

| | | |
|--|--|--|
| โรงพยาบาลกระสัง | | จำนวนหน้า : ๒ |
| นโยบายและวิธีปฏิบัติ KSH-IM-๐๒๔ | | ฉบับที่ ๑ |
| เรื่อง : แนวทางปฏิบัติด้านความปลอดภัยของข้อมูลผู้ป่วยทั่วไปสำหรับโรงพยาบาล | | วันที่ ๑๖ ตุลาคม ๒๕๖๐ |
| แผนก : เทคโนโลยีสารสนเทศ | แผนกที่เกี่ยวข้อง : จนท.รพ.ที่เกี่ยวข้อง | วันที่ปรับปรุง : ๑ ตุลาคม ๒๕๖๒ |
| ผู้จัดทำ :: เทคโนโลยีสารสนเทศ | | ผู้อนุมัติ (นายโสมนัส โกยสวัสดิ์) นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง นายแพทย์เชี่ยวชาญ ผู้อำนวยการโรงพยาบาลกระสัง |

แนวทางปฏิบัติด้านความปลอดภัยของข้อมูลผู้ป่วยทั่วไปสำหรับโรงพยาบาล

วัตถุประสงค์

- ๑. เพื่อใช้เป็นแนวทางรักษาความปลอดภัยของข้อมูลผู้ป่วยทั่วไปสำหรับเจ้าหน้าที่ทุก
- ๒. เพื่อให้สามารถปฏิบัติเป็นแนวทางเดียว

ขอบเขต

ระเบียบนี้ใช้ในการรักษาความปลอดภัยของข้อมูลผู้ป่วยทั่วไปสำหรับเจ้าหน้าที่ทุกคนของโรงพยาบาลกระสัง

วิธีปฏิบัติ

- ๑. เจ้าหน้าที่ทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของมุลตลอดจนเอกสารเวชระเบียนของผู้ป่วย
- ๒. ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วย ในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการผู้อำนวยการ
- ๓. การแก้ไขข้อมูลผู้ป่วย ให้ดำเนินการได้ตามระเบียบปฏิบัติว่าด้วยการแก้ไขข้อมูลโดยเคร่งครัด เช่น หากเขียนผิดห้ามใช้ปากกากระบายสีที่ทับข้อความจนไม่เห็นข้อความเดิม ห้ามใช้น้ำยาลบคำผิดในเวชระเบียนผู้ป่วย การแก้ไขทำได้โดยการลากเส้นทับข้อความเดิมเพียงเส้นเดียว แล้ว เขียนข้อความที่แก้ไขไว้ใกล้กับผู้ป่วย การแก้ไขทำได้โดยการลากเส้นทับข้อความเพียงเส้นเดียว แล้ว เขียนข้อความที่แก้ไขไว้ใกล้กับข้อความเดิม พร้อมลงนามกำกับ และวันเวลาที่แก้ไข สำหรับการแก้ไขข้อมูลในระบบคอมพิวเตอร์ ห้ามลบข้อมูลเดิมทิ้ง แต่ให้ทำเครื่องหมายว่ามีการแก้ไขแล้ว เชื่อมโยงข้อมูลที่เพิ่มเติมแก้ไขให้รู้ว่าข้อความใหม่ใช้แทนข้อความเดิมอย่างไร
- ๔. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกัน ให้ดำเนินการตามระเบียบการส่งข้อมูลลับโดยเคร่งครัด เช่น ไม่ใช่ให้ผู้ป่วยเป็นผู้ถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุดอื่นๆ
- ๕. ห้ามส่งข้อมูลผู้ป่วยโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ส่งทาง LINE หรือ Social Media

๖. ตั้งรหัสผ่านในการเข้าระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยาก ตรงตามระเบียบของสถานพยาบาล ปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัด ไม่อนุญาตให้ผู้อื่นนำรหัสผ่าน ของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
๗. ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอกทุกกรณี สำหรับการเปิดไฟล์งานจากหน่วยงานภายในให้ตรวจหาไวรัสภายในไฟล์ทุกครั้งก่อนเปิดไฟล์
๘. ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูลเช่น CD-ROM ,USB Drive External Hard Disk อุปกรณ์เครือข่าย เช่น Hub, Switch, Wi-Fi Router ฯลฯ
๙. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเทอร์เน็ต ทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเทอร์เน็ตพร้อมกัน กับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ
๑๐. ห้ามใช้ Line Social media ขณะให้บริการผู้ป่วย ยกเว้นเพื่อการรักษา
๑๑. ระยะเวลาในการเปลี่ยนรหัสผ่าน ๑๕ วัน และไม่ใช้รหัสเดิมใน ๙๐ วัน