การรักษาความปลอดภัยของข้อมูลผู้รับบริการโรงพยาบาลหนองม่วง

<u>การรักษาความปลอดภัย และป้องกันการสูญหายของแฟ้มเวชระเบียน</u> มีแนวทางในการปฏิบัติดังนี้

1. จัดสถานที่ให้เหมาะสำหรับจัดการเก็บรักษา โดยมีชั้นสำหรับใส่แฟ้มประวัติผู้ป่วยนอกและแฟ้มผู้ป่วยในและเน้นให้เก็บอย่างระมัดระวัง เพื่อลดความเสียหายทางกายภาพ มีช่องที่มีขนาดเหมาะสมหยิบใช้สะดวก ลดการเกิดการชำรุดของเวชระเบียน
2. สำรวจสายไฟในหน่วยงานไม่ให้ชำรุดสามารถใช้งานได้อย่างปลอดภัย เพื่อป้องกันอัคคีภัย
3. มีการจำลองเหตุการณ์ ร่วมซ้อมแผนภาวะฉุกเฉินของโรงพยาบาลและเตรียมความพร้อมเมื่อเกิดเหตุการณ์ฉุกเฉิน
4. จัดให้มีอุปกรณ์ดับเพลิง และมีการตรวจสอบให้ใช้งานได้อย่างมีประสิทธิภาพเพื่อป้องกันหรือบรรเทาความเสียหายทางกายภาพที่อาจเกิดขึ้นของเวชระเบียน
5. การสำรวจปลวกและกำจัดปลวกในหน่วยงาน และมีระบบการจัดการขยะที่เหมาะสมในหน่วยงานเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นในภายหลัง
6. สถานที่จัดเก็บแฟ้มเวชระเบียนของผู้ป่วยทุกประเภทห้ามบุคคลภายนอกเข้าไปโดยไม่ได้รับอนุญาต
7. การขอประวัติผู้ป่วยเพื่อไปใช้ภายนอกโรงพยาบาล ต้องทำบันทึกการขอข้อมูลตามแบบฟอร์มไว้เป็นหลักฐาน เพื่อขออนุญาตกับผู้บังคับบัญชา และพิจารณาเป็นรายกรณีไป โดยให้เฉพาะสำเนาเอกสารที่เกี่ยวข้องเท่านั้น
8. เจ้าหน้าที่ของแผนกเวชระเบียนทุกคนมีสิทธิที่จะเข้าถึงแฟ้มเวชระเบียนผู้ป่วยในได้ โดยทุกคนจะได้รับการอบรมในเรื่องการรักษาข้อมูลผู้ป่วย จรรยาบรรณของเจ้าหน้าที่เวชระเบียน ในการไม่เปิดเผยข้อมูล ไม่ว่าจะเป็นทางโทรศัพท์หรือการขอเข้าดู
9. มีการจัดเวรปฏิบัติงานตลอด 24 ชั่วโมง โดยเวรเช้าวันเสาร์-อาทิตย์จัดเวรละ 2 คน เวรบ่าย-ดึก เวรละ 1 คน และจัดเจ้าหน้าที่เสริมในวันที่มีผู้รับบริการมาเป็นพิเศษ เพื่อให้เพียงพอต่อการให้บริการ
10. แฟ้ม IPD ภายใน 15 วัน หลังจากผู้ป่วย Discharge เจ้าหน้าที่ผู้คืนจะต้องลงบันทึกการคืนในสมุดส่งคืนแฟ้มผู้ป่วยใน ส่วนเจ้าหน้าที่เวชระเบียนมีหน้าที่รับคืนโดย manual และบันทึกใน Computer
11. การประชุมชี้แจงนโยบายด้านเวชระเบียนให้กับเจ้าหน้าที่ของโรงพยาบาลทราบ
12. กรรมการสารสนเทศกำหนดผู้มีสิทธิและระดับความสามารถในการเข้าถึงข้อมูลในแฟ้มเวชระเบียนผู้ป่วย ดังนี้

ผู้มีสิทธิ

เจ้าหน้าที่ของหน่วยงานเวชระเบียนทุกคน

1. แพทย์/พยาบาล ที่ทำหน้าที่ดูแลผู้ป่วย
2. ผู้ทำงานวิจัย หรือนักศึกษาหลักสูตรทางการแพทย์และสาธารณสุขต่างๆ ที่ได้รับอนุญาตให้เข้าฝึกอบรมที่โรงพยาบาลหนองม่วง
3. ศาล ,บริษัทประกันชีวิต,สำนักงานหลักประกันสุขภาพแห่งชาติ, สำนักงานประกันสังคม,บริษัทกลางคุ้มครองผู้ประสบภัยจากรถ,กรมบัญชีกลาง ต้องทำหนังสือขอเข้าดูข้อมูล หรือมีหมายศาลโดยผ่านผู้อำนวยการโรงพยาบาล

ข้อมูลที่เกี่ยวข้องและระดับความสามารถเข้าถึงข้อมูล

1. ข้อมูลทางการแพทย์กำหนดให้แพทย์หรือผู้ที่รับมอบหมายเท่านั้นที่จะเป็นผู้เข้าถึง
2. ข้อมูลทางการพยาบาล กำหนดให้แพทย์/พยาบาลเท่านั้นที่จะเป็นผู้เข้าถึง
3. ข้อมูลทางเวชระเบียนผู้เกี่ยวข้องมีสิทธิ์สามารถเข้าถึงได้แต่ไม่สามารถแก้ไขข้อมูลได้

<u>การรักษาความปลอดภัย และป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบElectronic file</u>

โรงพยาบาลหนองม่วงใช้โปรแกรม HOSxP ในการจัดเก็บข้อมูลเวชระเบียนและการเข้ารับบริการของผู้ป่วยไว้ในคอมพิวเตอร์ โดยมีแนวทางในการปฏิบัติดังนี้

1. กำหนดให้เจ้าหน้าที่ที่ทำหน้าที่บันทึกข้อมูลต่างๆในคอมพิวเตอร์ มีรหัส username และ password เพื่อการเข้าถึงงานในแต่ละประเภท โดยรหัสที่กำหนดให้จะเข้าถึง(Access_menu) และใช้งานได้เฉพาะงานในหน้าที่ของตนเองเท่านั้นไม่สามารถใช้งานในด้านอื่นที่ไม่เกี่ยวข้องได้
2. เจ้าหน้าที่ของโรงพยาบาลทุกคนได้รับการอบรม ในเรื่องการรักษาข้อมูลผู้ป่วย จรรยาบรรณในการไม่เปิดเผยข้อมูล ซึ่งจะต้องปฏิบัติตามระเบียบการขอประวัติการรักษาเวชระเบียนผู้ป่วย
3. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งาน HOSxP ต้อง Log out ออกจากโปรแกรมทุกครั้งหากไม่ได้ปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ และตั้งเวลาให้โปรแกรม Log out อัตโนมัติกรณีที่ไม่มีใช้งานเป็นเวลานานเกิน 5 นาที
4. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งาน HOSxP ต้องเปลี่ยนรหัสผ่านใหม่ทุก 6 เดือน และตั้งค่าโปรแกรมให้มีการแจ้งเตือนและลบค่า password เดิมอัตโนมัติหากไม่มีการเปลี่ยนรหัสผ่านใหม่ภายในเวลาที่กำหนด
5. กำหนดให้โปรแกรมสามารถตรวจสอบเหตุผิดพลาดของงานและสืบสวนย้อนกลับได้ว่ามีการเข้าถึง การบันทึกหรือแก้ไข ข้อมูลของผู้ป่วยที่อยู่ในคอมพิวเตอร์ โดยรหัสผู้ใช้ของใคร มีการดำเนินการเมื่อไหร่

6. กำหนดให้โปรแกรมสามารถป้องกันการเข้าถึงข้อมูลและการนำข้อมูลในคอมพิวเตอร์ไปใช้งานโดยไม่ได้รับอนุญาต เช่น จำกัดสิทธิการ print รายงานข้อมูลประวัติผู้ป่วย,กำหนดเครื่องพิมพ์ใบเสร็จ เป็นต้น
7. กำหนดให้มีการติดตั้งโปรแกรมเพื่อป้องกันและปกป้องข้อมูลจากไวรัส มัลแวร์ โทรจัน หนอนคอมพิวเตอร์ และตรวจสอบให้มีการ update อัตโนมัติ
8. กำหนดให้มีการปิดระบบเพื่อป้องกันการใช้อุปกรณ์พกพา เช่น Hard disk External, USB Flash drive
9. สำรวจสายไฟในหน่วยงานไม่ให้ชำรุดสามารถใช้งานได้อย่างปลอดภัย เพื่อป้องกันอัคคีภัย
10. การจำลองเหตุการณ์ ร่วมซ้อมแผนภาวะฉุกเฉินของโรงพยาบาลและเตรียมความพร้อมเมื่อเกิดเหตุการณ์ฉุกเฉิน และมีเหตุจำเป็นต้องขนย้ายเครื่อง Server
11. จัดให้มีอุปกรณ์ดับเพลิง และมีการตรวจสอบให้ใช้งานได้อย่างมีประสิทธิภาพเพื่อป้องกันหรือบรรเทาความเสียหายทางกายภาพที่อาจเกิดขึ้นของเวชระเบียน
12. ห้องจัดเก็บ Server ปรับปรุงมาตรฐานเทคโนโลยีสารสนเทศ ของโรงพยาบาล โดยจัดเก็บ Server ไว้ในตู้ Rack สำหรับขนย้าย ภายในห้องติดตั้งเครื่องปรับอากาศ 2 ตัว เพื่อสลับการทำงานทุก 6 ชั่วโมง และล็อคห้อง server เพื่อป้องกันบุคคลภายนอกเข้าไปโดยไม่ได้รับอนุญาต
13. กำหนดสิทธิรหัสผู้ใช้ username และ password สำหรับการใช้งาน server และการเข้าถึง database ข้อมูลเวชระเบียนผู้ป่วย
14. การ Backup ข้อมูลที่จัดเก็บในรูปแบบ Electronic files ดังนี้
    - ทำ Raid 1 ที่เครื่อง Server ทั้ง Master และ Slave
    - ติดตั้งเครื่อง Server อีกเครื่องให้ทำงานเป็น Replicate Server และควรอยู่คนละที่กันกับ Server หลัก พร้อมตรวจสอบข้อมูลอยู่เสมอ
    - สำรองข้อมูลแบบ Full วันละ 1 ครั้งเวลา 20.15 น. และแบบ Skip log/Image เวลา 12.00 น. ของวันทำการ พร้อมทดสอบการนำข้อมูลสำรองกลับมาเดือนละ 1 ครั้ง
    - จัดเก็บข้อมูลที่สำรองไว้แบบ Full ใน Hard disk External ขนาด 1 TB สัปดาห์ละ 1 ครั้ง และเก็บข้อมูล Back up ของทุกวันย้อนหลัง 3 เดือน หลังจากเดือนที่ 3 ไปแล้วจะเก็บข้อมูล Back up ทุกวันที่ 1 ของเดือน