**มาตรฐานการจัดการความมั่นคงของข้อมูลผู้ป่วยโรงพยาบาลสัตหีบ กม.10**

สถานพยาบาลมีกิจกรรมหลักในการให้การดูแลรักษาส่งเสริมสุขภาพป้องกันโรคให้แก่ผู้มารับบริการกิจกรรมเหล่านี้ต้องใช้ข้อมูลผู้ป่วยหรือผู้มารับบริการเพื่อวินิจฉัยโรคและวางแผนการรักษาข้อมูลผู้ป่วยจะถูกบันทึกเป็นลายลักษณ์อักษรปรากฏอยู่ในเวชระเบียนเอกสารและฐานข้อมูลของสถานพยาบาลเจ้าหน้าที่สถานพยาบาลทุกคนจะต้องดำเนินการต่อข้อมูลผู้ป่วยเหล่านี้ด้วยความระมัดระวังโดยเฉพาะความลับผู้ป่วยต้องระวังมิให้เกิดความละเมิดความเป็นส่วนตัวหรือเปิดเผยความลับของผู้ป่วยโดยเด็ดขาด

**1. มาตรฐานความมั่นคงปลอดภัย (Security Standards**)

มาตรฐานนี้มุ่งเน้นการธำรงรักษาระบบสารสนเทศ (information systems) และข้อมูลสารสนเทศ(information) เพื่อเป้าหมายที่สำคัญ 3 ประการคือ

* การรักษาความลับของข้อมูล (confidentiality) เพื่อให้ปลอดภัยจากการล่วงรู้หรือเปิดเผย

โดยมิชอบโดยผู้ที่ไม่เกี่ยวข้อง

* การรักษาความถูกต้องครบถ้วนของข้อมูล (integrity) เพื่อไม่ให้ข้อมูลถูกลบเพิ่มหรือแก้ไขโดยมิชอบโดยผู้ที่ไม่เกี่ยวข้อง
* การรักษาความคงอยู่ของระบบสารสนเทศและข้อมูลสารสนเทศ (availability) เพื่อให้

สามารถใช้การและเข้าถึงได้เมื่อมีความจำเป็น

**2. มาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Privacy Standards)**

มาตรฐานนี้มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลโดยมีนโยบายและมาตรการต่างๆเพื่อจำกัดการ

เข้าถึงและเพื่อคุ้มครองไม่ให้มีการเก็บใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างไม่เหมาะสมและส่งผลกระทบต่อเจ้าของข้อมูล

**สถานพยาบาลของรัฐจึงเข้าข่ายหน่วยงานที่ต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด**

**พระราชบัญญัติสุขภาพแห่งชาติพ.ศ. 2550 มาตรา 7 บัญญัติไว้ว่า “ข้อมูลด้านสุขภาพของบุคคล**

**เป็นความลับส่วนบุคคลผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรงหรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผยแต่ไม่ว่าในกรณีใดๆผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้”**

ประมวลกฎหมายอาญามาตรา 323 วรรคหนึ่งบัญญัติไว้ว่า “ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น

โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่โดยเหตุที่ประกอบอาชีพเป็นแพทย์เภสัชกรคนจำหน่ายยานางผดุงครรภ์ผู้พยาบาลนักบวชหมอความทนายความหรือผู้สอบบัญชีหรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้นแล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใดต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งพันบาทหรือทั้งจำทั้งปรับ”

**แนวทางปฏิบัติสำหรับโรงพยาบาล**

ทุกคนที่เกี่ยวข้องกับการจัดการข้อมูลผู้ป่วยจึงต้องมีหน้าที่รับผิดชอบในการดูแลรักษาความลับผู้ป่วยตามแนวทาง 3 ด้านคือ

1. แนวปฏิบัติทั่วไป

2. แนวปฏิบัติสำหรับเจ้าหน้าที่ทุกคน

3. แนวปฏิบัติสำหรับเจ้าหน้าที่เวชระเบียนและเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

แนวปฏิบัติข้อ 1 และ 2 ใช้บังคับกับเจ้าหน้าที่ทุกคนที่มีโอกาสเข้าถึงข้อมูลผู้ป่วยส่วนแนวปฏิบัติข้อ

3 ใช้บังคับกับเจ้าหน้าที่ผู้รับผิดชอบดูแลเวชระเบียนและเจ้าหน้าที่ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและ

ฐานข้อมูลเท่านั้น

**แนวทางปฏิบัติทั่วไปสำหรับโรงพยาบาล**

แนวทางปฏิบัติทั่วไปหมายถึงการป้องกันดูแลมิให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยและ

ความลับผู้ป่วยจะต้องปฏิบัติให้ได้อย่างน้อยตามแนวทางปฏิบัตินี้รวม 7 เรื่องคือ

1. กำหนดและแบ่งแยกบริเวณพื้นที่จัดเก็บเวชระเบียนและเครื่องแม่ข่ายคอมพิวเตอร์ให้ชัดเจน

กำหนดเป็นเขตหวงห้ามเฉพาะปิดหรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่

ประจำอยู่

2. จัดให้มีสมุดทะเบียนบันทึกการเข้าออกห้องเครื่องแม่ข่ายคอมพิวเตอร์และสมุดทะเบียนบันทึกการนำเวชระเบียนออกมาใช้และการส่งเวชระเบียนกลับคืน

3. จัดให้มีระบบตรวจสอบการส่งเวชระเบียนกลับคืนว่ามีการส่งกลับครบเท่ากับจำนวนเวชระเบียนที่นำออกไปดำเนินการตรวจสอบทุกวันให้เสร็จสิ้นก่อนเวลา 16.00 น. หากพบเวชระเบียนที่ยัง

ไม่ส่งกลับให้ดำเนินการติดตามค้นหานำกลับคืนมาให้เสร็จสิ้นก่อนเวลา 16.30 น.

4. จัดให้มีระบบฉุกเฉินสำหรับปฏิบัติงานเมื่อไฟฟ้าดับหรือระบบคอมพิวเตอร์ใช้งานไม่ได้ให้มั่นใจว่าการค้นหาบันทึกและจัดเก็บข้อมูลผู้ป่วยดำเนินไปได้อย่างครบถ้วนถูกต้องไม่บกพร่องและมี

การซักซ้อมเป็นระยะๆเช่นทุกปีและปรับปรุงกระบวนการทำงานเมื่อระบบขัดข้องให้เหมาะสม

อยู่เสมอ

5. กำหนดชั้นความลับของข้อมูลผู้ป่วยเป็นระดับ “ลับ” และดำเนินการแบบเดียวกับการรับส่ง

เอกสารลับดังนี้5.1 การทำสำเนาการพิมพ์สำเนาต้องบันทึกจำนวนชุดชื่อตำแหน่งของผู้ดำเนินการชื่อ

สถานพยาบาลที่จัดทำวันเวลาไว้ที่ต้นฉบับและฉบับสำเนาทุกฉบับกรณีสั่งพิมพ์สำเนาออก

จากระบบคอมพิวเตอร์ต้องบันทึกการสั่งพิมพ์จำนวนชุดชื่อตำแหน่งของผู้ดำเนินการชื่อ

สถานพยาบาลที่จัดทำวันเวลาที่สั่งพิมพ์ทุกครั้งเก็บไว้ในระบบฐานข้อมูล

5.2 การส่งออกเวชระเบียนหรือสำเนาเวชระเบียนออกนอกสถานพยาบาลต้องบรรจุซอง

หรือภาชนะทึบแสงสองชั้นอย่างมั่นคงบนซองชั้นในให้จ่าหน้าระบุเลขที่หนังสือนำส่งชื่อหรือ

ตำแหน่งผู้รับและหน่วยงานผู้ส่งพร้อมทำเครื่องหมายแสดงชั้นความลับทั้งด้านหน้าและ

ด้านหลังบนซองชั้นนอกให้จ่าหน้าระบุเลขที่หนังสือนำส่งชื่อหรือตำแหน่งผู้รับและหน่วยงานผู้ส่งเช่นเดียวกับซองชั้นในแต่ไม่ต้องมีเครื่องหมายแสดงชั้นความลับใดๆการส่งออกในรูปแบบไฟล์อิเล็กทรอนิกส์ต้องเข้ารหัสมิให้ผู้ที่ไม่มีสิทธิ์สามารถเปิดไฟล์ดูได้

5.3 การจัดเก็บเวชระเบียนเวชระเบียนผู้ป่วยที่อยู่ในพื้นที่รับผิดชอบของโรงพยาบาลให้

จัดเก็บไว้ตลอดไปหากผู้ป่วยเสียชีวิตให้แยกเวชระเบียนของผู้เสียชีวิตออกมาเก็บไว้ใน

สถานที่เก็บเวชระเบียนผู้เสียชีวิตโดยหากเป็นการเสียชีวิตผิดธรรมชาติให้เก็บรักษาไว้ไม่ต่ำ

กว่า 20 ปีหากมิใช่การเสียชีวิตผิดธรรมชาติให้เก็บรักษาไว้ไม่ต่ำกว่า 10 ปีแล้วอาจพิจารณา

ทำลายเวชระเบียนถ้ามีปัญหาพื้นที่จัดเก็บไม่เพียงพอการทำลายเวชระเบียนให้ดำเนินการ

โดยหลักการทำลายเอกสารเช่นใช้เครื่องทำลายเอกสารตัดออกเป็นชิ้นเล็กๆ

6. จัดให้มีกระบวนการกลั่นกรองและพิจารณาความเหมาะสมในการนำข้อมูลของผู้ป่วยที่สามารถระบุตัวบุคคลได้ (เช่นมีชื่อหรือเลขประจำตัวผู้ป่วย) ไปใช้ประโยชน์อย่างอื่นเช่นการวิจัยหรือ

เปิดเผยต่อบุคคลอื่นนอกโรงพยาบาลให้เป็นไปตามกฎหมายและไม่เป็นการละเมิดสิทธิของผู้ป่วย

7. จัดให้มีระบบยินยอมให้ใช้ข้อมูลผู้ป่วยดังตัวอย่าง**หนังสืออนุญาตของผู้ป่วยให้ใช้ข้อมูลของตนเพื่อการตรวจรักษาโรคและส่งข้อมูลให้กับกระทรวงสาธารณสุข**ให้ผู้ป่วยได้อ่านทำความเข้าใจและอนุญาตให้โรงพยาบาลใช้ข้อมูลเพื่อประโยชน์ในการดูแลรักษา

**แนวทางปฏิบัติทั่วไปสำหรับเจ้าหน้าที่ทุกคนที่มีโอกาสเข้าถึงข้อมูลผู้ป่วยของโรงพยาบาล**

แนวทางปฏิบัติทั่วไปสำหรับเจ้าหน้าที่หมายถึงแนวทางการรักษาความมั่นคงปลอดภัยและความลับ

ผู้ป่วยที่เจ้าหน้าที่ทุกคนที่มีโอกาสเข้าถึงข้อมูลผู้ป่วยต้องปฏิบัติให้ได้อย่างน้อยตามแนวทางปฏิบัตินี้รวม9เรื่องคือ

1. เจ้าหน้าที่ทุกคนมีหน้าที่ต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสารเวชระเบียนของผู้ป่วย

2. ห้ามเผยแพร่ทำสำเนาถ่ายภาพเปลี่ยนแปลงลบทิ้งหรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณีนอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ

3. การแก้ไขข้อมูลผู้ป่วยให้ดำเนินการได้ตามระเบียบปฏิบัติว่าด้วยการแก้ไขข้อมูลโดยเคร่งครัดเช่นหากเขียนผิดห้ามใช้ปากการะบายสีทึบทับข้อความจนไม่เห็นข้อความเดิมห้ามใช้น้ำยาลบ

คำผิดในเวชระเบียนผู้ป่วยการแก้ไขทำได้โดยการลากเส้นทับข้อความเดิมเพียงเส้นเดียวแล้ว

เขียนข้อความที่แก้ไขไว้ใกล้กับข้อความเดิมพร้อมลงนามกำกับและวันเวลาที่แก้ไขสำหรับการ

แก้ไขข้อมูลในระบบคอมพิวเตอร์ห้ามลบข้อมูลเดิมทิ้งแต่ให้ทำเครื่องหมายว่ามีการแก้ไขแล้ว

เชื่อมโยงข้อมูลที่เพิ่มเติมแก้ไขให้รู้ว่าข้อความใหม่ใช้แทนข้อความเดิมอย่างไร

4. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกันให้ดำเนินการตามระเบียบการส่งข้อมูลลับโดยเคร่งครัดเช่นไม่ใช้ให้ผู้ป่วยเป็นผู้ถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุดอื่นๆ

5. ห้ามส่งข้อมูลผู้ป่วยโดยใช้ช่องทางที่ไม่เหมาะสมเช่นส่งทาง LINE หรือ Social Media

6. ตั้งรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยากตรงตามระเบียบของสถานพยาบาลปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัดไม่อนุญาตให้ผู้อื่นนำรหัสผ่าน

ของตนเองไปใช้เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ

7. ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอกทุกกรณีสำหรับการเปิดไฟล์งานจากหน่วยงานภายในให้ตรวจหาไวรัสภายในไฟล์ทุกครั้งก่อนเปิดไฟล์

8. ห้ามนำเครื่องคอมพิวเตอร์อุปกรณ์อื่นๆรวมถึงอุปกรณ์จัดเก็บข้อมูลเช่น CD-ROM, USB Drive,External Hard Disk อุปกรณ์เครือข่ายเช่น Hub, Switch, Wi-Fi Router ฯลฯมาเชื่อมต่อกับ

เครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลที่ใช้ฐานข้อมูลผู้ป่วยยกเว้นได้รับอนุญาต

จากผู้อำนวยการ

9. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วยในการติดต่อกับ

อินเทอร์เน็ตทุกกรณียกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเทอร์เน็ตพร้อม

กันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วยซึ่งได้รับอนุญาตจากผู้อำนวยการ

**หนังสืออนุญาตของผู้ป่วยให้ใช้ข้อมูลของตนเพื่อการตรวจรักษาโรคและส่งข้อมูลให้กับกระทรวงสาธารณสุข โรงพยาบาลสัตหีบ กม.10**

---------------------------------------------------------------------------------------

ข้าพเจ้านางสาว/นาง/นาย………………………………………………………..…...ซึ่งเป็น [ ] ผู้ป่วยหรือ [ ] เป็นผู้แทนผู้ป่วยในฐานะ……………..............................................ของ

นางสาว/นาง/นาย……………………………………………………….. ได้รับการอธิบายจาก

.…………………………………………. ………ในฐานะตัวแทนคณะผู้ประกอบวิชาชีพเวชกรรม/

ประกอบโรคศิลปะที่ให้การดูแลแก่ผู้ป่วยภายใต้ขอบเขตของแพทย์แผนปัจจุบันเกี่ยวกับการสอบถามการบันทึกการจัดเก็บและการส่งต่อข้อมูลการเจ็บป่วยของข้าพเจ้าหรือผู้ป่วยที่ข้าพเจ้าเป็นตัวแทนตามคำอธิบายดังกล่าวข้าพเจ้าเข้าใจและรับทราบว่ามีสิทธิได้รับการปกปิดข้อมูลและมีหน้าที่ให้ข้อมูลสุขภาพและข้อเท็จจริงต่างๆทางการแพทย์ที่เป็นจริงและครบถ้วนตามคำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วยซึ่งปรากฏอยู่ด้านหลังของหนังสือฉบับนี้

ข้าพเจ้ายืนยันว่า

1. [ ] อนุญาต [ ] ไม่อนุญาตให้คณะแพทย์และเจ้าหน้าที่ของโรงพยาบาลบันทึกข้อมูลของผู้ป่วยไว้ในระบบเวชระเบียนและฐานข้อมูลของโรงพยาบาลเพื่อใช้ข้อมูลดังกล่าวประกอบการดูแลตรวจและรักษาแก่ข้าพเจ้า / ผู้ป่วยของข้าพเจ้าและส่งข้อมูลตามมาตรฐานการส่งข้อมูลให้กับกระทรวงสาธารณสุข

2. กรณีที่ข้าพเจ้าไม่อนุญาตให้บันทึกข้อมูลของผู้ป่วยไว้ในระบบเวชระเบียนและฐานข้อมูลของโรงพยาบาลการไม่อนุญาตนี้จะไม่ครอบคลุมกรณีฉุกเฉินเร่งด่วนที่คณะแพทย์และเจ้าหน้าที่ได้ให้การดูแลรักษาผู้ป่วยและได้บันทึกข้อมูลไปแล้วและข้าพเจ้าทราบดีว่าหากข้าพเจ้าไม่อนุญาตให้บันทึกข้อมูลของผู้ป่วยคณะแพทย์และเจ้าหน้าที่อาจไม่ได้ข้อมูลที่จำเป็นเพื่อการตัดสินใจรักษาโรคอย่างเหมาะสมและอาจจำเป็นต้องยุติการรักษาหรือส่งต่อผู้ป่วยไปยังโรงพยาบาลอื่นต่อไป

3. ในกรณีเจ็บป่วยฉุกเฉินวิกฤต [ ] อนุญาต [ ] ไม่อนุญาตให้คณะแพทย์และเจ้าหน้าที่ของโรงพยาบาลส่งข้อมูลของผู้ป่วยเพื่อขอคำปรึกษาจากผู้เชี่ยวชาญภายนอกโรงพยาบาลเพื่อให้ได้รับคำปรึกษามาช่วยประกอบการดูแลและรักษาโรคแก่ข้าพเจ้า / ผู้ป่วยของข้าพเจ้า

4. คำอนุญาตดังกล่าวให้มีผลตลอดระยะเวลาที่ผู้ป่วยยังคงรับการรักษาจากโรงพยาบาลทั้งกรณีผู้ป่วยนอกและผู้ป่วยในยกเว้นกรณีที่ข้าพเจ้าขอให้มีผลถึงวันที่ที่ระบุไว้คือ…………………………………..

ลงนามผู้อนุญาต…………………………. ลงนามพยานฝ่ายผู้ป่วย………………………

(…………………………………) (……………………………)

ความเกี่ยวข้องกับผู้ป่วย………………………….ความเกี่ยวข้องกับผู้ป่วย…………………

ลงนามเจ้าหน้าที่รพ. ..........…………… ……….ลงนามพยานฝ่ายเจ้าหน้าที่………………………

(…………………………………) (………………………………)

วันที่………เดือน…………………….พ.ศ…………………เวลา………….น.