ประกาศโรงพยาบาลปราสาท
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙

โรงพยาบาลปราสาท ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) จึงได้จัดทำนโยบายฉบับนี้ขึ้น เพื่อกำหนดหลักเกณฑ์ แนวทาง และมาตรการในการเก็บรวบรวม ใช้ เปิดเผย และประมวลผลข้อมูลส่วนบุคคลของทุกภาคส่วนที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล

เพื่อให้การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพ สอดคล้องตามกฎหมาย และเป็นมาตรฐานเดียวกันทั้งองค์กร โรงพยาบาลปราสาทจึงกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

คำนิยามคำศัพท์

เว้นแต่จะกำหนดไว้เป็นอย่างอื่น คำนิยามศัพท์ในแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ให้มีความหมาย ดังนี้

“โรงพยาบาล” หมายถึง โรงพยาบาลปราสาท

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ทั้งนี้ตามมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒

“ข้อมูลส่วนบุคคลอ่อนไหว” หมายถึง ข้อมูลส่วนบุคคลตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒ เช่น ข้อมูลสุขภาพ ข้อมูลชีวภาพ (ลายนิ้วมือ ระบบจดจำใบหน้า) ข้อมูลเชื้อชาติ ข้อมูลความพิการ เป็นต้น

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดาที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง โรงพยาบาลปราสาท ในฐานะผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของโรงพยาบาล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)” หมายถึง บุคคลซึ่งโรงพยาบาลแต่งตั้งเพื่อทำหน้าที่ ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒

๑. วัตถุประสงค์

ประกาศ นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙ ฉบับนี้ มีวัตถุประสงค์เพื่อ

๑.๑ กำหนดนโยบายและแนวทางการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาล ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้อง

๑.๒ สร้างความเชื่อมั่นให้แก่ผู้รับบริการ บุคลากร และผู้มีส่วนเกี่ยวข้อง ว่าข้อมูลส่วนบุคคลจะได้รับการคุ้มครองอย่างเหมาะสม

๑.๓ กำหนดบทบาทหน้าที่ของบุคลากรทุกระดับในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๒. ขอบเขตการบังคับใช้

ประกาศ นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙ ฉบับนี้ มีผลบังคับใช้กับ

๒.๑ บุคลากรของโรงพยาบาล ทุกประเภท ได้แก่ ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานกระทรวงสาธารณสุข นักศึกษาฝึกงาน อาสาสมัคร และบุคคลภายนอกที่ปฏิบัติงานในนามโรงพยาบาล

๒.๒ ข้อมูลส่วนบุคคลทุกประเภท ที่โรงพยาบาลเก็บรวบรวม ใช้ หรือเปิดเผย ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์ ครอบคลุม ดังนี้

๑) ข้อมูลผู้ป่วย/ผู้รับบริการ (ข้อมูลการรักษาพยาบาล เวชระเบียน ข้อมูลการเงิน)

๒) ข้อมูลบุคลากร (ข้อมูลการบริหารทรัพยากรบุคคล)

๓) ข้อมูลผู้มาติดต่อ ผู้ร้องเรียน ญาติผู้ป่วย คู่สัญญา

๒.๓ ระบบสารสนเทศทุกระบบ ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล รวมถึงระบบ HIS, ระบบจองคิว, ระบบเวชระเบียนอิเล็กทรอนิกส์ และระบบสนับสนุนอื่น ๆ

๓. หลักการคุ้มครองข้อมูลส่วนบุคคล

โรงพยาบาลยึดถือหลักการดังต่อไปนี้

๓.๑ หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส

๑) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำบนฐานทางกฎหมายที่ชอบด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒

๒) แจ้งวัตถุประสงค์และรายละเอียดการประมวลผลข้อมูล ให้เจ้าของข้อมูลทราบผ่าน Privacy Notice

๓.๒ หลักการจำกัดวัตถุประสงค์

๑) เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะตามวัตถุประสงค์ที่แจ้งไว้ ไม่นำไปใช้เพื่อวัตถุประสงค์อื่นโดยไม่ชอบด้วยกฎหมาย

๓.๓ หลักการเก็บรวบรวมข้อมูลเท่าที่จำเป็น

๑) เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ (Data Minimization)

๓.๔ หลักความถูกต้อง

๑) ดำเนินการให้ข้อมูลส่วนบุคคลมีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

๓.๕ หลักการจำกัดระยะเวลาจัดเก็บ

๑) จัดเก็บข้อมูลส่วนบุคคลไว้ไม่เกินระยะเวลาที่จำเป็นตามวัตถุประสงค์ หรือตามที่กฎหมายกำหนด

๒) เวชระเบียน: จัดเก็บไม่น้อยกว่า ๑๐ ปี นับแต่วันที่ผู้ป่วยมารับบริการครั้งสุดท้าย (ตามข้อบังคับแพทย์สภา)

๓) ข้อมูลบุคลากร: จัดเก็บตลอดระยะเวลาที่มีนิติสัมพันธ์ และอีก ๑๐ ปี หลังพ้นสภาพ

๔) เมื่อพ้นระยะเวลาจัดเก็บ จะลบหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

๓.๖ หลักความมั่นคงปลอดภัย

๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ทั้งทางเทคนิค

กายภาพ และทางบริหารจัดการ

๓.๗ หลักความรับผิดชอบ

๑) โรงพยาบาลสามารถแสดงให้เห็นว่าได้ปฏิบัติตามหลักการข้างต้นได้

๔. ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

โรงพยาบาลอาศัยฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ดังนี้

ฐานทางกฎหมาย	ตัวอย่างการใช้งาน
ฐานหน้าที่ตามกฎหมาย (มาตรา ๒๔(๖))	การรักษาพยาบาลตาม พ.ร.บ.สถานพยาบาล, การรายงานโรคตาม พ.ร.บ.โรคติดต่อ
ฐานประโยชน์สำคัญต่อชีวิต (มาตรา ๒๔(๒))	การรักษาพยาบาลฉุกเฉิน กรณีเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
ฐานภารกิจของรัฐ (มาตรา ๒๔(๔))	การจัดบริการสาธารณสุข การเฝ้าระวังโรค การส่งเสริมสุขภาพ
ฐานความยินยอม (มาตรา ๑๙)	กรณีที่ไม่มีฐานทางกฎหมายอื่นรองรับ เช่น การวิจัย การแพทย์ทางไกลบางกรณี
ฐานสัญญา (มาตรา ๒๔(๓))	การจ้างงาน สัญญาจัดซื้อจัดจ้าง

๕. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒ ดังนี้

๕.๑ สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (มาตรา ๓๐)

๕.๒ สิทธิในการขอรับสำเนาข้อมูลส่วนบุคคล และขอให้โอนข้อมูล (มาตรา ๓๑)

๕.๓ สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล (มาตรา ๓๒)

๕.๔ สิทธิในการขอให้ลบหรือทำลายข้อมูล (มาตรา ๓๓)

๕.๕ สิทธิในการขอให้ระงับการใช้ข้อมูล (มาตรา ๓๔)

๕.๖ สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (มาตรา ๓๕)

๕.๗ สิทธิในการถอนความยินยอม (มาตรา ๑๙ วรรค ๕)

๕.๘ สิทธิในการร้องเรียน (มาตรา ๗๓)

ช่องทางการใช้สิทธิ

๑) ยื่นแบบฟอร์มขอใช้สิทธิ ณ จุดบริการเวชระเบียน โรงพยาบาลปราสาท

๒) ส่งเอกสารทางไปรษณีย์ ถึง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โรงพยาบาลปราสาท ๖๐๒ หมู่ ๒ ถ.โชคชัย-เดชอุดม ต.กังแอน อ.ปราสาท จ.สุรินทร์ ๓๒๑๔๐

๖. มาตรการรักษาความมั่นคงปลอดภัย

โรงพยาบาลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล อย่างน้อยดังต่อไปนี้

๖.๑ มาตรการทางเทคนิค

๑) ระบบควบคุมการเข้าถึง (Access Control) ระบบสารสนเทศ โดยกำหนดสิทธิ์ตามภาระหน้าที่

๒) การเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลที่มีความอ่อนไหว

๓) ระบบป้องกันการบุกรุก (Firewall, Antivirus, IDS/IPS)

๔) การสำรองข้อมูล (Backup) อย่างสม่ำเสมอ

๕) การบันทึก Log การเข้าถึงข้อมูลส่วนบุคคล

๖.๒ มาตรการทางกายภาพ

๑) ห้องเซิร์ฟเวอร์มีระบบควบคุมการเข้า - ออก

๒) เอกสารที่มีข้อมูลส่วนบุคคลจัดเก็บในตู้ที่ล็อคกุญแจ

๓) การทำลายเอกสารด้วยเครื่องทำลายเอกสาร

๖.๓ มาตรการทางบริหารจัดการ

๑) กำหนดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

๒) อบรมและสร้างความตระหนักแก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง

๓) ตรวจสอบและทบทวนมาตรการรักษาความมั่นคงปลอดภัยอย่างน้อยปีละ ๑ ครั้ง

๔) จัดให้มีข้อตกลงการประมวลผลข้อมูล (DPA) กับผู้ประมวลผลภายนอก

๕) จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูล (ROPA)

๗. การเปิดเผยข้อมูลส่วนบุคคลให้บุคคลภายนอก

การเปิดเผยข้อมูลส่วนบุคคลให้บุคคลภายนอกต้องดำเนินการ ดังนี้

๗.๑ มีฐานทางกฎหมายรองรับ หรือได้รับความยินยอมจากเจ้าของข้อมูล

๗.๒ จัดทำข้อตกลงการแบ่งปันข้อมูล (DSA) หรือข้อตกลงการประมวลผลข้อมูล (DPA) แล้วแต่กรณี

๗.๓ กรณีส่งข้อมูลไปยังต่างประเทศ ต้องปฏิบัติตามหลักเกณฑ์ตามมาตรา ๒๘ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๘. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

๘.๑ เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ

๘.๒ กรณีที่เหตุการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า

๘.๓ ให้ปฏิบัติตามแนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของโรงพยาบาลปราสาท

๙. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๙.๑ โรงพยาบาลแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามคำสั่งโรงพยาบาลปราสาทที่เกี่ยวข้อง

๙.๒ DPO มีหน้าที่ตามมาตรา ๔๒ แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒ ดังนี้

๑) ให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎหมาย

๒) ตรวจสอบการดำเนินงานของโรงพยาบาลให้เป็นไปตามกฎหมาย

๓) ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๑๐. การทบทวนและปรับปรุง

ให้ทบทวนและปรับปรุงประกาศฉบับนี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของกฎหมาย ระเบียบ หรือมาตรฐานที่เกี่ยวข้อง

๑๑. การบังคับใช้

ประกาศฉบับนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ลงนามเป็นต้นไป

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชูหงส์ มหรรทัศนพงศ์)
ผู้อำนวยการโรงพยาบาลปราสาท