



ประกาศ โรงพยาบาลสมเด็จพระยุพราชบ้านดุง

เรื่อง ประกาศระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านโพธิ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ และเพื่อการปฏิบัติที่เคารพสิทธิผู้ป่วยโรงพยาบาลบ้านโพธิ์ จึงเห็นสมควรกำหนดนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ดังนี้

๑.นโยบายการรักษาความปลอดภัยในระบบ HIS (Hospital Information System)

- ๑.๑ ห้ามบุคคลภายนอกหรือผู้ที่ไม่มีความเกี่ยวข้อง ใช้งานในระบบ HIS
- ๑.๒ ห้ามไม่ให้ดูประวัติของผู้ป่วย นอกจากเป็นประวัติผู้ป่วยที่อยู่ในความรับผิดชอบและกำลังทำการรักษาอยู่เท่านั้น ยกเว้น กรณีต้องติดตามประวัติผู้ป่วยเพื่อการดูแลต่อเนื่อง หรืออื่น ๆ เพื่อเกิดประโยชน์แก่การรักษาพยาบาลผู้ป่วย
- ๑.๓ ตั้งรหัสผ่านในการใช้งานระบบ HIS ให้คาดเดาได้ยาก ปกปิดรหัสผ่านเป็นส่วนตัว ไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
- ๑.๔ ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาใช้กับคอมพิวเตอร์ในระบบ HIS นอกจากได้รับอนุญาตจากงานคอมพิวเตอร์
- ๑.๕ ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรือปรับเปลี่ยนหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ในระบบ HIS
- ๑.๖ ห้ามมิให้เปิดเผยประวัติผู้ป่วยกับผู้อื่น ในกรณีไม่มีหนังสือลายลักษณ์อักษร มาแสดง
- ๑.๗ มีการจำกัดการเข้าถึงข้อมูลที่เป็นความลับ เช่น ประวัติผู้ป่วย ให้เข้าถึงได้เฉพาะที่ตนเองได้รับอนุญาตตามหน้าที่ปฏิบัติและความเหมาะสมเท่านั้น
- ๑.๘ ห้ามแก้ไข/ดัดแปลง ประวัติผู้ป่วยจากความเป็นจริง นอกจากมีลายลักษณ์อักษร ยินยอมหรืออยู่ในความรับผิดชอบเจ้าหน้าที่ที่เกี่ยวข้อง
- ๑.๙ ห้ามใช้คอมพิวเตอร์ที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเทอร์เน็ตทุกกรณี ยกเว้น เครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเทอร์เน็ต ซึ่งได้รับอนุญาตจากผู้อำนวยการ
- ๑.๑๐ หลังจากใช้งานระบบ HIS เสร็จแล้ว ให้ออกจากระบบหรือเปลี่ยนผู้ใช้งาน

๑.๑๑ จัดตำแหน่งที่ตั้งจอภาพ และเครื่องพิมพ์ ให้อยู่ในตำแหน่งที่ผู้ป่วยหรือญาติไม่สามารถมองเห็นหรือเข้าถึงได้

๒.นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๒.๑ ห้ามนำอุปกรณ์ Wireless มาติดตั้ง หรือเปิดใช้งานเองภายในโรงพยาบาล โดยไม่ได้รับอนุญาต

๒.๒ ห้ามให้ Username และ Password แก่ผู้อื่น ต้องรักษาเป็นความลับ

๒.๓ ห้ามเคลื่อนย้ายอุปกรณ์ Wireless Lan โดยไม่ได้รับอนุญาต

๓.นโยบายการใช้สื่อสังคมออนไลน์ (Social Media)

๓.๑ ขอให้สมาชิกกลุ่มไลน์ต่าง ๆ ห้ามมิให้แสดงข้อความ รูปภาพที่ไม่เหมาะสม ส่อไปในทางลามก อนาจาร การปลุกเร้าให้เกิดการแตกแยก การทำลายสถาบันต่าง ๆ หรือเอกสารที่สามารถระบุตัวตนผู้ป่วยก่อน แสดงถึงการเปิดเผยความลับของผู้ป่วย

๓.๒ ขอให้สมาชิกกลุ่มไลน์ต่าง ๆ ห้ามมิให้แสดงรูปภาพ ชื่อ ที่อยู่ ที่จะนำไปสู่การระบุตัวตนผู้ป่วยอย่างชัดเจน หากกระทำเพื่อประโยชน์ทางการรักษาพยาบาล ควรปกปิดใบหน้าและควรขออนุญาตผู้ป่วยก่อน เมื่อดำเนินการเสร็จสิ้นต้องลบภาพนั้นทันที

๔.นโยบายการใช้อินเทอร์เน็ต

๔.๑ ห้ามเข้าเว็บไซต์ ลามก อนาจาร สิ่งผิดกฎหมาย ผิดศีลธรรม จริยธรรม การวิพากษ์วิจารณ์ ขาด ศาสนา และพระมหากษัตริย์

๔.๒ ห้ามเข้าเว็บไซต์ เล่นเกมส์ ดูภาพยนตร์ ฟังเพลง ในขณะที่ปฏิบัติงาน หรือกำลังให้บริการผู้ป่วย

๔.๓ ห้ามดาวน์โหลดหรือส่ง กระจาย แจกจ่าย ข้อมูลลามก อนาจาร ข้อมูลส่วนบุคคล สื่อสิ่งพิมพ์ ซึ่งเป็นการละเมิดสิทธิทางปัญญา

๔.๔ ห้ามกระทำการใดๆ ซึ่งขัดต่อ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.

๒๕๕๐

๕.นโยบายการป้องกันโปรแกรมไม่พึงประสงค์

๕.๑ ห้ามนำโปรแกรมใด ๆ มาติดตั้งภายในเครื่องคอมพิวเตอร์ หากต้องการติดตั้งเนื่องจากมีผลกับการปฏิบัติราชการต้องติดต่อกับงานคอมพิวเตอร์

๖.นโยบายการป้องกันไวรัส บนเครื่องคอมพิวเตอร์

๖.๑ ห้ามใช้ USB Port กับเครื่องในระบบเครือข่าย HIS

๖.๒ ห้ามดาวน์โหลด หรือติดตั้งโปรแกรมใด ๆ โดยไม่ได้รับอนุญาต

๖.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับและส่งข้อมูลทุกครั้ง

๗.นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- ๗.๑ ห้ามจด หรือบันทึก Username และ Password ไว้ในสิ่งง่ายต่อการสังเกต เช่น ที่โต๊ะทำงาน,บนหน้าจอ,แป้นพิมพ์ หรือ ไวท์บอร์ด ควรเก็บเป็นความลับ หรือจดไว้ในสมุดที่เก็บในลิ้นชักส่วนตัว
- ๗.๒ กรณีที่จำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนเพื่อประโยชน์ในการรักษาพยาบาล หลังจากทำงานเสร็จแล้ว ให้ทำการเปลี่ยนรหัสผ่านทันที
- ๗.๓ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ อย่างน้อย ๑๕ นาที
- ๗.๔ ผู้ใช้งานต้องสำรองข้อมูล (Backup) ที่สำคัญทุกวัน จากเครื่องคอมพิวเตอร์ไปไว้บนสื่อบันทึกอื่นๆเช่น Cloud (Google drive,Dropbox,One drive) หรือNetwork drive ของโรงพยาบาล เป็นต้น
- ๗.๕ เครื่องคอมพิวเตอร์ทุกเครื่องที่ทำการเปลี่ยนทดแทน หรือต้องจำหน่ายด้วยกระบวนการทางพัสดุ ให้ดำเนินการทำลายข้อมูลที่อยู่ในฮาร์ดดิสก์ ด้านวิธีการเปลี่ยนโครงสร้างทางกระบวนการทางพัสดุ ให้ดำเนินการทำลายข้อมูลที่อยู่ในฮาร์ดดิสก์มาตรฐาน DOD ๕๒๒๐.๒๒ M ด้านวิธีการเปลี่ยนโครงสร้างทางกายภาพก่อนส่งไปงานพัสดุ

๘.นโยบายการป้องกันทรัพย์สินทางคอมพิวเตอร์

- ๘.๑ ห้ามเคลื่อนย้ายคอมพิวเตอร์ เครื่องพิมพ์ อุปกรณ์ต่อพ่วงต่าง ๆ โดยไม่ได้รับอนุญาตจากงานคอมพิวเตอร์
- ๘.๒ ห้ามนำวัสดุ หรือ ครุภัณฑ์คอมพิวเตอร์ ออกนอกโรงพยาบาลโดยไม่ได้รับอนุญาตจากงานคอมพิวเตอร์ หรือกระบวนการทางพัสดุ
- ๘.๓ ห้ามมิให้บุคคลภายนอกใช้วัสดุและครุภัณฑ์คอมพิวเตอร์ นอกเหนือจากที่ได้จัดสถานที่ไว้บริการ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรการด้านความปลอดภัยในการใช้งานระบบสารสนเทศของโรงพยาบาล ซึ่งเจ้าหน้าที่ของโรงพยาบาลบ้านโพธิ์ จะต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๑ พฤษภาคม ๒๕๖๖

(นายวันชัย ศรีพุท)

นายแพทย์ชำนาญการ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลบ้านโพธิ์