



เอกสารวิชาการส่วนบุคคล
(Individual Study)

สิทธิในข้อมูลด้านสุขภาพส่วนบุคคล
และแนวทางการจัดการข้อมูลของโรงพยาบาล

จัดทำโดย ผศ.นพ.อิทธิรัตน์ วัชรานานนท์
รหัส ๖๘๑๓๔๘

รายงานนี้เป็นส่วนหนึ่งของการอบรม
หลักสูตร “หลักนิติธรรมเพื่อประชาธิปไตย” (นรป.) รุ่นที่ ๑๓
วิทยาลัยศาลรัฐธรรมนูญ
สำนักงานศาลรัฐธรรมนูญ

ลิขสิทธิ์ของสำนักงานศาลรัฐธรรมนูญ

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศใช้เต็มรูปแบบตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ ซึ่งประมวลกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) มีความสำคัญต่อการจัดการข้อมูลผู้ป่วยในโรงพยาบาล โดยมุ่งเน้นไปที่การปกป้องข้อมูลและสร้างความมั่นใจว่าข้อมูลจะถูกใช้อย่างถูกต้องและปลอดภัย ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้น ไม่ว่าทางตรงหรือทางอ้อม โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและอ่อนไหว ซึ่งมีบทลงโทษที่รุนแรงกรณีข้อมูลรั่วไหลสู่สาธารณะ ดังนั้นผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล อาทิเช่น เจ้าของข้อมูลส่วนบุคคล (ผู้ป่วย) ผู้ควบคุมข้อมูลส่วนบุคคล (แพทย์และโรงพยาบาล) และผู้ประมวลผลข้อมูลส่วนบุคคล (ผู้วิจัย แพทย์ บริษัทประกัน เป็นต้น) จึงต้องทราบรายละเอียดของสิทธิและมีการบริหารจัดการข้อมูลอย่างถูกต้องและเหมาะสม สิทธิของเจ้าของข้อมูล มีตั้งแต่สิทธิขอเข้าถึงข้อมูลส่วนบุคคล สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล สิทธิขอให้ลบหรือทำลาย เพิกถอนความยินยอม และสิทธิในการขอแก้ไขหรือโอนข้อมูลส่วนบุคคล

ในส่วนของผู้ควบคุมข้อมูลและประมวลผลข้อมูลจะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เท่าที่จำเป็น และมีฐานทางกฎหมายรองรับโดยมีรายละเอียดที่เกี่ยวข้องกับการจัดการข้อมูลของโรงพยาบาล ตั้งแต่การได้รับความยินยอม (Consent) การจำกัดวัตถุประสงค์ (Purpose Limitation) การควบคุมขนาดข้อมูล (data minimization) การรักษาความปลอดภัยของข้อมูล (Data Security) สิทธิของผู้ป่วย (Data Subject Rights) การแจ้งเตือนการละเมิดข้อมูล (Data Breach Notification) การปฏิบัติตามกฎหมาย และการตรวจสอบ (Compliance and Audit) รวมถึงนโยบายการเก็บรักษาข้อมูล (Data Retention Policy) การปฏิบัติตามสิทธิในข้อมูลด้านสุขภาพส่วนบุคคลเป็นการสร้างความเชื่อมั่นให้กับผู้ป่วยเกี่ยวกับการจัดการข้อมูลส่วนบุคคล และช่วยลดความเสี่ยงทางกฎหมายที่อาจเกิดขึ้น รวมถึงกรณีศึกษาเรื่องขอหาหรือเกี่ยวกับการขอลบหรือทำลายข้อมูลส่วนบุคคลของโรงพยาบาล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศใช้เต็มรูปแบบตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ โดยก่อนหน้านี้มีประมวลกฎหมายและพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ ที่คุ้มครองข้อมูลของผู้ป่วยอยู่แล้ว เช่น

ประมวลกฎหมายอาญา

มาตรา ๓๒๓ ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่นโดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐

มาตรา ๗ ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์

ของบุคคลนั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้

ประมวลกฎหมายอาญาข้อบังคับแพทยสภาว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพเวชกรรม พ.ศ. ๒๕๔๙ ข้อ ๒๗ ผู้ประกอบวิชาชีพเวชกรรมต้องไม่เปิดเผยความลับของผู้ป่วย หรือผู้ป่วยที่เสียชีวิตแล้วซึ่งตนทราบมาเนื่องจากการประกอบวิชาชีพ เว้นแต่ได้รับความยินยอมโดยชอบด้วยกฎหมาย หรือเมื่อต้องปฏิบัติตามกฎหมายหรือตามหน้าที่

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

“เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”

มาตรา ๑๕ ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายประกอบกัน รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกรานสิทธิส่วนบุคคลโดยไม่ควร ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย...

แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีรายละเอียดมากขึ้นในเรื่องของหลักการเพิ่มเติม เงื่อนไขและหน้าที่ของผู้ใช้ข้อมูล สิทธิที่เจ้าของข้อมูลพึงมี นอกจากนี้กฎหมายฉบับนี้ไม่ได้ห้ามเก็บ ห้ามใช้ หรือห้ามเปิดเผยข้อมูลส่วนบุคคล แต่เป็นการกำกับให้ทำด้วยความระมัดระวัง และคุ้มครองเจ้าของข้อมูลมากขึ้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

มาตรา ๕ พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยผู้ควบคุม ข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

มาตรา ๖ ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ประกอบไปด้วย

๑. เจ้าของข้อมูลส่วนบุคคล เช่น ผู้ป่วย หรือผู้ปกครอง
๒. ผู้ควบคุมข้อมูลส่วนบุคคล เช่น แพทย์ และโรงพยาบาล
๓. ผู้ประมวลผลข้อมูลส่วนบุคคล เช่น ผู้วิจัย แพทย์ บริษัทประกัน เป็นต้น

ด้านการคุ้มครองข้อมูลส่วนบุคคล ได้มีบัญญัติใน หมวด ๒ ดังนี้

ส่วนที่ ๑ บททั่วไป

มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้ หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องกระทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยมนั้นต้อง แยกส่วนออกจากข้อความอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่ อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจในวัตถุประสงค์ดังกล่าว ทั้งนี้คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบ และข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อ การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้ว โดยชอบตาม ที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

๑. วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึง วัตถุประสงค์ ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๒. แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือ สัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

๓. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

๔. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

๕. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

๑. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ตามที่คณะกรรมการประกาศกำหนด

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๔. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๕. เป็นความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของ บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่า สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๖. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนดโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

๑. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

๒. เป็นการดำเนินการกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือ

องค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

๓. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๔. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๕. เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสาธารณสุขหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคม สงเคราะห์ ทั้งนี้ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้น ว่าเป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคมซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตาหรือข้อมูลจำลองลายนิ้วมือ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตาม

กฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่ คณะกรรมการประกาศกำหนด

ส่วนที่ ๓ เรื่องการใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา ๒๗ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับ ยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ด้านสิทธิของเจ้าของข้อมูล มีตั้งแต่สิทธิขอเข้าถึงข้อมูลส่วนบุคคล สิทธิคัดค้านการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สิทธิขอให้ลบ หรือทำลาย เพิกถอนความยินยอม และสิทธิ ในการขอแก้ไขหรือโอนข้อมูลส่วนบุคคล ดังที่ได้ระบุไว้ใน หมวด ๓ พระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. ๒๕๖๒ ว่าด้วยเรื่อง สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา ๓๐ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคลที่ เกี่ยวกับตน ซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่ง ข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอ ตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็น การ ปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อโอกาสก่อให้เกิดความเสียหาย ต่อสิทธิและเสรีภาพของบุคคลอื่น

มาตรา ๓๑ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุม ข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่ สามารถอ่านหรือ ใช้งานโดยทั่วไปได้โดยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยวิธีการอัตโนมัติ รวมทั้งมีสิทธิ ดังต่อไปนี้

(๑) ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยัง ผู้ควบคุม ข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้โดยวิธีการอัตโนมัติ

(๒) ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบ ดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

มาตรา ๓๒ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้

(๑) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับข้อยกเว้นไม่ต้องขอความยินยอม ตาม มาตรา ๒๔(๔) หรือ (๕) เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า

(ก) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้ แสดงให้ เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า

(ข) การเก็บรวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตาม กฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้ สิทธิเรียกร้องตามกฎหมาย

(๒) กรณีที่เป็น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาด แบบตรง

(๓) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษา วิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ และสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์ สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๓๓ เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจตามกฎหมายที่จะเรียกเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(๓) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๓๒(๑) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา ๓๒(๑)(ก) หรือ (ข) หรือ เป็นการคัดค้านตามมาตรา ๓๒(๒)

(๔) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

มาตรา ๓๔ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา ๓๖

(๒) เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา ๓๓(๔) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน

(๓) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา ๓๒(๑) หรือตรวจสอบตาม มาตรา ๓๒(๓) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๓๒ วรรคสาม

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

ในส่วนของผู้ควบคุมข้อมูลและประมวลผลข้อมูล จะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นและมีฐานทางกฎหมายรองรับ ตามมาตราที่

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพ

ในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔(๑) หรือ (๔) หรือมาตรา ๒๖(๕)(ก) หรือ (ข) การใช้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ให้นำความในมาตรา ๓๓ วรรคห้ามาใช้บังคับกับการลบ หรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(๕) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำ

การแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) จัดทำและเก็บรักษาบันทึกรายงานของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักการ และวิธีการที่คณะกรรมการประกาศกำหนด

ทำให้สรุปได้ว่า ฐานทางกฎหมายรองรับ ตามมาตรา ๒๔ ที่รองรับข้อมูลในเรื่องดังต่อไปนี้

๑. Archiving, research or statistics เพื่อประโยชน์สาธารณะ หรือเกี่ยวกับการศึกษาวิจัย สถิติ

๒. Vital interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต

๓. Contractual Performance เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

๔. Public Task เพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๕. Legitimate interest เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

๖. Legal Obligation เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

การบริหารจัดการข้อมูลของโรงพยาบาลเพื่อปกป้องข้อมูลส่วนตัวของผู้ป่วยและจัดการกับการใช้งานข้อมูลเหล่านั้นอย่างเหมาะสมมีรายละเอียดที่สำคัญดังนี้

หลักการของการขอความยินยอม (Consent)

การขอความยินยอมจากผู้ป่วยภายใต้ประมวลกฎหมายเป็นขั้นตอนที่สำคัญ และจำเป็นสำหรับโรงพยาบาลซึ่งการขอความยินยอมนี้มีรายละเอียดที่สำคัญคือ

๑.๑ ความชัดเจนและโปร่งใส โรงพยาบาลต้องมีการชี้แจงข้อมูลให้ผู้ป่วยเข้าใจว่าข้อมูลอะไรบ้างจะถูกเก็บรวบรวมใช้และเปิดเผยและเพื่อวัตถุประสงค์ใดในการรักษาหรือบริการทางการแพทย์

๑.๒ การยินยอมที่สามารถเรียกคืนได้ ผู้ป่วยมีสิทธิ์ที่จะเปลี่ยนแปลงหรือถอดความยินยอมที่ได้ให้ไว้ก่อนหน้านี้ได้ตลอดเวลาโดยไม่ต้องแจ้งให้โรงพยาบาลทราบ

๑.๓ การให้ความยินยอมอย่างอิสระ ความยินยอมต้องถูกต้องและไม่ถูกบังคับ ผู้ป่วยต้องมีเสรีภาพในการตัดสินใจโดยไม่ถูกกดดัน

๑.๔ การให้ข้อมูลที่เหมาะสม โรงพยาบาลต้องให้ข้อมูลที่ชัดเจนเกี่ยวกับการใช้และการเก็บรักษาข้อมูล เช่น ความเสี่ยงที่อาจเกิดขึ้น การป้องกันข้อมูล และสิทธิ์ต่าง ๆ ของผู้ป่วย ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประเภทของความยินยอม

๑. ความยินยอมทั่วไป ใช้สำหรับการเก็บรวบรวมข้อมูลที่เป็นมาตรฐานเช่นข้อมูลประวัติสุขภาพทั่วไป การรักษาเบื้องต้น

๒. ความยินยอมเฉพาะ ใช้เมื่อมีการเก็บรวบรวมข้อมูลที่มีความละเอียดอ่อนหรือข้อมูลที่มีผลกระทบสูงต่อความเป็นส่วนตัวของผู้ป่วย เช่น ข้อมูลทางการแพทย์ที่ละเอียดอ่อน ต้องมีการขอความยินยอมเฉพาะเจาะจง

ขั้นตอนการขอความยินยอม

๑. การแจ้ง โรงพยาบาลจะต้องแจ้งให้ผู้ป่วยทราบเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล รวมถึงการให้รายละเอียดเกี่ยวกับสิทธิของผู้ป่วย

๒. การขอความยินยอม ต้องมีรูปแบบการขอความยินยอมที่ชัดเจน ซึ่งอาจเป็นเอกสาร หรือในรูปแบบดิจิทัล

๓. การเก็บบันทึก โรงพยาบาลต้องมีการเก็บบันทึกเกี่ยวกับความยินยอมที่ได้รับ เช่น วันที่ เวลา วิธีการที่ผู้ป่วยให้ความยินยอม โดยสามารถใช้เพื่อการตรวจสอบในอนาคตได้

หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)

๑. ต้องมีวัตถุประสงค์ที่ชัดเจน โรงพยาบาลต้องกำหนดวัตถุประสงค์ในขณะที่เก็บรวบรวมข้อมูล ต้องมีการระบุว่าข้อมูลจะถูกนำไปใช้เพื่อทำอะไร เช่น การรักษา การวินิจฉัย การติดตามสุขภาพหรือบริการทางการแพทย์

๒. ต้องเป็นไปตามกฎหมาย วัตถุประสงค์ที่กำหนดไว้ต้องไม่ขัดต่อกฎหมายหรือเป็นการละเมิดสิทธิของผู้ป่วย

๓. การใช้ข้อมูลตามวัตถุประสงค์ที่กำหนดข้อมูลที่เก็บรวบรวมจะต้องถูกนำไปใช้เพื่อวัตถุประสงค์ที่ระบุไว้เท่านั้น การใช้ข้อมูลในวัตถุประสงค์อื่น ๆ จะต้องได้รับความยินยอมเพิ่มเติมจากผู้ป่วย

๔. ไม่ควรเก็บข้อมูลเกินกว่าที่จำเป็น การเก็บรวบรวมข้อมูลควรเป็นไปในระดับที่จำเป็นต่อวัตถุประสงค์ที่ตั้งไว้ ไม่ควรเก็บข้อมูลเพิ่มเติมที่ไม่เกี่ยวข้อง

๕. การแจ้งผู้ป่วย โรงพยาบาลต้องแจ้งให้ผู้ป่วยทราบเกี่ยวกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูล โดยเฉพาะอย่างยิ่งเมื่อข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อน เช่น ข้อมูลทางการแพทย์

ความสำคัญของการจำกัดวัตถุประสงค์

ปกป้องสิทธิของผู้ป่วย : การจำกัดวัตถุประสงค์ช่วยปกป้องความเป็นส่วนตัวของผู้ป่วย และทำให้ผู้ป่วยมีความมั่นใจว่าข้อมูลของพวกเขาจะถูกใช้ไปในทางที่เหมาะสม

ลดความเสี่ยงทางกฎหมาย : ประการสำคัญคือการปฏิบัติตามหลักการนี้ช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากการถูกฟ้องร้องหรือการถูกสอบสวนจากหน่วยงานที่เกี่ยวข้อง

หลักการลดข้อมูล (Data Minimization)

การลดข้อมูล (Data Minimization) หลักการสำคัญภายใต้ประมวลกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับการจัดการข้อมูลของผู้ป่วยในโรงพยาบาล โดยหลักการนี้มีรายละเอียดคือ

๑. **การเก็บรวบรวมข้อมูลที่จำเป็น** โรงพยาบาลควรเก็บรวบรวมเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต่อการให้บริการทางการแพทย์ การรักษา หรือการวินิจฉัยเท่านั้น ซึ่งหมายความว่าไม่ควรเก็บข้อมูลที่ไม่มีความเกี่ยวข้องหรือไม่จำเป็นต้องใช้

๒. **การประเมินความจำเป็น** ก่อนที่จะเก็บรวบรวมข้อมูลใด ๆ โรงพยาบาลต้องประเมินว่าข้อมูลนั้นมีความจำเป็นหรือไม่ต่อวัตถุประสงค์ที่ตั้งไว้ เช่น หากข้อมูลที่เก็บรวบรวมไม่ช่วยในการรักษาหรือดูแลผู้ป่วยแล้ว ควรหลีกเลี่ยงที่จะเก็บข้อมูลเหล่านั้น

๓. **การจัดการข้อมูลในระดับที่เหมาะสม** การเก็บข้อมูลควรอยู่ในระดับที่เหมาะสมและไม่เกินความจำเป็น เช่น ไม่ควรเก็บข้อมูลส่วนบุคคลในจำนวน มากเกินไป ซึ่งอาจทำให้เพิ่มความเสี่ยงในการจัดการข้อมูล

๔. **ข้อมูลที่มีความละเอียดอ่อน** สำหรับข้อมูลที่เกี่ยวข้องกับสุขภาพหรือข้อมูลที่มีความละเอียดอ่อน โรงพยาบาลต้องมีมาตรการเพิ่มเติมใน การประมวลผลและรักษาความปลอดภัยของข้อมูลเหล่านั้น ขั้นตอนการลดข้อมูลจึงควรให้ความสำคัญกับ การปกป้องข้อมูลเหล่านี้เป็นพิเศษ

๕. **การกำหนดระยะเวลาในการเก็บข้อมูล** โรงพยาบาลควรกำหนดระยะเวลาในการเก็บข้อมูล และเมื่อข้อมูลไม่จำเป็นต้องใช้งานอีกต่อไป ต้องมีมาตรการในการลบหรือทำลายข้อมูลนั้นอย่างเหมาะสม

ความสำคัญของการลดข้อมูล

ปกป้องความเป็นส่วนตัว : การลดข้อมูลช่วยปกป้องข้อมูลส่วนบุคคลของผู้ป่วย ทำให้มีการจัดการข้อมูลที่มีความปลอดภัยและเป็นส่วนตัวมากขึ้น

ลดความเสี่ยงในการละเมิดข้อมูล : การลดจำนวนข้อมูลที่เก็บรวบรวม ช่วยลดความเสี่ยงในการเกิดการละเมิดข้อมูล ซึ่งอาจเกิดจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือลักลอบข้อมูล

ปรับปรุงประสิทธิภาพการจัดการข้อมูล : การเก็บข้อมูลที่จำเป็นและเหมาะสมช่วยให้การจัดการข้อมูลในระบบภายในมีประสิทธิภาพมากขึ้น

มาตรการรักษาความปลอดภัย (Data security measures)

มาตรการรักษาความปลอดภัยภายใต้ประมวลกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความสำคัญอย่างยิ่ง สำหรับโรงพยาบาลเนื่องจากเกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลของผู้ป่วยที่มีความละเอียดอ่อนมาก ดังนั้นโรงพยาบาลจึงต้องดำเนินการตามมาตรการต่าง ๆ ดังนี้

๑. **การพัฒนา นโยบายการรักษาความปลอดภัยข้อมูล** โรงพยาบาลควรกำหนดและจัดทำเอกสารนโยบายเกี่ยวกับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เพื่อให้เจ้าหน้าที่ทุกคนเข้าใจ และสามารถปฏิบัติตามได้

๒. **การเข้าถึงข้อมูล** กำหนดสิทธิและการเข้าถึงข้อมูลส่วนบุคคล โดยอนุญาตให้เฉพาะผู้ที่มีสิทธิ์ในการเข้าถึงเท่านั้น เช่น แพทย์ หรือพนักงานที่เกี่ยวข้องกับการใช้ข้อมูลนั้น ๆ

๓. **การใช้เทคโนโลยีรักษาความปลอดภัย ใช้เทคโนโลยีที่เหมาะสม** เช่น การเข้ารหัสข้อมูล (Encryption) ระบบระบบการยืนยันตัวตน (Authentication systems) และไฟร์วอลล์ (Firewalls) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. **การฝึกอบรมเจ้าหน้าที่** จัดหลักสูตรฝึกอบรมและเพิ่มความรู้เกี่ยวกับการรักษาความปลอดภัยข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่ เพื่อให้เข้าใจถึงความสำคัญของการปกป้องข้อมูลและวิธีการปฏิบัติ

๕. การจัดการความเสี่ยง ดำเนินการประเมินความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล และวางแผนการจัดการ ความเสี่ยงให้เหมาะสม โดยอาจรวมถึงการตรวจสอบและทดสอบระบบความปลอดภัยเป็นระยะ ๆ

๖. การสร้างระบบจัดเก็บและจัดการข้อมูลที่ปลอดภัย สร้างโครงสร้างในการเก็บรักษาข้อมูลทั้งในรูปแบบดิจิทัลและกระดาษอย่างถูกต้อง เช่น การเก็บข้อมูลใน พื้นที่ที่ปลอดภัย และการทำลายข้อมูลที่ไม่จำเป็นอย่างถูกต้อง

๗. การตรวจสอบและติดตามการเข้าถึงข้อมูล ติดตามการเข้าถึงข้อมูลอย่างสม่ำเสมอ เพื่อจัดการและระบุการเข้าใช้ที่น่าสงสัยหรือผิดปกติ

๘. การแจ้งเตือนเมื่อเกิดเหตุการณ์ละเมิดข้อมูล มีมาตรการในการแจ้งเตือนในกรณีที่เกิดการละเมิดข้อมูล โดยต้องแจ้งให้ผู้ป่วยและหน่วยงานที่เกี่ยวข้อง ทราบอย่างรวดเร็วและเหมาะสม

ความสำคัญของมาตรการรักษาความปลอดภัย

สร้างความเชื่อมั่น : การมีมาตรการรักษาความปลอดภัยที่เข้มงวดช่วยสร้างความเชื่อมั่นให้กับผู้ป่วยว่า ข้อมูลของพวกเขาจะได้รับการปกป้อง

ปฏิบัติตามกฎหมาย : การรักษาความปลอดภัยในข้อมูลช่วยให้โรงพยาบาลปฏิบัติตามกฎหมายและลดความเสี่ยงทางกฎหมาย

ปกป้องข้อมูลที่ละเอียดอ่อน : มาตรการเหล่านี้ช่วยลดความเสี่ยงในการละเมิดหรือการสูญหายของข้อมูลที่ละเอียดอ่อน

สิทธิของผู้ป่วยตามประมวลกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ภายใต้ประมวลกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ป่วยมีสิทธิหลายประการที่มีความสำคัญในการปกป้อง ข้อมูลส่วนบุคคลของตนในโรงพยาบาลดังนี้

๑. สิทธิในการเข้าถึงข้อมูล (Right to Access) ผู้ป่วยมีสิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลของตนที่โรงพยาบาลเก็บรวบรวม โดยสามารถขอข้อมูลว่าจะ มีข้อมูลอะไรเกี่ยวกับตนบ้างและสามารถได้รับสำเนาขอข้อมูลนั้น

๒. สิทธิในการแก้ไขข้อมูล (Right to Rectification) ผู้ป่วยสามารถขอให้โรงพยาบาลแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่ครบถ้วนได้ หากข้อมูลนั้นมีผลกระทบต่อการรักษาหรือบริการที่ได้รับ

๓. สิทธิในการลบข้อมูล (Right to Erasure) ผู้ป่วยมีสิทธิ ในการขอลบข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องใช้งานหรือในกรณีที่ได้อนุญาตยินยอมในการ ประมวลผลข้อมูลดังกล่าว

๔. สิทธิในการจำกัดการประมวลผล (Right to Restrict Processing) ผู้ป่วยสามารถขอให้โรงพยาบาลจำกัดการประมวลผลข้อมูลส่วนบุคคลของตนได้ในบางกรณี เช่น เมื่อกำลังตรวจสอบความถูกต้องของข้อมูล

๕. สิทธิในการขอรับข้อมูล (Right to Data Portability) ผู้ป่วยมีสิทธิในการขอให้ข้อมูลส่วนบุคคลของตนถูกส่งต่อไปยังผู้ควบคุมข้อมูลอื่น หรือรับข้อมูลในรูปแบบที่ สามารถอ่านได้ในระบบคอมพิวเตอร์ เพื่อสะดวกในการโอนย้ายข้อมูล

๖. สิทธิในการถอนความยินยอม (Right to Withdraw Consent) ผู้ป่วยสามารถถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ได้ให้ไว้ในทันที โดยจะต้องมีการแจ้งให้โรงพยาบาลทราบ

ความหมายของการถอนความยินยอม : ผู้ป่วยมีสิทธิในการถอนความยินยอมที่เคยให้ไว้ในการเก็บรวบรวม ใช้ หรือประมวลผลข้อมูลส่วนบุคคลของตนตลอดเวลา โดยไม่มีผลกระทบใด ๆ ต่อสิทธิที่ได้รับในการรักษา หรือบริการที่โรงพยาบาลมอบให้

วิธีการถอนความยินยอม : ผู้ใช้บริการสามารถแจ้งความต้องการโดยใช้ช่องทางการแจ้งถอนความยินยอมที่ระบุไว้ในเอกสาร หรือช่องทางอื่นตามที่โรงพยาบาลกำหนด ในกรณีที่ไม่มีกำหนดช่องทาง ผู้ใช้บริการสามารถแจ้งความต้องการผ่านช่องทางติดต่อโรงพยาบาล หรือเจ้าหน้าที่ที่ให้บริการได้โดยตรง

ผลกระทบเมื่อถอนความยินยอม : เมื่อผู้ใช้ขอถอนความยินยอม โรงพยาบาลจะต้องยุติการประมวลผล ข้อมูลส่วนบุคคลของผู้ใช้ ยกเว้นในกรณีที่มีเหตุผลอันสมควรหรือมีหน้าที่ที่ต้องปฏิบัติตามกฎหมายต่อไป หากถอนความยินยอมแล้ว ไม่มีผลกระทบกับการให้บริการประมวลผลที่ได้ดำเนินการภายใต้ความยินยอมก่อนหน้านี้

การรักษาความปลอดภัยของข้อมูล : โรงพยาบาลมีหน้าที่ต้องรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลที่เกี่ยวข้องตามมาตราฐานที่กฎหมายกำหนด โดยต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามที่กฎหมาย PDPA

การแจ้งข้อมูลให้กับผู้ป่วย : โรงพยาบาลต้องแจ้งให้ผู้ป่วยทราบเกี่ยวกับสิทธินี้รวมถึงขั้นตอนในการถอนความยินยอมในรูปแบบที่ชัดเจนและเข้าใจง่าย เช่น ในข้อกำหนดหรือเอกสารที่เกี่ยวข้องกับการให้ความยินยอม ความสำคัญของสิทธิในการถอนความยินยอม ปกป้องสิทธิของผู้ใช้ สิทธิในการถอนความยินยอมทำให้ผู้ใช้สามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้มากขึ้น

สร้างความเชื่อมั่น : ผู้ป่วยจะรู้สึกสบายใจมากขึ้นเมื่อรู้ว่าสามารถถอนความยินยอมได้หากไม่พอใจกับการจัดการข้อมูลของตน

เพิ่มความโปร่งใส : ตลอดจนช่วยเสริมสร้างความเชื่อมั่นในระบบการดูแลสุขภาพเมื่อผู้ป่วยสามารถควบคุมข้อมูลส่วนบุคคลได้

๗. สิทธิในการร้องเรียน (Right to Complain) ผู้ป่วยมีสิทธิในการร้องเรียนต่อหน่วยงานที่รับผิดชอบเรื่องการคุ้มครองข้อมูลส่วนบุคคล หากรู้สึกว่าคุณสมบัติข้อมูลส่วนบุคคลของตนถูกละเมิดหรือไม่ได้รับการปฏิบัติตามที่กฎหมายคุ้มครอง

ความสำคัญของสิทธิของผู้ป่วย

สร้างความเชื่อมั่น : การมีสิทธิที่ชัดเจนช่วยเสริมสร้างความเชื่อมั่นให้กับผู้ป่วยในระบบการดูแลสุขภาพ

ปกป้องข้อมูลส่วนบุคคล : สิทธิเหล่านี้เป็นมาตรการที่ช่วย ปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ป่วย

ให้ความโปร่งใส : ช่วยให้ข้อมูลเกี่ยวกับการจัดการข้อมูลส่วนบุคคลมีความโปร่งใสและชัดเจน

การแจ้งเตือนเมื่อเกิดการละเมิดข้อมูล

ความหมายของการละเมิดข้อมูล

การละเมิดข้อมูลส่วนบุคคล หมายถึง เหตุการณ์ที่มีการเข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือการส่งข้อมูลสูญหายหรือเสียหาย ซึ่งอาจส่งผลกระทบต่อความเป็นส่วนตัวหรือความปลอดภัยของข้อมูลผู้ป่วย

การแจ้งเตือนเจ้าของข้อมูลเมื่อมีการละเมิดข้อมูล

ในกรณีที่เกิดการละเมิดข้อมูล โรงพยาบาลต้องแจ้งให้ผู้ที่ได้รับผลกระทบ เช่น ผู้ป่วย และหน่วยงานที่รับผิดชอบ (ในประเทศไทยคือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) ทราบโดยเร็วที่สุดโดยทั่วไปจะต้องดำเนินการภายในระยะเวลาที่กำหนด (ปกติไม่เกิน ๗๒ ชั่วโมง)

ข้อมูลที่ต้องระบุในการแจ้งเตือน

โรงพยาบาลจะต้องให้ข้อมูลในการแจ้งเตือนที่ชัดเจนและครบถ้วนรวมถึง

- รายละเอียดของข้อมูลที่ถูกละเมิด
- ข้อมูลเกี่ยวกับสาเหตุของการละเมิด
- ผลกระทบที่อาจเกิดขึ้นกับผู้ป่วย
- มาตรการที่ได้ดำเนินการเพื่อแก้ไขสถานการณ์
- มาตรการที่ผู้ป่วยควรดำเนินการหรือติดต่อเพื่อป้องกันความเสี่ยง

การดำเนินการแก้ไข

นอกจากการแจ้งเตือน โรงพยาบาลต้องมีการดำเนินการที่เหมาะสมเพื่อแก้ไขปัญหาและให้ข้อมูลเพิ่มเติมแก่ผู้ป่วยรวมถึงมาตรการป้องกันไม่ให้เกิดเหตุการณ์ดังกล่าวเกิดขึ้นอีกในอนาคต

การจัดเก็บบันทึก

โรงพยาบาลต้องเก็บบันทึกหลักฐานที่เกี่ยวกับเหตุการณ์การละเมิดข้อมูล รวมถึงการแจ้งเตือนและแนวทาง การที่ได้ดำเนินการไปเพื่อความชัดเจนและการตรวจสอบในอนาคต

ความสำคัญของการแจ้งเตือนเมื่อเกิดการละเมิดข้อมูล

คุ้มครองสิทธิของผู้ป่วย : การแจ้งเตือนทำให้ผู้ป่วยสามารถรู้เท่าทันต่อการละเมิดและสามารถดำเนินการเพื่อการป้องกันและแก้ไขเหตุการณ์

สร้างความไว้วางใจ : โรงพยาบาลที่มีการแจ้งเตือนอย่างโปร่งใส และมีมาตรการแจ้งเตือนที่ชัดเจนย่อมได้รับความเชื่อถือแก่ผู้รับบริการมากขึ้น ปฏิบัติตามกฎหมายการแจ้งเตือนช่วยให้หน่วยงานปฏิบัติตาม PDPA อย่างถูกต้อง และช่วยลดความเสี่ยงทางกฎหมายที่อาจเกิดขึ้น

การปฏิบัติตามกฎหมาย (Compliance)

การพัฒนาแผนและแนวปฏิบัติ :

โรงพยาบาลต้องมีแผนการดำเนินการที่สอดคล้องกับแนวทางปฏิบัติ PDPA ซึ่งรวมถึงขั้นตอนการบริหาร จัดการ ข้อมูลส่วนบุคคล การควบคุมข้อมูล การรักษาความลับ และการแจ้งเตือนเมื่อมีการละเมิดข้อมูล

การฝึกอบรมบุคลากร :

การอบรมให้กับเจ้าหน้าที่ทุกคนทราบและเข้าใจในข้อกำหนดที่เกี่ยวข้องกับ PDPA เพื่อให้สามารถดำเนินการภายใต้การปฏิบัติตามกฎหมายได้อย่างถูกต้อง และการป้องกันการละเมิดข้อมูล

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล :

โรงพยาบาลต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) เพื่อดูแลและรับผิดชอบในการคุ้มครองข้อมูลตามกฎหมาย PDPA

การตรวจสอบ (Auditing)

การตรวจสอบภายใน :

โรงพยาบาลต้องมีการดำเนินการตรวจสอบภายในเกี่ยวกับการปฏิบัติตามโดยเฉพาะมาตรการในการปกป้องข้อมูลตาม PDPA โดยอาจมีการตรวจสอบเป็นระยะ ๆ เพื่อให้แน่ใจว่าการปฏิบัติเป็นไปอย่างมีประสิทธิภาพ

การประเมินความเสี่ยง

การประเมินความเสี่ยงที่อาจเกิดขึ้นจากการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งจะช่วยให้อาจารย์สามารถวางมาตรการป้องกันและลดความเสี่ยงได้อย่างเหมาะสม

การรวบรวมและบันทึกผล

ต้องมีการจัดทำรายงานที่เกี่ยวกับผลการตรวจสอบและประเมินความเสี่ยง ซึ่งจะช่วยในการประเมิน และปรับปรุงระบบการดูแลข้อมูลส่วนบุคคล

การตอบสนองต่อการสอบถามจากหน่วยงานภายนอก

หากมีการตรวจสอบจากหน่วยงานจากภาครัฐหรือองค์กรที่เกี่ยวข้อง เช่น สำนักงานคุ้มครองข้อมูลส่วนบุคคล (PDPC) โรงพยาบาลต้องให้ความร่วมมือในการให้ข้อมูลและหลักฐานที่เกี่ยวข้อง

ความสำคัญของการปฏิบัติตามกฎหมายและการตรวจสอบ

การรักษามาตรฐาน : การปฏิบัติตามกฎหมายช่วยรักษามาตรฐานที่ดีเกี่ยวกับข้อมูลส่วนบุคคลของหน่วยงาน และให้บริการที่ปลอดภัยแก่ประชาชน

ลดความเสี่ยงทางกฎหมาย : การปฏิบัติตาม PDPA ช่วยลดความเสี่ยงทางกฎหมายจากข้อร้องเรียนหรือการฟ้องร้อง

ปรับปรุงการจัดการข้อมูล : การตรวจสอบและประเมินจะช่วยทำให้โรงพยาบาลสามารถปรับปรุงกระบวนการในการจัดการข้อมูลส่วนบุคคลได้ต่อเนื่องอย่างมีประสิทธิภาพ

นโยบายการจัดเก็บข้อมูล

โรงพยาบาลมีความจำเป็นต้องเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการให้บริการตรวจรักษาทางการแพทย์และสาธารณสุข วินิจฉัยโรค วางแผนการรักษา และให้การดูแลสุขภาพ ติดต่อผู้ป่วยหรือผู้เกี่ยวข้องในกรณีฉุกเฉิน ดำเนินการทางบัญชี การเบิกจ่าย และประกันสุขภาพ รวมถึงรายงานหรือส่งต่อข้อมูลต่อหน่วยงานของรัฐตามข้อกำหนดกฎหมายกำหนด ดังนั้นโรงพยาบาลควรกำหนด นโยบายเกี่ยวกับข้อมูลส่วนบุคคลที่จะเก็บรวบรวม ระยะเวลาการเก็บรักษาข้อมูล และ การจำกัดข้อมูลที่ไม่จำเป็นต้องใช้งานอีกต่อไป

โดยปกติโรงพยาบาลจะเก็บรักษาข้อมูลส่วนบุคคลของผู้ป่วยไว้ในระยะเวลาที่เหมาะสมกับวัตถุประสงค์ของการให้บริการและอาจเก็บไว้ต่อเมื่อมีกฎหมายกำหนดเช่นเวชระเบียนที่ต้องเก็บไว้อย่างน้อย ๕ ถึง ๑๐ ปี หรือมากกว่านั้นตามลักษณะของข้อมูล

ดังนั้นโรงพยาบาลต้องมีมาตรการทั้งทางทางเทคนิคและองค์กรในการรักษาความปลอดภัยของข้อมูล เช่น การเข้ารหัสข้อมูล การควบคุมสิทธิเข้าถึงระบบสารสนเทศ และฝึกอบรมบุคลากรให้ตระหนักถึงความปลอดภัยของข้อมูล

จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ทำให้เราสรุปข้อพึงปฏิบัติสำหรับเจ้าหน้าที่ บุคลากรทางด้านสาธารณสุขในการปฏิบัติงานดังตารางด้านล่างนี้

สิ่งที่พึงปฏิบัติ	สิ่งที่ไม่พึงปฏิบัติ
คิดถึงความจำเป็นก่อนเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วย	เก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วย โดยที่ไม่ ได้ไตร่ตรองให้รอบคอบ
การเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วย หากไม่ต้องระบุตัวตนด้วยชื่อ Hospital number (HN) หรือสิ่งอื่น ๆ ก็ช่วยลดความเสี่ยงและไม่ต้องทำตามกฎ PDPA	คิดว่า HN, ID หรือข้อมูลอื่น ๆ ไม่ได้เป็นข้อมูลส่วนบุคคล และสามารถทำอะไรกับข้อมูลนั้นก็ได้
เก็บรักษาข้อมูลที่อยู่ในความดูแลให้ปลอดภัยและลบทิ้งเมื่อหมดความจำเป็นต้องใช้	เก็บสำเนาข้อมูลหลายชุดแล้วไม่ได้ลบเมื่อใช้เสร็จ หรือ สำเนาโดยปราศจากการปกปิดข้อมูลหรือจำกัดผู้เข้าใช้ ทำให้เสี่ยงต่อการรั่วไหลของข้อมูล
หากผู้ป่วยขอสำเนา ขอแก้ไข ขอคัดค้านการเก็บ ใช้ หรือเปิดเผยข้อมูล หรือขอลบข้อมูล ให้ผู้ป่วยติดต่อที่ หน่วยงานที่เกี่ยวข้อง เช่น แผนกเวชระเบียน หรือสำนักงานฝ่ายบริหารของโรงพยาบาล	เพื่อผู้ป่วยขอใช้สิทธิตาม PDPA ก็ปฏิเสธไปในทันที โดยไม่ได้ตรวจสอบข้อกำหนดให้รอบคอบ
ในกรณีที่จำเป็นต้องเปิดเผยข้อมูลให้หน่วยงานภายนอกที่มีอำนาจตามกฎหมายได้ตามปกติ แต่ต้องตรวจสอบความจำเป็นและดูแลให้รอบคอบรัดกุม	อ้าง PDPA ในการไม่เปิดเผยข้อมูลที่เป็นต้องเปิดเผย เช่น ให้กองทุนประกันสุขภาพ หรือหน่วยงานที่มีอำนาจตามกฎหมาย

ขอเอกสารรับความยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลเฉพาะกรณีทีพิจารณาแล้วไม่เข้าฐานทางกฎหมายอื่น ๆ	ขอเอกสารรับความยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วยทุกอย่าง ทำให้มีปัญหาเมื่อผู้ป่วยขอถอนเอกสารรับความยินยอมหรือขอลบข้อมูล
หากต้องขอเอกสารรับความยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลต้องปฏิบัติให้ถูกต้องตามมาตรา ๑๙	บังคับให้ผู้ป่วยเซ็นเอกสารให้การยินยอม
การสื่อสารข้อมูลผู้ป่วยผ่านแอปพลิเคชันต่าง ๆ เช่น LINE สามารถทำได้แต่ขอให้ดูแลให้รัดกุมเปิดเผย ให้รู้เท่าที่จำเป็น และปฏิบัติตามนโยบายขององค์กร เช่น ไม่ส่งต่อในกลุ่มที่ไม่จำเป็น ถ้ามีการปรึกษาก็ควรส่งให้แพทย์ผู้เกี่ยวข้องโดยตรง	ส่งข้อมูลผู้ป่วยเข้าในกลุ่ม LINE ที่มีคนอื่นที่ไม่จำเป็นต้องรู้ข้อมูลผู้ป่วยอยู่เป็นจำนวนมากโดยไม่มีเหตุผลอันสมควร
เวลาที่มีบุคคลผู้มีชื่อเสียงมารักษาที่โรงพยาบาลก็ปฏิบัติเหมือนผู้ป่วยทุกคน รักษาความลับ เข้าถึงข้อมูลเฉพาะในการปฏิบัติหน้าที่ และไม่เปิดเผยข้อมูลให้คนที่ไม่มี ความจำเป็นต้องทราบ	ไปดูข้อมูลของบุคคลผู้มีชื่อเสียงที่มารักษาโดยที่ตนเองไม่ได้เกี่ยวข้องกับการรักษานั้น

ข้อพึงระวังอื่น ๆ ในขณะปฏิบัติงานในโรงพยาบาล

๑. ไม่คุยเรื่องคนไข้ที่ข้างเตียงผู้ป่วยท่านอื่น และไม่คุยเรื่องข้อมูลละเอียดอ่อนระหว่างทำงานที่เตียงผู้ป่วย
๒. เมื่อสั่งการรักษาเสร็จเรียบร้อยแล้ว ให้ออกจากแอปพลิเคชันอย่าเปิดหน้าจอทิ้งไว้
๓. ระวังเรื่องการคุย การแซท การโพสต์สิ่งที่เกี่ยวข้องกับผู้ป่วยและสามารถระบุตัวตนได้
๔. ไม่เปิดเผยข้อมูลผู้ป่วยที่เราไม่ได้มีส่วนเกี่ยวข้องกับการรักษา
๕. ถ้าส่งข้อมูลผ่านทาง LINE ให้ส่งไปที่แพทย์ที่เกี่ยวข้องโดยตรง หลีกเลี่ยงการส่งในกลุ่มใหญ่
๖. การประชุมต้องลบชื่อของผู้ป่วยในเอกสารทุกชิ้น ทุกหน้า และถ้าไม่จำเป็นไม่ต้องใส่ hospital number
๗. ภาพถ่ายต้องไม่สามารถระบุตัวตนได้ ต้องไม่เห็นหน้า ไม่เห็นตำหนิสำคัญ รอยสัก หรือแผลเป็นที่มีลักษณะจำเพาะ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ไม่ใช่เรื่องใหม่ เพราะข้อมูลของผู้ป่วยเป็นข้อมูลที่ได้รับการคุ้มครองและต้องใช้อย่างระมัดระวังอยู่แล้ว กฎหมายนี้ไม่ได้ห้ามเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่เป็นการกำกับให้ทำด้วยความระมัดระวังและคุ้มครองเจ้าของข้อมูลมากขึ้น ดังนั้นในฐานะเจ้าหน้าที่ของโรงพยาบาลจึงควรมีความรู้และระมัดระวังเรื่องการใช้ข้อมูลแบบไม่เหมาะสม ปกป้องข้อมูลที่จะระบุตัวตนผู้อื่นเหมือนปกป้องข้อมูลส่วนตัวของเราเอง การปฏิบัติ

ตามสิทธิในข้อมูลด้านสุขภาพส่วนบุคคลเป็นการสร้างความเชื่อมั่นให้กับผู้ป่วยเกี่ยวกับการจัดการข้อมูลส่วนบุคคลและช่วยลดความเสี่ยงทางกฎหมายที่อาจเกิดขึ้น

กรณีศึกษาเรื่อง ตอบข้อหาหรือเกี่ยวกับการขอลบหรือทำลายข้อมูลส่วนบุคคล โดยโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ตามเอกสารแนบฉบับที่หนึ่ง และโดยคณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ตามเอกสารแนบฉบับที่สอง



งานกฎหมายเลขที่.....๔๖๐
รับครั้งที่ ๑.....15 กค. 2568 1544
รับครั้งที่ ๒.....เวลา.....
รับครั้งที่ ๓.....เวลา.....

ศูนย์อำนวยการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล

สำนักงานอธิการบดี มหาวิทยาลัยมหิดล

โทรศัพท์ ๐ ๒๘๔๔ ๖๔๔๐ โทรสาร ๐ ๒๘๔๔ ๖๔๔๑

ด่วนที่สุด

ที่ อว ๗๘.๐๑๔๕ / ๓๖

วันที่ ๕ กุมภาพันธ์ พ.ศ. ๒๕๖๘

เรื่อง ตอบข้อหาหรือเกี่ยวกับการขอลบหรือทำลายข้อมูลส่วนบุคคล

เรียน คณะบดีคณะแพทยศาสตร์ศิริราชพยาบาล

ตามที่คณะแพทยศาสตร์ศิริราชพยาบาล โดยโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ได้รับคำขอจากผู้รับบริการของโรงพยาบาล ซึ่งแจ้งความประสงค์ขอลบและทำลายข้อมูลส่วนบุคคลทั้งหมดของผู้รับบริการจากฐานข้อมูลของโรงพยาบาล โดยอ้างว่าเป็นสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และคณะแพทยศาสตร์ศิริราชพยาบาลขอหารือข้อกฎหมายในประเด็นดังกล่าวว่าสามารถยกข้อกฎหมายหรือฐานทางกฎหมายประการใดในการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้รับบริการในฐานะเจ้าของข้อมูลส่วนบุคคล เพื่อเป็นแนวทางให้กับคณะแพทยศาสตร์ศิริราชพยาบาลในการพิจารณาคำขอของผู้รับบริการดังกล่าวต่อไป ความละเอียดแจ้งแล้ว นั้น

ศูนย์อำนวยการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล ได้พิจารณาข้อหาหรือดังกล่าวของคณะแพทยศาสตร์ศิริราชพยาบาลแล้ว ปรากฏข้อเท็จจริงเพิ่มเติมตามลำดับเหตุการณ์ ดังนี้

๑. ผู้รับบริการมีประวัติการเข้ารับการรักษาที่โรงพยาบาลศิริราช ปิยมหาราชการุณย์ ครั้งแรกในวันที่ ๔ มกราคม ๒๕๖๑ โดยได้ลงนามในหนังสือแสดงเจตนารับบริการด้านสุขภาพ มีข้อความสำคัญตอนหนึ่งว่า “...ข้าพเจ้าอนุญาตให้โรงพยาบาลทำลายเอกสารประวัติการรักษาและฟิล์มเอ็กซเรย์ของข้าพเจ้าในกรณีที่ข้าพเจ้าไม่ได้มารับบริการหรือขาดการติดต่อกับโรงพยาบาลเป็นระยะเวลา ๑๐ ปี นับตั้งแต่การเข้ารับบริการครั้งสุดท้าย...”

๒. ต่อมา เมื่อวันที่ ๑๙ มิถุนายน ๒๕๖๗ ผู้รับบริการได้มีหนังสือขอเพิกถอนคำยินยอมในการให้โรงพยาบาลเก็บรวบรวมข้อมูลส่วนบุคคล และต้องการให้โรงพยาบาลลบและทำลายข้อมูลส่วนบุคคลทั้งหมด ซึ่งรวมถึงแต่ไม่จำกัดเพียงข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่อ่อนไหว และข้อมูลการรักษาพยาบาล เนื่องจากไม่ได้เข้าใช้บริการที่โรงพยาบาลมาเกิน ๕ ปีแล้ว และไม่ประสงค์ที่จะเข้าใช้บริการที่โรงพยาบาลอีกต่อไป และอ้างว่าทางโรงพยาบาลมีความจำเป็นทางกฎหมายในการเก็บและรวบรวมข้อมูลส่วนบุคคลของตนเพียง ๕ ปี นับจากวันที่จัดทำเท่านั้น โดยขอความกรุณาโรงพยาบาลช่วยดำเนินการโดยเร็วและแจ้งกลับ ทั้งนี้ ไม่เกิน ๓๐ วัน ตามที่กฎหมายกำหนด

๓. โรงพยาบาลศิริราช ปิยมหาราชการุณย์ ได้ปฏิเสธคำร้องขอให้ลบข้อมูลส่วนบุคคลตาม ๒. เมื่อวันที่ ๘ กรกฎาคม ๒๕๖๗ โดยให้เหตุผลว่า การจัดเก็บข้อมูลด้านสุขภาพ ดำเนินการด้วยวัตถุประสงค์เพื่อการวินิจฉัยโรคทางการแพทย์ การบริการด้านสุขภาพ การรักษาทางการแพทย์ การจัดการด้านสุขภาพ ตามมาตรา ๓๓ วรรคสอง ประกอบมาตรา ๒๖ (๕) (ก) ซึ่งเป็นฐานความจำเป็นเพื่อการปฏิบัติตามสัญญา ตามมาตรา ๒๔ (๓) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่โรงพยาบาลกำหนดข้อตกลงในการให้บริการไว้ ดังนั้น โรงพยาบาลจึงไม่สามารถดำเนินการลบข้อมูลส่วนบุคคลตามที่ร้องขอได้ อนึ่ง ข้อมูลการรักษาของผู้รับบริการ จัดเก็บในรูปแบบไฟล์อิเล็กทรอนิกส์ มีการจำกัดสิทธิการเข้าถึงของบุคลากร ขอให้มั่นใจว่า ข้อมูลของผู้รับบริการจะไม่มี การรั่วไหลออกไปภายนอก

๔. ผู้รับบริการมีหนังสือขอใช้สิทธิลบและทำลายข้อมูลส่วนบุคคล ครั้งที่ ๒ เมื่อวันที่ ๑๗ กรกฎาคม ๒๕๖๗ โดยชี้แจงว่า ตามมาตรา ๓๕ (๓) ของพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ กำหนดให้โรงพยาบาล จัดเก็บข้อมูลเพียง ๕ ปีเท่านั้น นับจากวันจัดทำ ซึ่งขณะนี้ได้เกินระยะเวลา ๕ ปีแล้วนับจากวันที่ตนไปใช้บริการที่ โรงพยาบาลครั้งล่าสุด ทางโรงพยาบาลจึงไม่มีความจำเป็นตามกฎหมายในการจัดเก็บข้อมูลส่วนบุคคลของตนอีกต่อไป นอกจากนี้ เนื่องจากตนไม่ประสงค์จะเข้าใช้บริการที่โรงพยาบาลอีก จึงขอยกเลิกสัญญาทั้งหมดระหว่างตนและ โรงพยาบาล รวมถึงผู้ประกอบวิชาชีพทางการแพทย์ของโรงพยาบาลนับจากวันที่ในหนังสือฉบับนี้ และตนในฐานะ เจ้าของข้อมูลส่วนบุคคล มีความประสงค์ที่จะเพิกถอนคำยินยอมในการให้โรงพยาบาลเก็บรวบรวมข้อมูลส่วนบุคคล ของตน และต้องการให้โรงพยาบาลลบและทำลายข้อมูลส่วนบุคคลของตนทั้งหมดซึ่งรวมถึงแต่ไม่จำกัดเพียงข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่อ่อนไหว และข้อมูลการรักษาพยาบาล ด้วยเหตุที่ตนต้องการใช้สิทธิตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และโรงพยาบาลไม่มีความจำเป็นตามกฎหมายและสัญญาใด ๆ ในการจัดเก็บ ข้อมูลดังกล่าวของตนอีกต่อไป โดยขอความกรุณาโรงพยาบาลช่วยดำเนินการโดยเร็วและแจ้งกลับ ทั้งนี้ ไม่เกิน ๓๐ วัน ตามที่กฎหมายกำหนด

๕. โรงพยาบาลศิริราช ปิยมหาราชการุณย์ ได้ปฏิเสธคำร้องขอให้ลบข้อมูลส่วนบุคคล ครั้งที่ ๒ ตาม ๔. เมื่อวันที่ ๑๓ สิงหาคม ๒๕๖๗ โดยชี้แจงว่า โรงพยาบาลได้นำคำร้องเข้าพิจารณาในคณะกรรมการที่เกี่ยวข้อง เป็นกรณีพิเศษ (อีกครั้ง) และที่ประชุมคณะกรรมการที่เกี่ยวข้องมีมติขอปฏิเสธคำร้องขอใช้สิทธิดังกล่าว เนื่องจาก โรงพยาบาลมีความจำเป็นต้องเก็บรวบรวมข้อมูลสุขภาพเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการวินิจฉัยโรค ทางทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ หรือการจัดการด้านสุขภาพ ตาม มาตรา ๒๖ (๕) (ก) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับเวชระเบียนผู้ป่วยเป็น หนังสือราชการที่มีความสำคัญต่อผู้ป่วยและโรงพยาบาลในด้านการวินิจฉัยโรคทางการแพทย์ การให้บริการด้าน สุขภาพหรือด้านสังคม การรักษาทางการแพทย์ หรือการจัดการด้านสุขภาพ หากมีการลบหรือทำลายข้อมูลไปแล้ว อาจมีข้อพิจารณาสำคัญในการใช้เป็นพยานหลักฐานตามกฎหมายอื่นที่เกี่ยวข้องกับการรับฟังพยานหลักฐานของศาล หรือหน่วยงานรัฐอื่น หรือกฎหมายอื่นที่เกี่ยวข้องกับสาธารณสุข นอกจากนี้ ตามข้อ ๔ ของระเบียบสำนัก นายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๖๖ และที่แก้ไขเพิ่มเติม กำหนดให้หนังสือราชการ คือ เอกสารที่เป็น หลักฐานในราชการ กรณีเวชระเบียนผู้ป่วยของโรงพยาบาลเป็นเอกสารที่ได้จัดทำขึ้น เพื่อรวบรวมประวัติและข้อมูล การเจ็บป่วยสำหรับใช้ประกอบการรักษาผู้ป่วย และใช้เป็นหลักฐานในราชการได้ จึงถือเป็นหนังสือราชการ และเมื่อ เวชระเบียนผู้ป่วยเป็นหนังสือราชการแล้วจะต้องถือปฏิบัติเกี่ยวกับการเก็บรักษาหนังสือให้สอดคล้องกับระเบียบฯ ที่กำหนด โดยปกติกำหนดให้เก็บไว้ไม่น้อยกว่า ๑๐ ปี ซึ่งทางโรงพยาบาลกำหนดให้เก็บรักษาเวชระเบียนในรูปแบบ

ที่เป็นกระดาษไว้ไม่น้อยกว่า ๕ ปี และในรูปแบบอิเล็กทรอนิกส์ไม่มีอายุการเก็บหนังสือ โดยปกติกำหนดให้เก็บไว้ตลอดไป ตามข้อ ๘๔/๕ ของระเบียบสำนักนายกรัฐมนตรีฯ สำหรับการทาลายหนังสือราชการที่เป็นกระดาษ (เวชระเบียน) โรงพยาบาลดำเนินการทาลายหนังสือตามแนวทางปฏิบัติของมหาวิทยาลัยมหิดล ซึ่งมีวิธีการและขั้นตอนปฏิบัติเช่นเดียวกับระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม ในหมวดที่ ๓ การเก็บรักษา ยืม และทาลายหนังสือ ที่กำหนดไว้ในส่วนที่ ๓ เรื่อง การทาลาย อย่างไรก็ตาม โรงพยาบาลมีนโยบายเวชระเบียน เรื่องการรักษาความลับ ความปลอดภัย และความเป็นส่วนตัวของผู้ป่วย โดยกำหนดไว้ว่า ข้อมูลเวชระเบียนถือเป็นความลับ บุคลากรทุกคนในโรงพยาบาลมีหน้าที่ต้องรักษาความลับของผู้ป่วย และข้อมูลเวชระเบียนผู้มีสิทธิตามกฎหมาย และผู้ที่โรงพยาบาลอนุญาตเท่านั้นที่สามารถเข้าถึง ใช้งาน และเปิดเผยข้อมูลเวชระเบียนในส่วนที่เกี่ยวข้อง และเพียงเท่าที่จำเป็นต้องใช้งานได้ โรงพยาบาลมีระเบียบ และขั้นตอนปฏิบัติในการขอเข้าถึง บันทึกแก้ไข เปลี่ยนแปลง และเปิดเผยข้อมูล ความพยายามเข้าถึงข้อมูลโดยไม่มีสิทธิ หรือไม่ได้รับอนุญาตจากโรงพยาบาล รวมถึงความช่วยเหลือต่าง ๆ ให้เข้าถึง ใช้งาน และเปิดเผยข้อมูลเวชระเบียน ไม่ว่าจะกระทำสำเร็จหรือไม่ก็ตามถือเป็นความผิด และต้องถูกดำเนินการทั้งทางวินัย และกฎหมาย

๖. ผู้รับบริการมีหนังสือขอใช้สิทธิลบและทาลายข้อมูลส่วนบุคคล ครั้งที่ ๓ เมื่อวันที่ ๒๔ พฤศจิกายน ๒๕๖๗ โดยชี้แจงว่า ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ ข้อ ๔ วรรคหนึ่ง ได้กำหนดให้ระเบียบนี้ใช้บังคับแก่ส่วนราชการ และข้อ ๖ ได้กำหนดบทนิยามคำว่า “ส่วนราชการ” ไว้ว่า กระทรวง ทบวง กรม สำนักงาน หรือหน่วยงานอื่นใดของรัฐ ทั้งในราชการบริหารส่วนกลาง ราชการบริหารส่วนภูมิภาค ราชการบริหารส่วนท้องถิ่น หรือในต่างประเทศ ซึ่งข้อกำหนดในระเบียบดังกล่าวมีเจตนารมณ์มุ่งหมายให้หมายความถึงส่วนราชการและหน่วยงานในสังกัดส่วนราชการที่อยู่ในฝ่ายบริหารตามที่บัญญัติไว้ในพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม และเนื่องจากพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ มาตรา ๕ วรรคสอง ได้บัญญัติให้มหาวิทยาลัยมหิดลมีฐานะเป็นหน่วยงานในกำกับของรัฐ ซึ่งไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน กฎหมายว่าด้วยระเบียบบริหารราชการกระทรวงศึกษาธิการ และกฎหมายว่าด้วยการปรับปรุงกระทรวง ทบวง กรม และไม่เป็นรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณและกฎหมายอื่น ดังนั้น คณะแพทยศาสตร์ศิริราชพยาบาล (โรงพยาบาลศิริราช ปิยมหาราชการุณย์) จึงไม่ได้เป็นส่วนราชการตามนัยบทนิยามคำว่า “ส่วนราชการ” ที่กำหนดไว้ในข้อ ๖ ของระเบียบฯ และไม่ได้อยู่ในบังคับของระเบียบฯ อย่างไรก็ตาม หากข้อปฏิเสธของโรงพยาบาลฯ อยู่บนพื้นฐานของข้อเท็จจริงที่ว่า คณะแพทยศาสตร์ศิริราชพยาบาล (โรงพยาบาลศิริราช ปิยมหาราชการุณย์) เป็นส่วนราชการที่อยู่ในบังคับของระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม แต่ข้อ ๔ ของระเบียบดังกล่าวกำหนดให้หนังสือราชการ คือ เอกสารที่เป็นหลักฐานในราชการ กรณีเวชระเบียนผู้ป่วย เป็นเอกสารที่ได้จัดทำขึ้นเพื่อรวบรวมประวัติและข้อมูลการเจ็บป่วยสำหรับใช้ประกอบการรักษาผู้ป่วย และใช้เป็นหลักฐานในราชการได้ จึงถือเป็นหนังสือราชการตามนัยระเบียบฯ ข้อ ๔ และเมื่อเวชระเบียนผู้ป่วยเป็นหนังสือราชการแล้ว หน่วยงานดังกล่าวสมควรจะต้องถือปฏิบัติเกี่ยวกับการรักษาหนังสือให้สอดคล้องกับระเบียบฯ ที่กำหนดด้วย และโดยระเบียบฯ ข้อ ๕๗ วรรคหนึ่ง ได้กำหนดให้อายุการเก็บหนังสือ โดยปกติให้เก็บไม่น้อยกว่า ๑๐ ปี เว้นแต่เป็นหนังสือตามที่ระบุไว้ในข้อ ๕๗.๑ ถึง ๕๗.๖ และระเบียบข้อ ๕๗.๖ ได้กำหนดให้กรณีที่เป็นหนังสืออื่นใด หากได้มีกฎหมายหรือระเบียบแบบแผนกำหนดไว้เป็นพิเศษแล้ว การเก็บให้เป็นไปตามกฎหมายและระเบียบแบบแผนนั้น ดังนั้น เวชระเบียนผู้ป่วย จึงอยู่ในข่ายที่เป็นหนังสืออื่นใด หากได้มีกฎหมายหรือระเบียบแบบแผนกำหนดไว้เป็นพิเศษแล้ว การเก็บให้เป็นไปตาม

กฎหมายและระเบียบแบบแผนนั้นตามระเบียบข้อ ๕๗.๒ ซึ่งเรื่องนี้สำนักนายกรัฐมนตรีได้เคยวางหลักการเกี่ยวกับอายุ การเก็บรักษาประวัติผู้ป่วย (หรือเวชระเบียนผู้ป่วย) ไว้ด้วยแล้วว่า ให้เก็บรักษาไว้ไม่น้อยกว่า ๕ ปี ตามหนังสือสำนัก นายกรัฐมนตรี ที่ นร ๑๐๐๒/ว ๘ ลงวันที่ ๓๑ มีนาคม ๒๕๓๐ ดังนั้น ไม่ว่าประวัติเวชระเบียนของผู้รับบริการจะเข้า ขายเป็นหนังสือราชการหรือไม่ ทางโรงพยาบาลฯ ไม่มีความจำเป็นทางกฎหมายและสัญญาใด ๆ ในการจัดเก็บข้อมูล ดังกล่าวของตนอีกต่อไป ตนในฐานะเจ้าของข้อมูลส่วนบุคคลมีความประสงค์ที่จะเพิกถอนคำยินยอมในการให้ โรงพยาบาลฯ เก็บรวบรวมข้อมูลส่วนบุคคลของตน และต้องการให้โรงพยาบาลฯ ลบและทำลายข้อมูลส่วนบุคคลของตนทั้งหมดซึ่งรวมถึงแต่ไม่จำกัดเพียงข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่อ่อนไหว และข้อมูลการรักษาพยาบาล ด้วย เหตุที่ตนต้องการใช้สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงขอความกรุณาโรงพยาบาลฯ ช่วยดำเนินการโดยเร็วและแจ้งกลับ ทั้งนี้ ไม่เกิน ๓๐ วัน ตามที่กฎหมายกำหนด โดยได้แนบคำวินิจฉัยของสำนัก นายกรัฐมนตรีเกี่ยวกับการเก็บรักษาเวชระเบียนผู้ป่วยของคณะแพทยศาสตร์โรงพยาบาลรามาธิบดี ตามหนังสือสำนัก นายกรัฐมนตรี ที่ นร ๐๑๐๖/๗๔ ลงวันที่ ๑๒ มกราคม ๒๕๕๘ เรื่อง การขอลดอายุการเก็บรักษาเวชระเบียนผู้ป่วย ของคณะแพทยศาสตร์โรงพยาบาลรามาธิบดี ไว้ด้วยเพื่อประโยชน์แห่งการพิจารณา

เมื่อได้พิจารณาข้อหาหรือประกอบข้อเท็จจริงเพิ่มเติมดังกล่าวแล้ว ศูนย์อำนวยการด้านข้อมูล ส่วนบุคคล มหาวิทยาลัยมหิดล เห็นว่า มีประเด็นที่ต้องพิจารณา ๑ ประเด็น คือ เมื่อเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้รับบริการสุขภาพขอใช้สิทธิขอให้มหาวิทยาลัยมหิดล โดยคณะแพทยศาสตร์ศิริราชพยาบาล (โรงพยาบาลศิริราช ปิยมหาราชการุณย์) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลของตน รายละเอียด ตามข้อเท็จจริงประกอบข้อหาหรือนี้ โรงพยาบาลฯ มีหน้าที่ต้องดำเนินการตามคำขอใช้สิทธิดังกล่าวหรือไม่ อย่างไร

มาตรา ๓๓ วรรคหนึ่งและวรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ บัญญัติว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูล ส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(๓) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม มาตรา ๓๒ (๑) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา ๓๒ (๑) (ก) หรือ (ข) ได้ หรือเป็นการ คัดค้านตามมาตรา ๓๒ (๒)

(๔) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการ แสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข)

การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย”

นอกจากนี้ ข้อ ๓ วรรคหนึ่ง ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗ ซึ่งออกตามความในมาตรา ๓๓ วรรคห้า แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดว่า เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามมาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และไม่ใช้กรณีที่ได้รับยกเว้นการใช้บังคับตามมาตรา ๓๓ วรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเก้าสิบวันนับแต่วันที่รับคำขอ ดังนั้น เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา ๓๓ ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องพิจารณาก่อนว่า กรณีดังกล่าวเป็นกรณีที่ใช้ข้อยกเว้นตามมาตรา ๓๓ วรรคหนึ่ง (๑) ถึง (๔) หรือไม่ และเป็นกรณีที่ได้รับยกเว้นการใช้สิทธิตามมาตรา ๓๓ วรรคสองหรือไม่ หากเป็นกรณีที่ใช้ข้อยกเว้นตามมาตรา ๓๓ วรรคหนึ่ง (๑) ถึง (๔) และไม่ใช้กรณีที่ได้รับยกเว้นการใช้สิทธิตามมาตรา ๓๓ วรรคสอง จึงจะต้องดำเนินการตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอโดยไม่ชักช้า แต่ต้องไม่เกิน ๔๐ วันนับแต่วันที่รับคำขอ

สำหรับข้อมูลส่วนบุคคลตามประเด็นข้อหานี้ เป็นข้อมูลส่วนบุคคลของผู้รับบริการสุขภาพของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ คณะแพทยศาสตร์ศิริราชพยาบาล ที่มีการเก็บรวบรวมในเอกสารเวชระเบียนในรูปแบบกระดาษ และข้อมูลอิเล็กทรอนิกส์ในระบบสารสนเทศของโรงพยาบาลฯ ซึ่งย่อมปรากฏทั้งข้อมูลส่วนบุคคลโดยทั่วไป และข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล การพิจารณาว่าโรงพยาบาลฯ จะต้องดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ หรือไม่ อย่างไร นั้น จะต้องพิจารณาก่อนว่า คำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามมาตรา ๓๓ วรรคหนึ่ง (๑) ถึง (๔) ข้อใดข้อหนึ่งหรือไม่ ตลอดจนได้รับยกเว้นการนำความในมาตรา ๓๓ วรรคหนึ่งมาใช้บังคับ ตามมาตรา ๓๓ วรรคสอง หรือไม่

ในประเด็นนี้ ศูนย์อำนวยการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล พิจารณาจากข้อเท็จจริงเกี่ยวกับวัตถุประสงค์และลักษณะการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ แล้ว เห็นว่า โรงพยาบาลศิริราช ปิยมหาราชการุณย์ มีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยดังนี้

๑. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้รับบริการ มีวัตถุประสงค์หลักเพื่อการให้บริการสุขภาพแก่ผู้รับบริการซึ่งตัดสินใจเข้ารับบริการกับทางโรงพยาบาล จึงถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น ตามมาตรา ๒๔ (๓) แห่งพระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และสำหรับข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพ ถือเป็นกรณการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพ การรักษาทางการแพทย์ และการจัดการด้านสุขภาพ ไม่ว่าจะเป็นกรณีที่เป็นกรณการจำเป็นในการปฏิบัติตามกฎหมาย หรือเป็นการปฏิบัติตามสัญญา ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ ซึ่งข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ตามมาตรา ๒๖ (๕) (ก) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เว้นแต่ในกรณีจำเป็นที่ต้องเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งจะเป็นไปตามมาตรา ๒๔ (๒) หรือมาตรา ๒๖ (๑) แล้วแต่กรณี แทน โดยแม้ว่าผู้รับบริการจะแสดงเจตนาว่าไม่ประสงค์จะเข้ารับบริการสุขภาพกับทางโรงพยาบาลอีก แต่โรงพยาบาลยังอาจมีความจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวไว้เพื่อการให้บริการสุขภาพตามมาตรฐานของโรงพยาบาลและมาตรฐานวิชาชีพของบุคลากรที่เกี่ยวข้อง ในกรณีที่ผู้รับบริการตัดสินใจกลับเข้ามาใช้บริการสุขภาพในอนาคตหรือในกรณีฉุกเฉิน เพื่อป้องกันปัญหาข้อผิดพลาดในการตรวจวินิจฉัยหรือรักษาพยาบาลผู้ป่วยที่อาจเกิดขึ้นจากการไม่มีประวัติสุขภาพของผู้ป่วยที่ถูกต้องครบถ้วนสมบูรณ์ และอาจทำให้โรงพยาบาลให้บริการโดยไม่เป็นไปตามมาตรฐาน หรือมีความรับผิดทางกฎหมายได้ โรงพยาบาลจึงสามารถพิจารณาเก็บรักษาข้อมูลส่วนบุคคลของผู้รับบริการไว้เพื่อวัตถุประสงค์เกี่ยวกับการวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพ การรักษาทางการแพทย์ และการจัดการด้านสุขภาพได้ตามระยะเวลาที่โรงพยาบาลเห็นว่ามีความจำเป็นเพื่อการให้บริการตามมาตรฐานการให้บริการของตน

๒. การเก็บรักษาข้อมูลส่วนบุคคลเกี่ยวกับการรับบริการของผู้รับบริการของโรงพยาบาลไว้เพื่อเป็นหลักฐานอ้างอิงทางกฎหมายในกรณีที่มีการดำเนินคดีต่อสถานพยาบาลหรือบุคลากรที่เกี่ยวข้อง ไม่ว่าจะเป็นคดีอาญา คดีแพ่ง คดีปกครอง หรือการดำเนินการด้านจริยธรรมหรือจรรยาบรรณของผู้ประกอบวิชาชีพหรือผู้ประกอบโรคศิลปะ ในระหว่างที่ยังอยู่ในอายุความของคดีที่อาจถูกฟ้องร้องดำเนินคดีหรือถูกกล่าวหาได้ ซึ่งถือเป็นกรณีที่เป็นกรณการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งประโยชน์ดังกล่าวมีความสำคัญไม่น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๒๔ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และสำหรับข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพ ถือเป็นกรณีที่เป็นกรณการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมายตามมาตรา ๒๖ (๕)

ดังนั้น การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ จึงไม่ใช่กรณกรณีที่ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๓๓ วรรคหนึ่ง (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ แต่อย่างใด นอกจากนี้ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ เมื่อเจ้าของข้อมูลส่วนบุคคลมาใช้บริการสุขภาพที่โรงพยาบาล ไม่ใช่กรณที่อาศัยฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๔ หรือมาตรา ๒๖ จึงไม่ใช่กรณที่เจ้าของข้อมูลส่วนบุคคลจะสามารถถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

บุคคลได้ ตามมาตรา ๓๓ วรรคหนึ่ง (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้ตั้งแต่ต้น ประกอบกับกรณีดังกล่าว แม้จะมีการเก็บรวบรวมข้อมูลส่วนบุคคลโดยได้รับยกเว้นไม่ต้องขอความยินยอม ซึ่งวัตถุประสงค์หนึ่ง คือ เพื่อเป็นหลักฐานอ้างอิงทางกฎหมายในกรณีที่มีการดำเนินคดีต่อสถานพยาบาลหรือบุคลากรที่เกี่ยวข้อง ตามมาตรา ๒๔ (๔) (เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล) แต่ก็เกินไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย จึงไม่เข้าเงื่อนไขที่เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๓๒ (๑) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา ๓๒ (๑) (ก) หรือ (ข) ได้ แต่อย่างใด และไม่เข้าการคัดค้านตามมาตรา ๓๒ (๒) (เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง) กรณีจึงไม่เข้าเงื่อนไขของการใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ วรรคหนึ่ง (๓) ทั้งยังไม่ใช่ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย ตามมาตรา ๓๓ วรรคหนึ่ง (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ด้วยเหตุนี้ เจ้าของข้อมูลส่วนบุคคลจึงไม่สามารถขอใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ วรรคหนึ่ง (๑) (๒) (๓) และ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับเมื่อพิจารณาจากวัตถุประสงค์ในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวไว้ของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ซึ่งเป็นการเก็บรักษาไว้เพื่อการให้บริการสุขภาพตามมาตรฐานของโรงพยาบาลและมาตรฐานวิชาชีพของบุคลากรที่เกี่ยวข้อง ในกรณีที่ผู้รับบริการตัดสินใจกลับเข้ามาใช้บริการสุขภาพในอนาคตหรือในกรณีฉุกเฉิน ซึ่งเป็นวัตถุประสงค์ตามมาตรา ๒๖ (๕) (ก) รวมทั้งเป็นการเก็บรักษาไว้เพื่อเป็นหลักฐานอ้างอิงทางกฎหมาย ซึ่งถือเป็นการใช้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย จึงได้รับยกเว้นการใช้บังคับการขอใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ วรรคหนึ่ง ตามนัยมาตรา ๓๓ วรรคสองอีกด้วย

โรงพยาบาลศิริราช ปิยมหาราชการุณย์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล จึงสามารถปฏิเสธการขอใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ของเจ้าของข้อมูลส่วนบุคคลรายดังกล่าวได้ โดยเป็นกรณีที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเทียบเคียงได้กับการตอบข้อหารือตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ของคณะกรรมการตอบข้อหารือและให้คำแนะนำในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง “คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ขอหารือการขอลบประวัติการรักษาในโรงพยาบาล” ที่เผยแพร่ในเว็บไซต์ของสำนักงานคณะกรรมการคุ้มครองข้อมูล

ส่วนบุคคล (<https://www.pdpc.or.th/wp-content/uploads/2024/11/PDPC-consultation-47.pdf>) และแนบมาพร้อมหนังสือฉบับนี้

อนึ่ง ศูนย์อำนวยการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล มีข้อสังเกตเพิ่มเติมว่า แม้บทบัญญัติมาตรา ๓๕ (๓) แห่งพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ จะกำหนดหน้าที่และความรับผิดชอบของผู้รับอนุญาตและผู้ดำเนินการของสถานพยาบาลในการจัดให้มีและรายงานหลักฐานเกี่ยวกับผู้ประกอบวิชาชีพในสถานพยาบาลและผู้ป่วย และเอกสารอื่นที่เกี่ยวข้องกับการรักษาพยาบาล โดยต้องเก็บรักษาไว้ให้อยู่ในสภาพที่ตรวจสอบได้ไม่น้อยกว่า ๕ ปีนับแต่วันจัดทำ ประกอบกับโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ในฐานะสถานพยาบาลซึ่งดำเนินการโดยสถาบันการศึกษาของรัฐ ต้องมีลักษณะของสถานพยาบาลและมาตรฐานตามมาตรา ๕ ววรรคหนึ่งและวรรคสอง แห่งพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติสถานพยาบาล (ฉบับที่ ๔) พ.ศ. ๒๕๕๔ ประกอบข้อ ๖ (๓) ของประกาศกระทรวงสาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับตามกฎหมายว่าด้วยสถานพยาบาล ลงวันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๑ ซึ่งแก้ไขเพิ่มเติมโดยประกาศกระทรวงสาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับตามกฎหมายว่าด้วยสถานพยาบาล (ฉบับที่ ๒) ลงวันที่ ๒๘ มิถุนายน พ.ศ. ๒๕๖๒ โดยต้องจัดให้มีระบบการจัดการเวชระเบียนที่เป็นมาตรฐาน จัดให้มีระบบข้อมูลสำรองเพื่อป้องกันข้อมูลสูญหาย และมีพื้นที่เพียงพอที่จะเก็บเวชระเบียนได้อย่างน้อย ๕ ปี ตามข้อ ๓ ของประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง รายละเอียดเกี่ยวกับมาตรฐานระบบบริการสุขภาพของสถานพยาบาลประเภทที่รับผู้ป่วยไว้ค้างคืน ลงวันที่ ๘ มกราคม พ.ศ. ๒๕๖๔ ประกอบข้อ ๓ ของประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง หน่วยงานที่รับรองคุณภาพสถานพยาบาลซึ่งดำเนินการโดยกระทรวง ทบวง กรม องค์การปกครองส่วนท้องถิ่น รัฐวิสาหกิจ สถาบันการศึกษาของรัฐ หน่วยงานอื่นของรัฐ สภาวิชาชีพ พ.ศ. ๒๕๖๗ แต่บทบัญญัติดังกล่าวต่างกำหนดให้สถานพยาบาลเก็บรักษาเอกสารหรือข้อมูลดังกล่าวไว้เป็นระยะเวลาขั้นต่ำอย่างน้อย ๕ ปี และไม่มีบทบัญญัติแห่งกฎหมายใดกำหนดห้ามมิให้เก็บรักษาเอกสารหรือข้อมูลดังกล่าวไว้เกิน ๕ ปีตามที่เจ้าของข้อมูลส่วนบุคคลชี้แจงในหนังสือแต่อย่างใด โรงพยาบาลศิริราช ปิยมหาราชการุณย์ จึงย่อมสามารถเก็บรักษาเอกสารหรือข้อมูลดังกล่าวไว้เกิน ๕ ปีได้ โดยไม่ขัดกับกฎหมายว่าด้วยสถานพยาบาล

สำหรับประเด็นเรื่องหนังสือราชการ แม้โรงพยาบาลศิริราช ปิยมหาราชการุณย์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล จะไม่ใช่ส่วนราชการตามบทนิยามในระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม จึงไม่อยู่ในบังคับของระเบียบดังกล่าว ทำให้เวชระเบียนผู้ป่วยและเอกสารที่เกี่ยวข้องกับการให้บริการสุขภาพของโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ไม่ใช่หนังสือราชการตามระเบียบนี้ แต่โรงพยาบาลศิริราช ปิยมหาราชการุณย์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ก็อาจนำระเบียบดังกล่าวมาเทียบเคียงและปรับใช้ได้โดยอนุโลมตามความเหมาะสม เนื่องจากมหาวิทยาลัยมหิดลไม่ได้ออกข้อบังคับประกาศ หรือระเบียบเกี่ยวกับการเก็บรักษาหนังสือและเอกสารของมหาวิทยาลัยไว้เป็นอย่างอื่น และไม่ว่ากรณีใด ๆ การที่ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม ไม่นำมาใช้บังคับกับโรงพยาบาลศิริราช ปิยมหาราชการุณย์ ในเรื่องใด ก็ไม่ได้ทำให้โรงพยาบาลศิริราช ปิยมหาราชการุณย์ เสียสิทธิหรือหมิ่นหน้าที่ในการเก็บรักษาหนังสือและเอกสารไว้เพื่อประโยชน์ในการดำเนินงานของตนแต่อย่างใด

อย่างไรก็ตาม แม้โรงพยาบาลศิริราช ปิยมหาราชการุณย์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล จะไม่ต้องดำเนินการตามคำขอใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ในกรณีดังกล่าว แต่โรงพยาบาลและคณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล มีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ตามมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมีหน้าที่อื่นในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลด้วย

ทั้งนี้ ในกรณีที่สถานพยาบาลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือแก้ไขข้อมูลส่วนบุคคล ซึ่งไม่ใช่กรณีที่เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่น และเป็นกรณีที่เกี่ยวข้องกับประกันชีวิตหรือประกันวินาศภัย อันทำให้มีการเรียกร้องผลประโยชน์ตามกรมธรรม์ประกันภัยโดยทุจริตหรือแสดงหลักฐานอันเป็นเท็จในการเรียกร้อง ผู้เกี่ยวข้องของสถานพยาบาลอาจมีความผิดอาญาฐานกระทำความด้วยประการใด ๆ อันเป็นการช่วยเหลือหรือให้ความสะดวกในการที่ผู้อื่นกระทำการเรียกร้องผลประโยชน์ตามกรมธรรม์ประกันภัยโดยทุจริตหรือแสดงหลักฐานอันเป็นเท็จในการเรียกร้อง ตามมาตรา ๑๑๔/๔ วรรคสอง แห่งพระราชบัญญัติประกันชีวิต พ.ศ. ๒๕๓๕ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติประกันชีวิต (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ หรือมาตรา ๑๐๘/๔ วรรคสอง แห่งพระราชบัญญัติประกันวินาศภัย พ.ศ. ๒๕๓๕ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติประกันวินาศภัย (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ หรือบทบัญญัติแห่งกฎหมายอื่นที่เกี่ยวข้อง แล้วแต่กรณี ด้วย อย่างไรก็ตาม ในกรณีที่บริษัทประกันภัยหรือหน่วยงานใดขอให้สถานพยาบาลเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพของผู้รับบริการ สถานพยาบาลจะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน (ไม่ว่าจะเป็นความยินยอมที่ทำกับสถานพยาบาลหรือบริษัทประกันภัยก็ตาม) แต่เนื้อหาของความยินยอมครอบคลุมถึงการเปิดเผยข้อมูลส่วนบุคคลของสถานพยาบาลให้กับบริษัทประกันภัย) เว้นแต่จะเป็นกรณีที่ได้รับยกเว้นตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เช่น เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเรื่องใดตามที่กำหนดในมาตรา ๒๖ (๕) (ก) (ข) (ค) (ง) หรือ (จ) แล้วแต่กรณี เท่านั้น

การตอบข้อหาหรือและให้ความเห็นของศูนย์อำนาจการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล เป็นเพียงการให้ความเห็นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและข้อกฎหมายที่เกี่ยวข้อง เพื่อประโยชน์ในการดำเนินงานของมหาวิทยาลัยมหิดลและส่วนงาน เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิร้องเรียนตามมาตรา ๗๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งการพิจารณาความรับผิดชอบเป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ ตลอดจนการพิจารณาพิพากษาคดีของศาล ทั้งนี้ ในกรณีที่ส่วนงานหรือหน่วยงานที่เกี่ยวข้องมีข้อจำกัดในการปฏิบัติตามความเห็นในการตอบข้อหาหรือนี้ หรือมีคำถามหรือปัญหาอุปสรรคประการใดสามารถขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (data protection officer: DPO) ของมหาวิทยาลัยมหิดล ผ่านศูนย์อำนาจการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดลได้

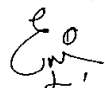
ความเห็นนี้ได้ผ่านการพิจารณาให้ความเห็นและตรวจสอบโดยผู้ช่วยศาสตราจารย์ ดร.พรชัย
 ชันยากร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ของมหาวิทยาลัยมหิดล และอาจารย์
 ดร. นายแพทย์นวนรรน ธีระอัมพรพันธุ์ ที่ปรึกษาศูนย์อำนวยการด้านข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล ด้วยแล้ว

จึงเรียนมาเพื่อโปรดทราบ

(รองศาสตราจารย์ นายแพทย์เชิดชัย นพมณีจารัสเลิศ)
 รักษาการแทนผู้อำนวยการศูนย์อำนวยการด้านข้อมูลส่วนบุคคล
 มหาวิทยาลัยมหิดล และรองอธิการบดีฝ่ายสารสนเทศ
 และดิจิทัลทรานส์ฟอร์มเมชัน มหาวิทยาลัยมหิดล

รับ บุคลากรงานกฎหมาย

- ☒ เพื่อทราบ
☐ เพื่อพิจารณา
☐ เพื่อดำเนินการ


 นางสาวยุติ แทบุงง
 หัวหน้างานกฎหมาย
 15 ก.ค. 2568

เรื่อง คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ขอรื้อการขอลบประวัติการรักษา ในโรงพยาบาล

ข้อกฎหมาย

๑. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
มาตรา ๖ มาตรา ๒๔ (๒) (๓) (๕) และ (๖) มาตรา ๒๖ (๑) (๔) และ (๕) (ก) และ (ข) มาตรา ๓๐
มาตรา ๓๑ มาตรา ๓๒ มาตรา ๓๓ มาตรา ๓๔ มาตรา ๓๖ มาตรา ๓๗ (๓) และมาตรา ๗๓
๒. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้
ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗
ข้อ ๓ วรรคหนึ่ง และข้อ ๘ วรรคสาม
๓. พระราชบัญญัติมหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๕๙
มาตรา ๕
๔. พระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ และที่แก้ไขเพิ่มเติม
มาตรา ๕ วรรคหนึ่งและวรรคสอง และมาตรา ๓๕ (๓)
๕. ประกาศกระทรวงสาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับ
การยกเว้นไม่ต้องอยู่ในบังคับตามกฎหมายว่าด้วยสถานพยาบาล ลงวันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๑
และที่แก้ไขเพิ่มเติม
ข้อ ๖ (๓)
๖. ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง รายละเอียดเกี่ยวกับมาตรฐานระบบบริการสุขภาพของ
สถานพยาบาลประเภทที่รับผู้ป่วยไว้ค้างคืน ลงวันที่ ๘ มกราคม พ.ศ. ๒๕๖๔
ข้อ ๓
๗. ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง หน่วยงานที่รับรองคุณภาพสถานพยาบาลซึ่งดำเนินการ
โดยกระทรวง ทบวง กรม องค์กรปกครองส่วนท้องถิ่น รัฐวิสาหกิจ สถาบันการศึกษาของรัฐ
หน่วยงานอื่นของรัฐ สภาวิชาชีพ พ.ศ. ๒๕๖๗
ข้อ ๓

ข้อหารือ

โรงพยาบาลสงขลานครินทร์ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ แจ้งว่า ได้รับคำขอ
จากผู้รับบริการของโรงพยาบาลสงขลานครินทร์ แจ้งความประสงค์ขอลบประวัติการรักษาของผู้ร้องจากฐานข้อมูล
โรงพยาบาลสงขลานครินทร์ โดยอ้างว่าเป็นสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงขอ
หารือข้อกฎหมายในประเด็นดังกล่าวว่า โรงพยาบาลสงขลานครินทร์ จะอ้างการเก็บรวบรวมข้อมูลส่วนบุคคลของ
เจ้าของข้อมูลส่วนบุคคลที่มีต่อโรงพยาบาลอันเป็นระบบการประกันสุขภาพ ซึ่งเป็นสวัสดิการพื้นฐานของรัฐ
หากเกิดกรณีมีผู้ร้องขอใช้สิทธิลบประวัติการรักษา ทางโรงพยาบาลฯ จะสามารถอ้างข้อกฎหมายหรือฐานทางกฎหมาย

ประการใด ทั้งนี้ เพื่อเป็นแนวทางให้กับโรงพยาบาลสงขลานครินทร์ และโรงพยาบาลอื่น ๆ ที่อาจได้รับ คำขอ ดังกล่าว

ความเห็น

คณะกรรมการการตอบข้อหารือและให้คำแนะนำในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้พิจารณาเรื่องหารือดังกล่าว โดยมีผู้แทน โรงพยาบาลสงขลานครินทร์ชี้แจงข้อเท็จจริงประกอบการพิจารณาแล้ว มีความเห็นว่า โรงพยาบาลสงขลานครินทร์ เป็นหน่วยงานภายใต้สังกัดคณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ โดยมหาวิทยาลัยสงขลานครินทร์ มีฐานะเป็นนิติบุคคลตามมาตรา ๕ แห่งพระราชบัญญัติมหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๕๔ จึงถือได้ว่า มหาวิทยาลัยสงขลานครินทร์เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ การที่โรงพยาบาลสงขลานครินทร์ทำการเก็บรวบรวมข้อมูลประวัติการรักษาของผู้รับบริการ มีวัตถุประสงค์หลักเพื่อให้บริการสุขภาพแก่ผู้รับบริการซึ่งตัดสินใจเข้ารับบริการกับทาง โรงพยาบาล จึงอาจถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น ตามมาตรา ๒๔ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และสำหรับข้อมูลส่วนบุคคล ตามมาตรา ๒๖ (เช่น ข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพ) ถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นการจำเป็น ในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมิน ความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ หรือในกรณี ที่ไม่ใช้การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือ ผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ก็อาจถือเป็นการปฏิบัติตามสัญญาระหว่าง เจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ ตามมาตรา ๒๖ (๕) (ก) แห่งพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เว้นแต่ในกรณีจำเป็นที่ต้องเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อป้องกันหรือระงับ อันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งจะเป็นไปตามมาตรา ๒๔ (๒) หรือมาตรา ๒๖ (๑) แล้วแต่กรณี

นอกจากนี้ พระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ มาตรา ๓๕ (๓) กำหนดหน้าที่ และความรับผิดชอบของผู้รับอนุญาตและผู้ดำเนินการของสถานพยาบาลในการจัดให้มีและรายงานหลักฐาน เกี่ยวกับผู้ประกอบวิชาชีพในสถานพยาบาลและผู้ป่วย และเอกสารอื่นที่เกี่ยวกับการรักษาพยาบาล โดยต้อง เก็บรักษาไว้ให้อยู่ในสภาพที่ตรวจสอบได้ไม่น้อยกว่า ๕ ปีนับแต่วันจัดทำ และโรงพยาบาลสงขลานครินทร์ ในฐานะสถานพยาบาลซึ่งดำเนินการโดยสถาบันการศึกษาของรัฐ ต้องมีลักษณะของสถานพยาบาล และมาตรฐานตามมาตรา ๕ วรรคหนึ่งและวรรคสอง แห่งพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ ซึ่งแก้ไข เพิ่มเติมโดยพระราชบัญญัติสถานพยาบาล (ฉบับที่ ๔) พ.ศ. ๒๕๕๔ ประกอบข้อ ๖ (๓) ของประกาศกระทรวง สาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับ ตามกฎหมายว่าด้วยสถานพยาบาล ลงวันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๑ ซึ่งแก้ไขเพิ่มเติมโดยประกาศกระทรวง

สาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับตามกฎหมายว่าด้วยสถานพยาบาล (ฉบับที่ ๒) ลงวันที่ ๒๘ มิถุนายน พ.ศ. ๒๕๖๒ โดยต้องจัดให้มีระบบการจัดการเวชระเบียนที่เป็นมาตรฐาน จัดให้มีระบบข้อมูลสำรองเพื่อป้องกันข้อมูลสูญหาย และมีพื้นที่เพียงพอที่จะเก็บเวชระเบียนได้อย่างน้อย ๕ ปี ตามข้อ ๓ ของประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง รายละเอียดเกี่ยวกับมาตรฐานระบบบริการสุขภาพของสถานพยาบาลประเภทที่รับผู้ป่วยไว้ค้างคืน ลงวันที่ ๘ มกราคม พ.ศ. ๒๕๖๔ ประกอบข้อ ๓ ของประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง หน่วยงานที่รับรองคุณภาพสถานพยาบาลซึ่งดำเนินการโดยกระทรวง ทบวง กรม องค์กรปกครองส่วนท้องถิ่น รัฐวิสาหกิจ สถาบันการศึกษาของรัฐ หน่วยงานอื่นของรัฐ สภากาชาดไทย พ.ศ. ๒๕๖๗ การที่โรงพยาบาลสงขลานครินทร์เก็บรวบรวมข้อมูลประวัติการรักษาของผู้รับบริการตามข้อกำหนดดังกล่าว จึงถือเป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๒๔ (๖) หรือเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุขตามมาตรา ๒๖ (๕) (ข) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ แล้วแต่กรณี อีกด้วย

วัตถุประสงค์อีกประการหนึ่งที่สถานพยาบาลต่าง ๆ เก็บรวบรวมข้อมูลประวัติการรักษาของผู้รับบริการ คือ เพื่อเป็นหลักฐานอ้างอิงทางกฎหมายในกรณีที่มีการดำเนินคดีต่อสถานพยาบาลหรือบุคลากรที่เกี่ยวข้อง ไม่ว่าจะเป็นคดีอาญา คดีแพ่ง คดีปกครอง หรือการดำเนินการด้านจริยธรรมหรือจรรยาบรรณของผู้ประกอบวิชาชีพหรือผู้ประกอบโรคศิลปะ ซึ่งอาจถือเป็นกรณีที่เป็นกรณีสืบเนื่องเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งประโยชน์ดังกล่าวมีความสำคัญไม่น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๒๔ (๕) หรือเป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมายตามมาตรา ๒๖ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อีกด้วย

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิของตนเองตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๐ ถึง ๓๔ และมาตรา ๓๖ นั้น ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องพิจารณาคำขอใช้สิทธิว่าสอดคล้องกับเงื่อนไขที่กฎหมายกำหนดในการขอใช้สิทธิแต่ละกรณีหรือไม่ โดยในส่วนขอใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ โรงพยาบาลสงขลานครินทร์อาจพิจารณาปฏิเสธคำขอใช้สิทธิของผู้รับบริการได้ หากเห็นว่าเป็นกรณีดังต่อไปนี้

(๑) ข้อมูลส่วนบุคคลนั้นยังมีความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยโรงพยาบาลสงขลานครินทร์จะต้องพิจารณาความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวตามวัตถุประสงค์ที่เก็บรวบรวมไว้ เช่น ยังมีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวไว้เพื่อการให้บริการสุขภาพตามมาตรฐานของสถานพยาบาล เพื่อการปฏิบัติตามกฎหมายว่าด้วยสถานพยาบาล หรือเพื่อเป็นหลักฐานอ้างอิงทางกฎหมายสำหรับคดีที่อาจเกิดขึ้นและยังไม่หมดอายุความ เป็นต้น ทั้งนี้ ตามนัยมาตรา ๓๓ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และไม่ใช้กรณีที่เข้าเงื่อนไขตาม (๒) (๓) หรือ (๔)

(๒) การเก็บรักษาไว้เพื่อวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพ หรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ หรือการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ ตามมาตรา ๒๖ (๕) (ก) หรือเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุขตามมาตรา ๒๖ (๕) (ข) หรือการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือ การใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ซึ่งมาตรา ๓๓ วรรคสอง กำหนดยกเว้นมิให้นำสิทธิขอให้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา ๓๓ วรรคหนึ่ง มาใช้บังคับกับการเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ดังกล่าว

ดังนั้น โรงพยาบาลสงขลานครินทร์สามารถปฏิเสธคำขอใช้สิทธิลบหรือทำลาย หรือทำให้ ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ของผู้ร้องขอ ดังกล่าวได้ หากมีความจำเป็นต้องเก็บรักษาข้อมูลประวัติการรักษาของผู้ป่วยนั้นไว้ตามกฎหมายว่าด้วย สถานพยาบาล หรือเพื่อวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมาย หรือเป็นข้อมูลส่วนบุคคลที่เก็บรักษาไว้ เพื่อวัตถุประสงค์ตามมาตรา ๒๖ (๕) (ก) หรือ (ข) หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ซึ่งเป็นกรณีเฉพาะที่ได้รับยกเว้นมิให้นำสิทธิดังกล่าวมาใช้บังคับ โรงพยาบาลสงขลานครินทร์ จึงควรพิจารณาแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบว่า ไม่อาจดำเนินการตามคำขอใช้สิทธิของเจ้าของ ข้อมูลส่วนบุคคลได้ พร้อมชี้แจงเหตุผล ตามมาตรา ๓๓ วรรคหนึ่งและวรรคสอง และวรรคห้า แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบข้อ ๓ วรรคหนึ่ง และข้อ ๘ วรรคสาม ของประกาศคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถ ระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการ ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของ ข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่จะเป็นกรณีที่ได้รับยกเว้น ตามที่กำหนดไว้ในมาตรา ๓๗ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อีกด้วย ดังนั้น สำหรับข้อมูลส่วนบุคคลเกี่ยวกับ ประวัติการรักษาของผู้รับบริการที่โรงพยาบาลได้เก็บรวบรวมไว้เกินกว่า ๕ ปีนับแต่วันจัดทำตามที่กฎหมายว่าด้วย สถานพยาบาลกำหนด มหาวิทยาลัยสงขลานครินทร์ โดยโรงพยาบาลสงขลานครินทร์ ในฐานะผู้ควบคุม ข้อมูลส่วนบุคคล จะต้องพิจารณาว่าข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ ต่าง ๆ ที่กำหนดไว้โดยชอบด้วยกฎหมายแล้วหรือไม่ หรือยังมีความจำเป็นต้องเก็บรักษาไว้เพื่อวัตถุประสงค์ ตามมาตรา ๒๖ (๕) (ก) หรือ (ข) หรือการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือ การใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย หากเห็นว่าการเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ต่าง ๆ หมดความจำเป็นแล้วตามมาตรา ๓๗ (๓) หรือเป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิตามมาตรา ๓๓ ได้ โรงพยาบาลสงขลานครินทร์

ต้องดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามหลักเกณฑ์ที่กำหนดไว้ในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗

ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ ตามมาตรา ๓๓ วรรคสี่ ประกอบมาตรา ๗๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒