ประกาศโรงพยาบาลปราสาท
เรื่อง นโยบายธรรมาภิบาลข้อมูลและการจัดจำแนกชั้นความลับ
(Data Governance & Data Classification Policy)

โรงพยาบาลปราสาท ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้จัดทำนโยบายธรรมาภิบาลข้อมูลและการจัดจำแนกชั้นความลับฉบับนี้ขึ้น เพื่อกำหนดหลักเกณฑ์ แนวทางและมาตรการในการดำเนินงานด้านธรรมาภิบาลข้อมูลและการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลให้เป็นไปอย่างมีประสิทธิภาพ สอดคล้องตามกฎหมายและเป็นมาตรฐานเดียวกันทั้งองค์กร

โรงพยาบาลปราสาทจึงกำหนดนโยบายธรรมาภิบาลข้อมูลและการจัดจำแนกชั้นความลับ ดังต่อไปนี้

๑. วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการข้อมูลของโรงพยาบาลให้เป็นระบบ มีการกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน และมีการจัดจำแนกชั้นความลับของข้อมูลตามระดับความสำคัญและความอ่อนไหว เพื่อให้มีมาตรการควบคุมที่เหมาะสมอันเป็นการป้องกันความเสี่ยงจากการเข้าถึง การใช้ การเปิดเผย การแก้ไขหรือการทำลายข้อมูลโดยมิชอบ ทั้งนี้ เพื่อคุ้มครองข้อมูลผู้ป่วย ข้อมูลส่วนบุคคล และข้อมูลองค์กรให้มีความมั่นคงปลอดภัย

๒. ขอบเขต

นโยบายฉบับนี้ครอบคลุมข้อมูลสารสนเทศทั้งหมดของโรงพยาบาล ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic Data) หรือเอกสารกระดาษรวมถึงข้อมูลที่จัดเก็บ ประมวลผล หรือส่งผ่านในระบบเทคโนโลยีสารสนเทศ อุปกรณ์สื่อสาร และสื่อบันทึกข้อมูลทุกประเภท ตลอดจนข้อมูลที่อยู่ภายใต้การดูแลของบุคลากรหรือผู้ให้บริการภายนอกที่เกี่ยวข้องกับโรงพยาบาล

๓. โครงสร้างธรรมาภิบาลข้อมูล

เพื่อให้การบริการจัดการข้อมูลเป็นไปตามหลักความรับผิดชอบและตรวจสอบได้ (Accountability) โรงพยาบาลปราสาทกำหนดบทบาทหน้าที่ ดังต่อไปนี้

๓.๑ เจ้าของข้อมูล (Data Owner)

หมายถึง ผู้บริหารหรือหัวหน้ากลุ่มงาน/ฝ่ายที่เป็นหน่วยงานเจ้าของกระบวนการ (Business Process Owner) ซึ่งมีอำนาจหน้าที่ในการกำหนดระดับชั้นความลับของข้อมูล อนุมัติสิทธิ์การเข้าถึง กำหนดวัตถุประสงค์การใช้ข้อมูลและกำกับดูแลให้การใช้ข้อมูลเป็นไปตามกฎหมายและนโยบายที่กำหนด

๓.๒ ผู้ดูแลข้อมูล (Data Custodian)

หมายถึง หน่วยงานหรือบุคลากรด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในการจัดเก็บ บำรุงรักษา และควบคุมความมั่นคงปลอดภัยของระบบที่ใช้จัดเก็บหรือประมวลผลข้อมูล โดยต้องดำเนินการตามข้อกำหนดของเจ้าของข้อมูลและมาตรการด้านความมั่นคงปลอดภัยขององค์กร

๓.๓ ผู้ใช้งานข้อมูล (Data User)

หมายถึง บุคลากรของโรงพยาบาลหรือผู้ได้รับอนุญาตที่มีสิทธิ์เข้าถึงและใช้ข้อมูลตามบทบาทหน้าที่ โดยต้องปฏิบัติตามนโยบาย ระเบียบและมาตรการควบคุมที่กำหนดอย่างเคร่งครัด และรับผิดชอบต่อการใช้ข้อมูลภายใต้สิทธิ์ที่ได้รับอนุญาต

๔. การจัดจำแนกชั้นความลับ (Data Classification)

โรงพยาบาลปราสาทกำหนดชั้นความลับข้อมูลเป็น ๔ ระดับ ดังนี้

ระดับชั้นความลับ	นิยาม	ตัวอย่างข้อมูล	มาตรการควบคุม
๑. ความลับที่สุด (Top Secret)	ข้อมูลสารสนเทศที่มีระดับความอ่อนไหวสูงสุด หากถูกเปิดเผย สูญหาย ถูกแก้ไข หรือเข้าถึงโดยมิชอบ จะก่อให้เกิดความเสียหายร้ายแรงอย่างยิ่งต่อผู้ป่วย บุคลากร ชื่อเสียงองค์กร หรือความมั่นคงของระบบบริการสุขภาพ	- เวชระเบียนฉบับสมบูรณ์และข้อมูลสุขภาพเชิงลึกของผู้ป่วย - ข้อมูลส่วนบุคคลอ่อนไหวตามกฎหมาย (เช่น ประวัติการเจ็บป่วย โรคประจำตัว ผลตรวจ HIV สุขภาพจิต) - รหัสผ่านระบบหลัก, Private Key, Token การเข้าระบบ - ฐานข้อมูลระบบ HIS ทั้งระบบ	- กำหนดสิทธิ์เข้าถึงแบบจำกัดเฉพาะรายบุคคล (Need-to-know) - ใช้ Multi-Factor Authentication (MFA) - เข้ารหัสข้อมูลทั้งขณะจัดเก็บ (Encryption at Rest) และขณะส่งผ่าน (Encryption in Transit) - บันทึกและตรวจสอบ Audit Log อย่างสม่ำเสมอ - ห้ามจัดเก็บในอุปกรณ์ส่วนบุคคลโดยไม่ได้รับอนุญาต - ทำลายเอกสาร/สื่อบันทึกข้อมูลตามมาตรฐานความปลอดภัย
๒. ความลับมาก (Secret)	ข้อมูลที่มีความอ่อนไหวสูง หากถูกเปิดเผยหรือรั่วไหล อาจก่อให้เกิดความเสียหายร้ายแรงต่อการดำเนินงาน ชื่อเสียง หรือก่อให้เกิดผลกระทบทางกฎหมายต่อหน่วยงาน	- ข้อมูลสุขภาพผู้ป่วย - รายบุคคลบางส่วน - รายงานการสอบสวนเหตุการณ์ทางการแพทย์ - รายงานเหตุการณ์ความเสี่ยง (Risk Report) - แผนรับมือเหตุฉุกเฉินด้าน IT	- จำกัดสิทธิ์ตามบทบาทหน้าที่ (Role-Based Access Control) - กำหนดการยืนยันตัวตนก่อนเข้าถึงระบบ - ห้ามเผยแพร่ผ่านช่องทางสาธารณะ-จัดเก็บในระบบที่มีการควบคุมสิทธิ์และมีการสำรองข้อมูล
๓. ข้อมูลลับ (Confidential)	ข้อมูลที่ใช้ภายในหน่วยงาน ซึ่งไม่ควรเปิดเผยต่อสาธารณะ	- ข้อมูลบุคลากร (ประวัติการทำงาน เงินเดือน)	- จำกัดสิทธิ์การเข้าถึงตามตำแหน่งงาน

ระดับชั้นความลับ	นิยาม	ตัวอย่างข้อมูล	มาตรการควบคุม
	หากรั่วไหลอาจส่งผลกระทบต่อการบริหารจัดการ ความเชื่อมั่น หรือสิทธิส่วนบุคคลในระดับหนึ่ง	- แผนงบประมาณที่ยังไม่ประกาศ - รายงานภายในฝ่ายงาน	- ระบุชั้นความลับ “Confidential” บนเอกสาร - หลีกเลี่ยงการส่งผ่านช่องทางที่ไม่ปลอดภัย
๔. ข้อมูลใช้งานภายใน (Internal)	ข้อมูลที่ใช้ร่วมกันภายในโรงพยาบาลเพื่อสนับสนุนการปฏิบัติงาน ไม่เหมาะสมต่อการเผยแพร่สู่ภายนอก แต่หากเปิดเผยจะมีผลกระทบในระดับต่ำ	- ระเบียบปฏิบัติงานภายใน - คำสั่งโรงพยาบาล - รายงานสถิติภายในที่ไม่ระบุตัวบุคคล	- ให้บุคลากรภายในเข้าถึงได้ตามความจำเป็น - ห้ามเผยแพร่ภายนอกโดยไม่ได้รับอนุญาต
๕. เปิดเผยได้ (Public)	ข้อมูลที่ได้รับอนุมัติให้เผยแพร่สู่สาธารณะโดยไม่ก่อให้เกิดผลกระทบต่อผู้ป่วย บุคลากร หรือองค์กร	- ข่าวประชาสัมพันธ์ - ข้อมูลบริการผู้ป่วย - แผ่นพับความรู้สุขภาพ - รายงานประจำปีที่เผยแพร่แล้ว	- เผยแพร่ผ่านเว็บไซต์หรือช่องทางสื่อสารอย่างเป็นทางการ - ตรวจสอบความถูกต้องก่อนเผยแพร่

๕. แนวระเบียบปฏิบัติในการจัดการข้อมูล (Information Handling Guidelines)

เพื่อให้การจัดการข้อมูลแต่ละระดับเป็นไปตามหลักความมั่นคงปลอดภัยของสารสนเทศ (Confidentiality, Integrity, Availability) กำหนดแนวปฏิบัติ ดังนี้

๕.๑ การพิมพ์เอกสาร (Printing Control) ข้อมูลที่จัดอยู่ในระดับ ๑ (ความลับที่สุด) และระดับ ๒ (ความลับมาก) ต้องควบคุมการพิมพ์อย่างเคร่งครัด โดยผู้พิมพ์ต้องอยู่รอรับเอกสารจากเครื่องพิมพ์ทันที และห้ามปล่อยทิ้งไว้โดยไม่มีผู้ดูแล ทั้งนี้ เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยมิชอบ

๕.๒ การส่งข้อมูลทางไปรษณีย์อิเล็กทรอนิกส์ (Email Transmission) การส่งข้อมูลระดับ ๑ ต้องดำเนินการผ่านระบบอีเมลของหน่วยงานที่มีมาตรการรักษาความมั่นคงปลอดภัย และต้องมีการเข้ารหัสข้อมูล (Encryption) ก่อนส่งทุกครั้งกรณีแนบไฟล์เอกสาร ให้บีบอัดไฟล์พร้อมกำหนดรหัสผ่าน (Password Protection) และส่งรหัสผ่านผ่านช่องทางสื่อสารอื่นที่แยกจากกัน เพื่อเพิ่มระดับความปลอดภัย

๕.๓ การทำลายข้อมูล (Secure Disposal) เอกสารหรือสื่อบันทึกข้อมูลที่จัดอยู่ในระดับ ๑ และระดับ ๒ เมื่อพ้นระยะเวลาการเก็บรักษาหรือไม่มีความจำเป็นต้องใช้งานแล้ว ต้องทำลายด้วยวิธีที่ปลอดภัย เช่น การใช้เครื่องทำลายเอกสาร (Paper Shredder) หรือวิธีการทำลายที่ไม่สามารถกู้คืนข้อมูลได้ห้ามนำเอกสารดังกล่าวไปจำหน่ายเป็นเศษกระดาษ หรือนำกลับมาใช้ซ้ำโดยเด็ดขาด

๖. บัญชีรายการกิจกรรมการประมวลผลข้อมูล (Record of Processing Activities: ROPA)

เพื่อให้เป็นไปตามหลักความรับผิดชอบและตรวจสอบได้ (Accountability) และสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖.๑ ทุกหน่วยงานต้องจัดทำ “บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)” ของตนเอง

๖.๒ ต้องจัดทำบัญชีรายการข้อมูล (Data Inventory) เพื่อระบุประเภทของข้อมูล วัตถุประสงค์การใช้แหล่งที่มา ระยะเวลาเก็บรักษาและระดับชั้นความลับของข้อมูล ตัวอย่างดังนี้

ลำดับ	รายการ	รายละเอียด
๑	ชื่อและข้อมูลติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล	ชื่อ ที่อยู่ ช่องทางติดต่อของโรงพยาบาล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๒	วัตถุประสงค์ของการประมวลผล	ระบุวัตถุประสงค์เฉพาะเจาะจงและชัดเจนของแต่ละกิจกรรม เช่น การรักษาพยาบาล การเบิกจ่ายค่ารักษา การวิจัย
๓	ฐานทางกฎหมาย (Lawful Basis)	ระบุฐานทางกฎหมายที่ใช้อ้างอิง เช่น ความยินยอม สัญญา หน้าที่ตามกฎหมาย ประโยชน์อันชอบด้วยกฎหมาย หรือภารกิจสาธารณะ
๔	ประเภทของเจ้าของข้อมูล	ระบุกลุ่มเจ้าของข้อมูล เช่น ผู้ป่วย บุคลากร ญาติผู้ป่วย คู่สัญญา นักศึกษาฝึกงาน อาสาสมัคร
๕	ประเภทของข้อมูลส่วนบุคคล	ระบุหมวดหมู่ข้อมูล เช่น ข้อมูลทั่วไป ข้อมูลสุขภาพ ข้อมูลชีวมิติ ข้อมูลทางการเงิน โดยจำแนกข้อมูลอ่อนไหว (Sensitive Data) ให้ชัดเจน
๖	แหล่งที่มาของข้อมูล	ระบุช่องทางการเก็บรวบรวม เช่น จากเจ้าของข้อมูลโดยตรง จากหน่วยงานที่ส่งต่อ จากระบบสารสนเทศ
๗	ผู้รับข้อมูล/หน่วยงานที่เปิดเผย	ระบุบุคคลหรือหน่วยงานที่ได้รับการเปิดเผยข้อมูล ทั้งภายในและภายนอก รวมถึงผู้ประมวลผลข้อมูล
๘	การส่งหรือโอนข้อมูลไปต่างประเทศ	ระบุว่ามีการส่งข้อมูลไปยังต่างประเทศหรือไม่ หากมี ให้ระบุประเทศปลายทางและมาตรการคุ้มครอง
๙	ระยะเวลาในการเก็บรักษาข้อมูล	ระบุระยะเวลาเก็บรักษาหรือเกณฑ์ในการกำหนดระยะเวลา โดยอ้างอิงตารางกำหนดอายุการเก็บเอกสาร
๑๐	มาตรการรักษาความมั่นคงปลอดภัย	ระบุมาตรการทางเทคนิคและทางองค์กรที่ใช้คุ้มครองข้อมูล เช่น การเข้ารหัส การควบคุมการเข้าถึง การสำรองข้อมูล
๑๑	ระดับชั้นความลับของข้อมูล	จำแนกระดับชั้นความลับ เช่น ข้อมูลสาธารณะ ข้อมูลภายใน ข้อมูลลับ ข้อมูลลับมาก

๖.๓ ต้องทบทวนและปรับปรุงข้อมูลดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกระบวนการประมวลผลข้อมูลอย่างมีนัยสำคัญ

๖.๔ บัญชีรายการดังกล่าว ในข้อ ๖.๒ ต้องสามารถแสดงต่อผู้มีอำนาจตรวจสอบได้เมื่อร้องขอจากผู้มีอำนาจตรวจสอบ ได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) กระทรวงสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุข สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.) หรือหน่วยงานกำกับดูแลอื่นที่เกี่ยวข้องได้

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชูหงส์ มหรรทัศนพงศ์)
ผู้อำนวยการโรงพยาบาลปราสาท