QM–ISI-MAK–001–00

นโยบายคุณภาพ/คู่มือคุณภาพ
เรื่อง
ความมั่นคงปลอดภัยของระบบสารสนเทศ

โรงพยาบาลเขาคิชฌกูฏ จังหวัดจันทบุรี

	ชื่อ – สกุล	ลายเซ็น	ว.ด.ป.
ผู้จัดทำ	นายเมธี เบ็ญจวรรณ์ (คณะกรรมการทีมคุณภาพ/หัวหน้างาน/งาน)	.....	.....
ผู้ทบทวน	นายศิลา หลิมเจริญ (ประธานทีมคุณภาพ/หัวหน้ากลุ่มงาน)	.....	.....
ผู้อนุมัติ	นายแพทย์สมยศ พนธารา (ผู้อำนวยการโรงพยาบาล)	.....	.....

สำเนาฉบับที่ A(1)

เอกสาร [/] ควบคุม [ ] ไม่ควบคุม

สารบัญ

หน้า

1.วัตถุประสงค์ 3

2. ขอบข่าย 3

3. วิธีการปฏิบัติ 3-5

การควบคุมระบบเอกสารคุณภาพ

ประวัติการแก้ไข จำนวนทั้งหมด 5 หน้า

ครั้งที่	วันที่ประกาศใช้	รายละเอียด	แผ่นที่
00	4 ม.ค. 2562	ประกาศใช้เอกสารทั้งฉบับ	-

1.วัตถุประสงค์

เพื่อเป็นมาตรฐานให้ทุกหน่วยงานถือปฏิบัติไปในแนวทางเดียวกัน

2.ขอบข่าย

ใช้เป็นแนวทางการปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ

3.วิธีการปฏิบัติ

3.1 ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) ได้แก่

- ห้องเก็บ server แยกเฉพาะ ตู้แร็คและห้องมีกุญแจล็อคเก็บไว้เฉพาะผู้ดูแลระบบเท่านั้น
- มีระบบสำรองไฟฟ้า 30 นาที
- เมื่อเกิดอัคคีภัยใช้ถังดับเพลิงสีเขียวที่ติดตั้งเตรียมไว้หน้าศูนย์คอมพิวเตอร์ อุปกรณ์ที่สำคัญติดตั้งในตู้แร็คมีล้อเลื่อนสามารถเคลื่อนย้ายได้ทันที

3.2 ความมั่นคงปลอดภัยทางบริหารจัดการ (Administrative Security) ได้แก่

- มีนโยบาย และ ระเบียบปฏิบัติชัดเจน
- การกำหนดสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมกับการเข้าใช้งาน
- การกำหนดการเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น โปรแกรมประยุกต์ ระบบเครือข่ายไร้สาย
- การจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับตามหน้าที่ที่รับผิดชอบ

3.3 ความมั่นคงปลอดภัยของผู้ใช้งาน (User Security) ได้แก่

- ต้องลงทะเบียนในอินเตอร์เน็ต และระบบ HOSxP ทุกคน
- ผู้ใช้งานมีรหัสส่วนตัวในการเข้าใช้ระบบ รับผิดชอบตามรหัสที่ได้รับ
- ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย และต้องเปลี่ยนรหัสผ่านทุก 6 เดือน
- ต้องเข้าระบบด้วยรหัสผู้ใช้งาน และรหัสผ่านของตนเองเท่านั้น ทั้งในระบบอินเตอร์เน็ต และระบบ HOSxP
- ต้องออกจากระบบทุกครั้งที่เลิกใช้งาน ทั้งระบบอินเตอร์เน็ต และระบบ HOSxP
- ห้ามเปิดเผยรหัสผู้ใช้งานและรหัสผ่านให้ผู้อื่นทราบ
- ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง ทำลายข้อมูลผู้ป่วยในเวชระเบียนและคอมพิวเตอร์
- ผู้ใช้งานต้องได้รับอนุญาตจากผู้ดูแลระบบ ในการเคลื่อนย้ายอุปกรณ์และเครื่องคอมพิวเตอร์

- ผู้ใช้งานห้ามติดตั้งโปรแกรมอื่นโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
- ผู้ใช้ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์โดยไม่ปกปิดหรือรักษาความลับผู้ป่วย ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยหรือญาติ
- ผู้ใช้ต้องรับผิดชอบในการกระทำอื่นๆ ที่เป็นสาเหตุที่ทำให้อุปกรณ์และเครื่องคอมพิวเตอร์เกิดความเสียหาย

3.4 ความมั่นคงปลอดภัยของระบบเครือขาย (Network Security) ได้แก่
- ผู้ดูแลระบบบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์
- การเข้าถึงตัวอุปกรณ์ไฟร์วอล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบ
- ข้อมูลจราจรทางคอมพิวเตอร์ ต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
- ผู้ดูและระบบมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย

3.5 ความมั่นคงปลอดภัยของระบบสารสนเทศ (System Security) ได้แก่
- การใช้ระบบล็อกหน้าจอเพื่อป้องกันการติดไวรัส หรือการเสียหายของเครื่องคอมพิวเตอร์
- ห้ามใช้ระบบอินเตอร์เน็ตของโรงพยาบาล เข้าเว็บไซต์ไม่เหมาะสมอันก่อให้เกิดความเสียหาย
- ห้ามนำโน๊ตบุคส่วนตัวเชื่อมต่อกับระบบโรงพยาบาล หากไม่ได้ติดตั้งโปรแกรมต้านไวรัสไว้
- ต้องลงทะเบียนก่อนนำคอมพิวเตอร์ โน้ตบุค หรือมือถือ มาเชื่อมต่อกับระบบโรงพยาบาล

3.6 ความมั่นคงปลอดภัยของข่อมูล (data security) ได้แก่
- ผู้ใช้งานมีรหัสในการเข้าถึงข้อมูลในระบบงานต่างๆ
- ระบบการสำรองข้อมูลจัดเก็บทุกวัน

4. สถานพยาบาลมีมาตรการคุ่มครองความเปนสวนตัว (Privacy) ของขอมูลสารสนเทศ ทั้งข้อมูลส่วนบุคคลเกี่ยวกับบุคลากร และข้อมูลสุขภาพของผูปวย ได้แก่

4.1 มีกระบวนการขอความยินยอมโดยไดรับการบอกกลาว (Informed Consent) ในการเก็บรวบรวม ใชและเปดเผยขอมูลสวนบุคคลของบุคลากรและผูปวย ยกเวน กรณีฉุกเฉิน หรือกรณีที่มีกฎหมายหรือระเบียบปฏิบัติกำหนดไว้เป็นอยางอื่น
- ในการขอความยินยอมจากผู้ป่วย หรือผู้แทนโดยชอบธรรม ต้องแจ้งให้ผู้นั้นทราบวัตถุประสงค์ รูปแบบ ช่องทาง และผลดีผลเสียของการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลดังกล่าวให้ทราบและเข้าใจอย่างถ่องแท้ พร้อมทั้งมีโอกาสซักถามก่อนให้ความยินยอม ทั้งนี้ต้องเป็นความยินยอมโดยสมัครใจอย่างแท้จริง

4.2 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลที่สำคัญเพียงเทาที่จำเป็น (Need-To-Know Basis) เพื่อให้สามารถทำงานได้ ได้แก่

- จำกัดการเข้าถึงข้อมูลในโปรแกรม HOSxP โดยรหัสผู้ใช้งาน และรหัสผ่าน

4.3 ระมัดระวังการระบุและเปิดเผยตัวตนของบุคลากรหรือผู้ป่วยในเอกสารตางๆ โดยระบุหรือเปดเผยเพียงเทาที่จำเปน และระมัดระวังการเขาถึงเอกสารเหลานี้และควรมีมาตรการทำลายเอกสารเหล่านี้อยางปลอดภัย ได้แก่

- การทำลายเอกสารที่เป็นประวัติผู้ป่วย โดยเอกสารที่จะทำลายจะต้องย้อนหลัง 5 ปี
- มีการล็อกกุญแจ ของห้องเก็บเอกสารที่รอทำลายเพื่อไม่ให้ผู้อื่นเข้าถึงเอกสาร ก่อนได้รับอนุญาต

4.4 มีมาตรการในการคุ่มครองความเปนสวนตัวของขอมูล ในการนำขอมูลสวนบุคคลของบุคลากรหรือผู่ป่วยไปใชงานอยางอื่น (secondary use of data) ได้แก่

- มีการกรอกแบบฟอร์มการขอประวัติผู้ป่วยทั้งที่เป็นประวัติของตนเองหรือเป็นญาติมาขอ เพื่อเป็นการแสดงความยินยอมในการเปิดเผยประวัติการรักษา เพื่อนำไปใช้ประโยชน์อื่น ส่วนตัว