โรงพยาบาลเกี่ยวกับการเคารพสิทธิในการคุ้มครองข้อมูลของผู้ป่วยอย่างต่อเนื่อง สิ่งนี้ควรเป็นส่วนหนึ่งในการสร้างแรงผลักดันโดยรวมของโรงพยาบาลในการส่งเสริมวัฒนธรรมองค์กรในหมู่พนักงานที่ให้ความสำคัญกับการรักษาความลับของข้อมูลผู้ป่วยอยู่เสมอ

ความเสี่ยง 3 พบว่า บันทึกของผู้ป่วยที่จัดเก็บไว้ในระบบข้อมูลผู้ป่วยอิเล็กทรอนิกส์ที่ทำงานในโรงพยาบาลอาจสามารถเข้าถึงได้จากโรงพยาบาลอื่น ๆ หลายแห่งในพื้นที่ทางภูมิศาสตร์เดียวกัน ในกรณีดังกล่าว ผู้ป่วยจะไม่ได้รับทราบว่าข้อมูลส่วนบุคคลอาจถูกแบ่งปันกับสถานพยาบาลอื่น ๆ กับผู้ควบคุมข้อมูลที่แตกต่างกันในที่อื่น นอกจากนี้ ยังพบว่ามีการปฏิบัติในการย้ายโอนย้ายข้อมูลผู้ป่วยไปยังโรงพยาบาลอื่นในภูมิภาคเดียวกัน โดยไม่แจ้งให้ผู้ป่วยทราบหรือได้รับความยินยอมจากผู้ป่วย จึงมีความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลรายหนึ่งไปยังอีกรายหนึ่งโดยไม่มีพื้นฐานทางกฎหมายในการดำเนินการดังกล่าว ซึ่งดำเนินการไปโดยผู้ป่วยไม่ได้รับแจ้งหรือยินยอมให้มีการถ่ายโอนข้อมูล

คำแนะนำ

- การเข้าถึงข้อมูลผู้ป่วยที่เก็บไว้ในระบบจากสถานพยาบาลอื่น ๆ ในภูมิภาคหรือทางภูมิศาสตร์เดียวกัน ผู้ป่วยควรจะต้องได้รับแจ้งการโอนข้อมูลนั้น โดยอาจใช้แผ่นพับข้อมูลผู้ป่วยที่มอบให้แก่ผู้ป่วยแต่ละราย และควรชี้แจงพื้นฐานทางกฎหมายสำหรับการโอนข้อมูลดังกล่าว

- ในกรณีที่โรงพยาบาลจำเป็นต้องแบ่งปันข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่ละเอียดอ่อนกับสถานพยาบาลอื่น ๆ ในระหว่างการดูแลหรือรักษาผู้ป่วย ผู้ป่วยที่เกี่ยวข้องควรได้รับรู้ถึงความจำเป็นในการแบ่งปันข้อมูลดังกล่าวและให้โอกาสในการได้รับความยินยอม

กรณีศึกษา 12 ความยินยอมสำหรับการวิจัย

บริบท

เข้าใจพื้นฐานแนวคิดเกี่ยวกับการวิจัยและการตรวจสอบทางคลินิกในด้านสุขภาพในลักษณะที่สอดคล้องกับกรอบของกฎหมายคุ้มครองข้อมูล โดยพบข้อเท็จจริงว่า ทางปฏิบัติในโรงพยาบาลแห่งหนึ่ง เจ้าหน้าที่ทางการแพทย์ เช่น พยาบาล หรือแพทย์ ได้รับอนุญาตให้ตรวจสอบแผนภูมิเวชระเบียนข้อมูลผู้ป่วยเพื่อวัตถุประสงค์ในการวิจัยของตนเอง เช่น สำเร็จการศึกษาด้านการแพทย์ ซึ่งไม่มีการขอความยินยอมของผู้ป่วยที่เกี่ยวข้องสำหรับการวิจัยดังกล่าวแต่อย่างใด

ทั้งนี้ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับ (GDPR) ได้กำหนดเงื่อนไขและองค์ประกอบของความยินยอมไว้ในมาตรา 7 (หากเป็นกฎหมายไทย คือ มาตรา 19 และมาตรา 20) โดยหัวใจคือ ผู้ควบคุมข้อมูลต้องทำให้แน่ใจว่า มีการขอความยินยอมโดยชอบ เป็นลายลักษณ์อักษร โดยการขอความยินยอมต้องชัดแจ้ง อยู่ในรูปแบบที่เข้าใจได้ง่าย และเข้าถึงได้ง่าย ใช้ภาษาที่ชัดเจนและเข้าใจง่าย โดยเจ้าของข้อมูลมีสิทธิที่จะเพิกถอนความยินยอมได้ตลอดเวลา และควรได้รับการแนะนำก่อนที่จะให้ความยินยอม และในการเพิกถอนความยินยอมก็จะต้องทำโดยง่ายเช่นกัน

ความเสี่ยง ผู้ป่วยในโรงพยาบาลมีความคาดหวังอย่างสมเหตุสมผลว่าข้อมูลด้านสุขภาพจะถูกเก็บเป็นความลับ และจะไม่ถูกนำไปใช้เพื่อวัตถุประสงค์นอกเหนือจากการดูแลและการรักษาโดยเจ้าหน้าที่ทางการแพทย์ที่ไม่เกี่ยวข้องกับการดูแล การอนุญาตให้เจ้าหน้าที่ทางการแพทย์เข้าถึงแผนภูมิผู้ป่วยหรือข้อมูลผู้ป่วยอื่น ๆ เพื่อวัตถุประสงค์ในการวิจัยสำหรับการศึกษาของตนเองเป็นรูปแบบหนึ่งของการประมวลผลเพิ่มเติมนอกเหนือจากวัตถุประสงค์ที่ได้รับข้อมูล ต้องได้รับความยินยอมโดยเฉพาะจากผู้ป่วย รวมถึงการป้องกันข้อมูลในขณะที่อยู่ในความครอบครองของพนักงานที่เกี่ยวข้อง

คำแนะนำ

- โรงพยาบาลทุกแห่งควรทบทวนแนวทางปฏิบัติในปัจจุบันที่เกี่ยวข้องกับการขอความยินยอมของผู้ป่วยสำหรับการวิจัยและการตรวจทางคลินิก เพื่อให้เป็นไปตามกฎหมาย แนวทางปฏิบัติที่มีอยู่หรือต่อเนื่องใดๆ ที่อนุญาตให้เจ้าหน้าที่ของโรงพยาบาลเข้าถึงแผนภูมิผู้ป่วยหรือข้อมูลผู้ป่วยอื่น ๆ เพื่อวัตถุประสงค์ของ

การศึกษาทางการแพทย์ ควรดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าข้อมูลผู้ป่วยจะไม่ถูกเข้าถึงหรือใช้ในกรณีดังกล่าวโดยปราศจาก ความรู้และความยินยอมของผู้ป่วยที่เกี่ยวข้อง

- ในทุกกรณีที่เจ้าหน้าที่ให้ข้อมูลผู้ป่วยเพื่อการวิจัยและเมื่อได้รับความยินยอมจากผู้ป่วย โรงพยาบาลควรตรวจสอบให้แน่ใจว่ามีการป้องกันที่เหมาะสมเพื่อคุ้มครองข้อมูล และเพื่อให้มั่นใจว่าข้อมูลนั้นถูกเก็บไว้ในสภาพแวดล้อมที่ปลอดภัยภายในโรงพยาบาลทุกครั้ง

บรรณานุกรม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

คณาธิป ทองรวีวงศ์, “คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล”, สำนักพิมพ์นิติธรรม, 2564.

ศูนย์วิจัยและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, “Thailand Data Protection Guideline 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล”, 2564.

Appari, Ajit, and M. Eric Johnson. "Information security and privacy in healthcare: current state of research." *International journal of Internet and enterprise management* 6, no. 4 (2010): 279-314.

Bygrave, Lee A. *Data protection law*. Wolters Kluwer Law & Business, 2002.

Lea, Nathan C., and Filip de Meyer. "How will the general data protection regulation affect healthcare?." *Acta medica portuguesa* 31, no. 7-8 (2018): 363-365.

Long, William, Anna Pavlou, and J. Walsch. "The new EU data protection regulation: What will the impact be on the life sciences industry." *Script Regulatory Affairs* (2012).

Lynskey, Orla. *The foundations of EU data protection law*. Oxford University Press, 2015.

Ortigosa, Adrian Palma, and Sara Lorenzo Cabrera. "Data in the Healthcare Sector." *Eur. J. Privacy L. & Tech.* (2019): 182.

The Data Protection Commissioner, Investigation Report,Data protection investigation in the hospitals sector, May 2018. https://www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC%20-%20Hospitals%20Sector%20Overall%20Report%20_0.pdf

Weerasnghe, Dasun, Muttukrishnan Rajarajan, and Veselin Rakocevic. "Device data protection in mobile healthcare applications." In *International Conference on Electronic Healthcare*, pp. 82-89. Springer, Berlin, Heidelberg, 2008.

PDPA

PERSONAL DATA
PROTECTION ACT

จัดทำขึ้นเพื่อประกอบการอบรมเชิงปฏิบัติการ "การคุ้มครองข้อมูลส่วนบุคคลในสถานพยาบาลภายใต้ พรบ.คุ้มครองข้อมูลส่วนบุคคล"
ระหว่างเดือนตุลาคม - พฤศจิกายน 2564