ระเบียบวิธีปฏิบัติ เรื่อง การรักษาความลับและการเข้าถึงข้อมูลของผู้ป่วย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการและขั้นตอนในการรักษาความลับและการควบคุมการเข้าถึงข้อมูลส่วนบุคคลของผู้ป่วยให้เป็นไปตามกฎหมายและมาตรฐานด้านความปลอดภัยของข้อมูล

๒. ขอบเขต

ใช้กับบุคลากรทุกคนของสถานพยาบาล
รวมถึงบุคลากรภายนอกที่ได้รับมอบหมายให้ปฏิบัติงานซึ่งต้องใช้ข้อมูลของผู้ป่วย

๓. คำจำกัดความ

- ข้อมูลส่วนบุคคล (Personal Data): ข้อมูลใด ๆ
ที่ทำให้สามารถระบุตัวตนบุคคลได้โดยตรงหรือโดยอ้อม

- ข้อมูลสุขภาพ (Health Data): ข้อมูลเกี่ยวกับสภาพร่างกาย จิตใจ การรักษา
หรือประวัติทางการแพทย์ของผู้ป่วย

- การเข้าถึงข้อมูล (Access): การดู แก้ไข หรือดาวน์โหลดข้อมูลในระบบหรือเอกสาร

๔. บทบาทและความรับผิดชอบ

- เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator): จัดการสิทธิ์การเข้าถึงข้อมูล
และตรวจสอบการใช้งานระบบ

- แพทย์/พยาบาล: เข้าถึงและใช้ข้อมูลเท่าที่จำเป็นต่อการรักษาพยาบาล

- เจ้าหน้าที่บันทึกเวชระเบียน: จัดเก็บและป้องกันเอกสารเวชระเบียนจากการเข้าถึงโดยไม่ได้รับอนุญาต

- บุคลากรทุกคน: รักษาความลับของข้อมูลผู้ป่วย และไม่เปิดเผยข้อมูลแก่บุคคลที่ไม่มีสิทธิ์

๕. ขั้นตอนการปฏิบัติ

๕.๑ การควบคุมการเข้าถึง (Access Control)

๑) ใช้รหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ที่กำหนดเป็นการส่วนตัว

๒) กำหนดสิทธิ์ตามหน้าที่งาน (Role-based Access Control – RBAC)

๓) ปิดสิทธิ์การเข้าถึงทันทีเมื่อบุคลากรลาออกหรือเปลี่ยนตำแหน่งงาน

๕.๒ การเก็บรักษาข้อมูล (Data Storage & Protection)

๑) เอกสารเวชระเบียนกระดาษต้องเก็บในตู้ที่ล็อกได้

๒) ข้อมูลอิเล็กทรอนิกส์ต้องจัดเก็บในระบบที่มีการเข้ารหัส (Encryption)

๓) สำรองข้อมูลเป็นประจำ และเก็บในพื้นที่ปลอดภัย

๕.๓ การใช้และการเปิดเผยข้อมูล (Use & Disclosure)

๑) ใช้ข้อมูลเท่าที่จำเป็น (Need-to-know basis)

๒) เปิดเผยข้อมูลแก่หน่วยงานภายนอกได้ต่อเมื่อมีความยินยอมเป็นลายลักษณ์อักษรจากผู้ป่วย หรือมีกฎหมายกำหนด

๓) จัดทำบันทึกการเปิดเผยข้อมูลทุกครั้ง

๕.๔ การติดตามและตรวจสอบ (Monitoring & Audit)

๑) บันทึก (Log) การเข้าถึงข้อมูลทุกครั้ง

๒) ตรวจสอบ Log อย่างน้อยเดือนละครั้ง

๓) รายงานเหตุการณ์ผิดปกติทันทีต่อผู้จัดการด้านความปลอดภัยข้อมูล

๖. การฝ่าฝืนระเบียบ

- อาจถูกลงโทษทางวินัย ตั้งแต่ตักเตือนเป็นลายลักษณ์อักษร ไปจนถึงเลิกจ้าง
- อาจมีความผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง

๗. การทบทวนและปรับปรุง

ทบทวนระเบียบนี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีกฎหมายหรือมาตรฐานใหม่ที่เกี่ยวข้อง

๘. เอกสารอ้างอิง

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ และที่แก้ไขเพิ่มเติม
- HIPAA Privacy Rule (Health Insurance Portability and Accountability Act, USA)