ประกาศโรงพยาบาลวาปีปทุม
เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)
โรงพยาบาลวาปีปทุม

โรงพยาบาลวาปีปทุมมีการนำระบบเทคโนโลยีสารสนเทศและเทคโนโลยีดิจิทัลมาใช้ในการบริหารจัดการ การให้บริการทางการแพทย์ และการดำเนินงานของหน่วยงานอย่างต่อเนื่อง ซึ่งเกี่ยวข้องกับการจัดเก็บ การใช้ การประมวลผล การเชื่อมโยง และการแลกเปลี่ยนข้อมูลจำนวนมาก จึงมีความจำเป็นต้องกำหนดแนวทางในการบริหารจัดการข้อมูล ให้มีคุณภาพ ถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย สามารถตรวจสอบได้ และนำไปใช้ประโยชน์ได้อย่างเหมาะสม โดยคำนึงถึงสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูล

เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลวาปีปทุมเป็นไปอย่างมีมาตรฐาน โปร่งใส ตรวจสอบได้ และสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และนโยบายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ตลอดจนแนวทางธรรมาภิบาลข้อมูลภาครัฐ และแนวทางของกระทรวงสาธารณสุข โรงพยาบาลวาปีปทุมจึงกำหนดนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) เพื่อใช้เป็นกรอบในการกำกับดูแล และบริหารจัดการข้อมูลขององค์กร ดังต่อไปนี้

๑. วัตถุประสงค์

๑.๑ กำหนดกรอบ หลักการ และแนวทางในการกำกับดูแลและบริหารจัดการข้อมูลของโรงพยาบาลให้เป็นระบบและมีมาตรฐานเดียวกัน

๑.๒ ส่งเสริมให้ข้อมูลมีคุณภาพ มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน น่าเชื่อถือ และพร้อมต่อการนำไปใช้ประโยชน์

๑.๓ กำหนดบทบาท หน้าที่ ความรับผิดชอบ และสิทธิในการเข้าถึงข้อมูลของบุคลากรและผู้เกี่ยวข้องอย่างชัดเจน

๑.๔ คุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพ รวมถึงลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๑.๕ สนับสนุนการเชื่อมโยง แลกเปลี่ยน และใช้ข้อมูลเพื่อการบริการ การบริหาร การพัฒนาคุณภาพ และการตัดสินใจเชิงนโยบายอย่างเหมาะสม

๒. ขอบเขตการบังคับใช้

นโยบายนี้ใช้กับข้อมูลทุกประเภทที่โรงพยาบาลวาปีปทุมเป็นผู้จัดเก็บ ครอบครอง ใช้ ประมวลผล หรือรับผิดชอบ ไม่ว่าจะอยู่ในรูปแบบเอกสาร กระดาษ ฐานข้อมูล ระบบสารสนเทศ สื่อดิจิทัล หรือบริการบนเครือข่าย รวมถึงข้อมูลผู้ป่วย ข้อมูลบุคลากร ข้อมูลทางการเงิน ข้อมูลพัสดุ ข้อมูลบริหารจัดการ ข้อมูลสถิติ และข้อมูลอื่นที่เกี่ยวข้องกับภารกิจของโรงพยาบาล โดยให้บุคลากร ลูกจ้าง ผู้รับจ้าง ผู้ให้บริการระบบ และผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูลถือปฏิบัติตามนโยบายนี้

๓. หลักการและแนวทางธรรมาภิบาลข้อมูล

๓.๑ การกำกับดูแลข้อมูล (Data Governance) ให้มีคณะกรรมการธรรมาภิบาลข้อมูลเป็นกลไกกำหนดนโยบาย กำกับ ติดตาม และทบทวนการบริหารจัดการข้อมูลของโรงพยาบาล รวมทั้งแต่งตั้งผู้รับผิดชอบข้อมูลในระดับที่เหมาะสม

๓.๒ การจัดทำทะเบียนข้อมูล (Data Inventory) ให้ทุกหน่วยงานสำรวจและจัดทำทะเบียนชุดข้อมูล ระบบสารสนเทศ แหล่งที่มาของข้อมูล ผู้รับผิดชอบ วัตถุประสงค์การใช้ และระดับความสำคัญของข้อมูล พร้อมทบทวนให้เป็นปัจจุบัน

๓.๓ มาตรฐานและคำอธิบายข้อมูล (Data Standard & Data Dictionary) ให้กำหนดมาตรฐานชื่อข้อมูล รูปแบบข้อมูล รหัสอ้างอิง และคำอธิบายข้อมูลที่สำคัญ เพื่อลดความซ้ำซ้อนและทำให้ข้อมูลสามารถเชื่อมโยงหรือแลกเปลี่ยนกันได้อย่างถูกต้อง

๓.๔ คุณภาพข้อมูล (Data Quality) ข้อมูลต้องมีความถูกต้อง ครบถ้วน สอดคล้อง เป็นปัจจุบัน ไม่ซ้ำซ้อน และสามารถตรวจสอบย้อนกลับได้ โดยหน่วยงานเจ้าของข้อมูลต้องมีกระบวนการตรวจสอบ แก้ไข และติดตามคุณภาพข้อมูลอย่างสม่ำเสมอ

๓.๕ การจำแนกชั้นข้อมูลและสิทธิ์การเข้าถึง (Data Classification & Access Control) ให้จำแนกข้อมูลตามระดับความสำคัญและความอ่อนไหว เช่น ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลลับ และข้อมูลส่วนบุคคล/ข้อมูลสุขภาพ และกำหนดสิทธิ์เข้าถึงตามหน้าที่และความจำเป็นเท่านั้น

๓.๖ การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) การเก็บรวบรวม ใช้ เปิดเผย ส่งต่อ หรือทำลายข้อมูลส่วนบุคคลต้องมีฐานกฎหมายหรือวัตถุประสงค์ที่ชัดเจน ใช้ข้อมูลเท่าที่จำเป็น และมีมาตรการคุ้มครองสิทธิของเจ้าของข้อมูลตามกฎหมาย

๓.๗ ความมั่นคงปลอดภัยของข้อมูล (Data Security) ต้องมีมาตรการทางเทคนิคและทางบริหารที่เหมาะสม เช่น การยืนยันตัวตน การกำหนดสิทธิ์ การเข้ารหัส การสำรองข้อมูล การบันทึกเหตุการณ์ การบริหารช่องโหว่ และการป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

๓.๘ การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Sharing & Exchange) การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายในหรือภายนอกต้องพิจารณาความจำเป็น วัตถุประสงค์ สิทธิในการใช้ข้อมูล ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งมีข้อตกลงหรือหลักฐานการอนุญาตเมื่อจำเป็น

๓.๙ การจัดเก็บและการทำลายข้อมูล (Data Retention & Disposal) ให้กำหนดระยะเวลาการจัดเก็บข้อมูลตามกฎหมาย ภารกิจ และความจำเป็น เมื่อพ้นระยะเวลาหรือหมดความจำเป็นให้มีวิธีทำลายข้อมูลอย่างเหมาะสมและไม่สามารถกู้คืนเพื่อใช้งานโดยมิชอบได้

๓.๑๐ การบันทึกและตรวจสอบย้อนหลัง (Logging & Auditability) ระบบสารสนเทศที่สำคัญควรมีการบันทึกการใช้งาน การเข้าถึง การแก้ไข และเหตุการณ์ที่เกี่ยวข้องกับข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังและใช้ประกอบการสอบสวนเหตุการณ์ได้

๓.๑๑ การบริหารเหตุการณ์ข้อมูล (Data Incident Management) เมื่อพบเหตุข้อมูลรั่วไหล สูญหาย ถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัย ให้รายงานผู้รับผิดชอบและดำเนินการตามแผนตอบสนองเหตุการณ์ของโรงพยาบาลโดยเร่งด่วน

๓.๑๒ การสร้างความตระหนักและพัฒนาบุคลากร โรงพยาบาลส่งเสริมให้บุคลากรได้รับความรู้และสร้างความตระหนักด้านธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๔. บทบาทและความรับผิดชอบ

๔.๑ คณะกรรมการธรรมาภิบาลข้อมูล กำหนดนโยบาย มาตรฐาน กำกับติดตาม ให้คำแนะนำ และทบทวนผลการดำเนินงานด้านธรรมาภิบาลข้อมูลของโรงพยาบาล

๔.๒ เจ้าของข้อมูล (Data Owner) กำหนดวัตถุประสงค์ การใช้ สิทธิ์เข้าถึง คุณภาพ และการดูแลชุดข้อมูลที่อยู่ในความรับผิดชอบ

๔.๓ ผู้ดูแลข้อมูล/ผู้ประสานงานข้อมูล (Data Steward) ดูแลความถูกต้อง มาตรฐาน คุณภาพ และประสานการปรับปรุงข้อมูลให้เป็นไปตามนโยบาย

๔.๔ ผู้ดูแลระบบ (System Administrator / IT) ดูแลระบบ โครงสร้างพื้นฐาน การสำรองข้อมูล การควบคุมสิทธิ์ การบันทึกเหตุการณ์ และมาตรการความมั่นคงปลอดภัยทางเทคนิค

๔.๕ ผู้ใช้งานข้อมูล (Data User) ใช้ข้อมูลตามสิทธิ์และวัตถุประสงค์ที่ได้รับอนุญาต ไม่เปิดเผย ส่งต่อ หรือใช้ข้อมูลนอกเหนือจากหน้าที่โดยไม่ได้รับอนุญาต

๕. การติดตาม ทบทวน และการปฏิบัติตามนโยบาย

๕.๑ ให้คณะกรรมการธรรมาภิบาลข้อมูลกำกับ ติดตาม และประเมินผลการดำเนินงานตามนโยบายนี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย ระบบสารสนเทศ หรือความเสี่ยงที่มีนัยสำคัญ

๕.๒ หน่วยงานทุกหน่วยต้องให้ความร่วมมือในการจัดทำทะเบียนข้อมูล การประเมินคุณภาพข้อมูล การประเมินความเสี่ยง และการตรวจสอบตามที่คณะกรรมการกำหนด

๕.๓ กรณีพบการฝ่าฝืนนโยบายหรือการใช้ข้อมูลไม่เหมาะสม ให้รายงานผู้บังคับบัญชาและคณะกรรมการธรรมาภิบาลข้อมูล เพื่อพิจารณาดำเนินการแก้ไขและมาตรการที่เหมาะสม

๕.๔ นโยบายฉบับนี้ให้เผยแพร่ให้บุคลากรและผู้เกี่ยวข้องรับทราบ และถือปฏิบัติอย่างเคร่งครัด

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ประกาศเป็นต้นไป

สั่ง ณ วันที่ ๒ เดือน กุมภาพันธ์ ๒๕๖๙

(นางเบญจพร อินทกรอุดม)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)
รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลวาปีปทุม