ประกาศโรงพยาบาลวัดจันทร์เฉลิมพระเกียรติ ๘๐ พรรษา

เรื่อง แนวทางปฏิบัติมาตรฐาน (SOPs) ด้านการบริหารจัดการข้อมูลและความมั่นคงปลอดภัยไซเบอร์ โรงพยาบาลวัดจันทร์เฉลิมพระเกียรติ ๘๐ พรรษา

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการรักษาพยาบาลและการบริหารจัดการข้อมูลสุขภาพ "ข้อมูล" จึงเปรียบเสมือนทรัพย์สินที่มีค่าที่สุดอย่างหนึ่งของโรงพยาบาลวัดจันทร์เฉลิมพระเกียรติ ๘๐ พรรษา ความถูกต้อง ความเป็นส่วนตัว และความพร้อมใช้งานของข้อมูลไม่เพียงแต่ส่งผลต่อประสิทธิภาพในการรักษาพยาบาลเท่านั้น แต่ยังรวมถึงความปลอดภัยในชีวิตของผู้ป่วยและความเชื่อมั่นของประชาชนที่มีต่อหน่วยงาน ปัจจุบันภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนมากขึ้น รวมถึงข้อกำหนดทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ทำให้โรงพยาบาลจำเป็นต้องมีมาตรฐานการปฏิบัติงานที่ชัดเจน เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ การรั่วไหลของข้อมูล หรือการใช้งานข้อมูลที่ผิดวัตถุประสงค์

เพื่อให้เจ้าหน้าที่ทุกระดับมีแนวทางปฏิบัติที่เป็นเอกภาพ สามารถรับมือกับสถานการณ์ปกติและสถานการณ์ฉุกเฉินได้อย่างทันท่วงที โรงพยาบาลจึงได้จัดทำ แนวทางปฏิบัติมาตรฐาน (Standard Operating Procedures: SOPs) ด้านการบริหารจัดการข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบเกณฑ์ในการปฏิบัติงานให้สอดคล้องกับหลักธรรมาภิบาลข้อมูลและมาตรฐานการสาธารณสุขสากลต่อไป

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑ มีนาคม ๒๕๖๙

(นายนคร รัตนรักษ์)
นายแพทย์ชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลวัดจันทร์เฉลิมพระเกียรติ ๘๐พรรษา

แนวทางปฏิบัติมาตรฐาน (SOPs) ด้านการบริหารจัดการข้อมูลและความมั่นคงปลอดภัยไซเบอร์ โรงพยาบาลวัดจันทร์เฉลิมพระเกียรติ ๘๐ พรรษา

หมวดที่ ๑ ขั้นตอนการเข้าถึงและใช้งานระบบสารสนเทศ (Access Management)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑. การขอสิทธิ เจ้าหน้าที่ใหม่ต้องกรอกแบบฟอร์มขอใช้งานระบบ โดยระบุบทบาทหน้าที่ (Role) และได้รับการอนุมัติจากหัวหน้าฝ่าย

๒. การยืนยันตัวตน ห้ามใช้ User ID และ Password ร่วมกันเด็ดขาด (One Account, One User)

๓. การออกจากระบบ ต้อง Log-out หรือ Lock หน้าจอ (Windows + L) ทุกครั้งที่ลุกจากที่นั่งทำงาน

๔. การยกเลิกสิทธิ ฝ่ายบริหารทรัพยากรบุคคล (HR) ต้องแจ้งฝ่าย IT ทันทีเมื่อมีเจ้าหน้าที่ลาออกหรือย้ายหน้าที่ เพื่อระงับสิทธิภายใน ๒๔ ชั่วโมง

หมวดที่ ๒ ขั้นตอนการจัดการข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล (Data Privacy)

วัตถุประสงค์ เพื่อคุ้มครองความเป็นส่วนตัวตามกฎหมาย PDPA

๑. การเก็บรวบรวม แจ้งวัตถุประสงค์การเก็บข้อมูลผ่าน "ประกาศความเป็นส่วนตัว" (Privacy Notice) ที่จุดลงทะเบียน

๒. การส่งต่อข้อมูลทางโซเชียล ห้าม ส่งภาพใบหน้าผู้ป่วย ผล Lab หรือข้อมูลที่ระบุตัวตนผู้ป่วยผ่านแอปพลิเคชัน Line หรือ Facebook ส่วนตัว (ให้ใช้ระบบส่งต่อของโรงพยาบาลที่กำหนดเท่านั้น)

๓. การขอสำเนาเวชระเบียน ผู้ป่วยหรือญาติที่มีสิทธิตามกฎหมายต้องกรอกแบบฟอร์มคำร้อง และแสดงบัตรประชาชนเพื่อยืนยันตัวตนก่อนได้รับข้อมูลทุกครั้ง

๔. การทำลายเอกสาร เอกสารที่มีชื่อ-นามสกุล หรือข้อมูลสุขภาพผู้ป่วยที่ไม่ได้ใช้งานแล้ว ต้องทำลายด้วยเครื่องย่อยเอกสารเท่านั้น ห้ามทิ้งลงถังขยะทั่วไป

หมวดที่ ๓: ขั้นตอนการสำรองและกู้คืนข้อมูล (Backup & Recovery)

วัตถุประสงค์ เพื่อความต่อเนื่องในการรักษาพยาบาล (Business Continuity)

๑. การสำรองข้อมูลอัตโนมัติ: ฝ่าย IT ตั้งค่าระบบสำรองข้อมูลฐานข้อมูล HIS ทุกวัน (Daily Backup)

๒. การจัดเก็บสำเนา เก็บข้อมูลสำรองไว้อย่างน้อย ๒ แหล่ง (Local Server และ Offline Storage/Cloud)

๓. การทดสอบกู้คืน: ฝ่าย IT ต้องทำการทดสอบกู้คืนข้อมูล (Restore Test) ทุก ๓ เดือน เพื่อตรวจสอบความพร้อมใช้งานของไฟล์สำรอง

หมวดที่ ๔ ขั้นตอนการตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์ (Incident Response)

วัตถุประสงค์ เพื่อระงับเหตุและลดความเสียหายเมื่อถูกโจมตี (เช่น Ransomware)

๑. การตรวจพบ เมื่อพบอาการผิดปกติ เช่น เครื่องช้าลงมาก, ไฟล์เปิดไม่ได้, มีข้อความเรียกค่าไถ่ ให้เจ้าหน้าที่ "ดึงสาย LAN หรือปิด Wi-Fi" ทันที

๒. การแจ้งเหตุ แจ้งฝ่าย IT หรือเลขานุการคณะกรรมการฯ ทันทีภายใน ๑๕ นาที

๓. การจำกัดวง ฝ่าย IT ตัดการเชื่อมต่อระบบเครือข่ายส่วนที่ติดเชื้อเพื่อป้องกันการแพร่กระจาย

๔. การบันทึกเหตุการณ์ บันทึกเวลาที่เกิดเหตุ ลักษณะความเสียหาย และประเมินว่ามีข้อมูลส่วนบุคคลรั่วไหลหรือไม่ เพื่อรายงานต่อหน่วยงานกำกับดูแลภายใน ๗๒ ชั่วโมง

/การ.....

การบังคับใช้

ให้หัวหน้ากลุ่มงานทุกฝ่าย ควบคุมกำดูแลให้เจ้าหน้าที่ในสังกัดปฏิบัติตาม SOPs นี้อย่างเคร่งครัด หากพบปัญหาในการปฏิบัติให้รายงานคณะกรรมการธรรมาภิบาลข้อมูลเพื่อพิจารณาปรับปรุงต่อไป