ประกาศโรงพยาบาลนาเยีย

เรื่อง นโยบายหลักด้านการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ

ด้วย กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ โรงพยาบาลนาเยีย มีหน้าที่ในการกำกับดูแลการใช้งานในระบบคอมพิวเตอร์ระบบเครือข่าย และระบบสารสนเทศพบว่าบางส่วนมีการใช้งานผิดประเภททำให้อาจเกิดความเสียหายในหน่วยงานดังนั้น เพื่อให้การปฏิบัติเป็นไปในทิศทางเดียวกัน จึงได้กำหนดนโยบายหลักเพื่อประกอบการควบคุมดังนี้

๑. นโยบายการรักษาความมั่นคงในระบบ HIWIN

๑.๑ ห้ามบุคคลภายนอกหรือผู้ไม่มีหน้าที่เกี่ยวข้อง เข้าใช้งานระบบ HIWIN

๑.๒ ห้ามไม่ให้เปิดดูประวัติของผู้ป่วย นอกจากเป็นประวัติผู้ป่วยในความรับผิดชอบและกำลังทำการรักษาอยู่เท่านั้นยกเว้น กรณีต้องติดตามประวัติผู้ป่วยเพื่อการดูแลรักษาต่อเนื่องหรืออื่นๆ เพื่อให้เกิดประโยชน์แก่การรักษาพยาบาลผู้ป่วย

๑.๓ ตั้งรหัสผ่านในการเข้าใช้งานระบบ HIWIN ให้คาดเดาได้ยาก ปกปิดรหัสผ่านเป็นความลับส่วนตัว ไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงเวลาบังคับ ทุกๆ ๓๐ วัน

๑.๔ ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาใช้กับเครื่องคอมพิวเตอร์ในระบบ HIWIN นอกจากได้รับการอนุญาตจากงานเทคโนโลยีสารสนเทศทางการแพทย์

๑.๕ ห้ามเคลื่อนย้ายคอมพิวเตอร์ หรือปรับเปลี่ยนหมายเลขไอพี (IP ADDRESS) ของเครื่องคอมพิวเตอร์ในระบบ HIWIN

๑.๖ ห้ามมิให้เปิดเผยประวัติผู้ป่วยแก่ผู้อื่น ในกรณีไม่มีหนังสือ แบบคำขอเข้าถึงเวชระเบียน-โรงพยาบาลนาเยีย มาแสดง

๑.๗ มีการจำกัดการเข้าถึงข้อมูลที่เป็นความลับเช่น ประวัติผู้ป่วย ให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตตามหน้าที่ที่ปฏิบัติ และความเหมาะสมเท่านั้น

๑.๘ ห้ามแก้ไข/ดัดแปลง ประวัติผู้ป่วยจากความเป็นจริง นอกจากมีลายลักษณ์อักษร ยินยอม หรืออยู่ในความรับผิดชอบเจ้าหน้าที่ที่เกี่ยวข้อง

๑.๙ ห้ามใช้คอมพิวเตอร์ที่เชื่อมกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเตอร์เน็ตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่เชื่อมต่ออินเตอร์เน็ต ซึ่งได้รับอนุญาตจากผู้อำนวยการ

๑.๑๐ กำหนดให้คอมพิวเตอร์ระบบ HIWIN มีการตัดและหมดระยะเวลาการใช้งานรวมทั้งปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๕ นาที

๑.๑๑ ตำแหน่งที่ตั้งจอภาพ และเครื่องพิมพ์ให้อยู่ในตำแหน่งผู้ป่วย หรือญาติไม่สามารถมองเห็นหรือเข้าถึงได้

๒. นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๒.๑ ห้ามนำอุปกรณ์ Wireless มาติดตั้ง หรือเปิดใช้งานเองในโรงพยาบาล โดยไม่ได้รับอนุญาต

๒.๒ ห้ามให้ User และ Password แก้ผู้อื่น ต้องรักษาเป็นความลับ

๒.๓ ห้ามเคลื่อนย้ายอุปกรณ์ Wireless LAN โดยไม่ได้รับอนุญาต

๓. นโยบายการใช้สื่อสังคมออนไลน์

๓.๑ ขอให้สมาชิกกลุ่มไลน์ต่างๆห้ามมิให้แสดงข้อความ รูปภาพที่ไม่เหมาะสม ส่อไปในทางลามก อนาจารการปลุกเร้าให้เกิดความแตกแยก การทำลายสถาบันต่างๆ หรือเอกสารที่สามารถระบุตัวตนผู้ป่วย แสดงถึงการเปิดความลับผู้ป่วย

๓.๒ ขอให้สมาชิกกลุ่มไลน์ต่างๆ ห้ามมิให้แสดงรูปภาพ ชื่อ ที่อยู่ ที่จะนำไประบุตัวตนผู้ป่วยอย่างชัดเจน หากกระทำเพื่อประโยชน์ทางการรักษาพยาบาล ควรปกปิดใบหน้า และควรขออนุญาตผู้ป่วยก่อนเมื่อดำเนินการเสร็จสิ้นต้องลบภาพภายใน ๓๐ นาที

๓.๓ ห้ามใช้โปรแกรม Line ใช้ในการสื่อสารการรักษาพยาบาล ยกเว้นเพื่อประโยชน์ในการรักษาผู้ป่วย เมื่อดำเนินการเสร็จต้องลบข้อความหรือรูปภาพ ภายใน ๓๐ นาที ทั้งผู้ส่งและผู้รับ

๔. นโยบายการใช้อินเตอร์เน็ต

๔.๑ ห้ามเข้าเว็บไซต์ลามก อนาจารสิ่งผิดกฎหมาย ผิดศีลธรรม จริยธรรม การวิพากษ์วิจารณ์ชาติ ศาสนา พระมหากษัตริย์

๔.๒ ห้ามเข้าเว็บไซต์ เล่นเกมส์ ดูภาพยนตร์ ฟังเพลง ในขณะปฏิบัติงาน หรือกำลังให้บริการผู้ป่ว

๔.๓ ห้ามดาวน์โหลดหรือส่งกระจายแจกจ่ายข้อมูลลามกอนาจารข้อมูลส่วนบุคคลสื่อสิ่งพิมพ์ซึ่งเป็นการละเมิดลิขสิทธิ์ทางปัญญา

๔.๔ ห้ามกระทำการใดๆ ขัดต่อ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐

๕. นโยบายการป้องกันโปรแกรมไม่พึงประสงค์

๕.๑ ห้ามนำโปรแกรมใดๆ มาติดตั้งภายในเครื่องคอมพิวเตอร์ หากต้องการติดตั้งเนื่องจากมีผลปฏิบัติกับทางราชการต้องติดต่อผ่านงานเทคโนโลยีสารสนเทศทางการแพทย์

๖. การโยบายการป้องกันไวรัส

๖.๑ห้ามใช้อุปกรณ์จัดเก็บข้อมูลเชื่อมต่อ USB Port กับเครื่องในระบบเครือข่าย HIWIN

๖.๒ ห้ามดาวน์โหลดหรือติดตั้งโปรแกรมใดๆ โดยไม่ได้รับอนุญาต

๖.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านอินเตอร์เน็ต จะต้องมีการตรวจสอบไวรัส โดยใช้โปรแกรมป้องกันไวรัสการรับและส่งข้อมูลทุกครั้ง

๗. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๑ ห้ามจดหรือบันทึกUser และ Password ไว้ในที่ง่ายต่อการสังเกตเห็น เช่น ที่โต๊ะทำงาน บนหน้าจอ, Clear Desk, Clear Screen Policy) แป้นพิมพ์ หรือ ไวท์บอร์ด ควรเก็บเป็นความลับหรือจดไว้ในสมุดที่เก็บในลิ้นชักส่วนตัว

๗.๒ กรณีจำเป็นที่ต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนเพื่อประโยชน์ในการรักษาพยาบาลหลักจากทำงานเสร็จแล้วให้เปลี่ยนรหัสผ่านทันที

๗.๓ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

๗.๔ ผู้ใช้งานต้องสำรองข้อมูล (backup) ที่สำคัญทุกวัน จากเครื่องคอมพิวเตอร์ ไว้บนสื่อบันทึกอื่นๆ เช่น Flash Drive หรือ External Harddisk เป็นต้น

๗.๕ เครื่องคอมพิวเตอร์ทุกเครื่องที่ต้องทำการเปลี่ยนทดแทนหรือต้องจำหน่ายด้วยกระบวนการทางพัสดุ ให้ดำเนินการทำลายข้อมูลที่อยู่ในฮาร์ดดิสก์ ด้วยวิธีการเปลี่ยนโครงสร้างทางการภาพ (Fdisk) ของฮาร์ดดิสก์ก่อนส่งไปงานพัสดุ

๘. นโยบายการป้องกันทรัพย์สินทางคอมพิวเตอร์

๘.๑ ห้ามเคลื่อนย้ายคอมพิวเตอร์เครื่องพิมพ์อุปกรณ์ต่อพ่วงต่างๆโดยไม่ได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศทางการแพทย์

๘.๒ ห้ามนำวัสดุหรือครุภัณฑ์ทางคอมพิวเตอร์ออกนอกโรงพยาบาลโดยไม่ได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศทางการแพทย์ หรืองานพัสดุ

๘.๓ ห้ามมิให้บุคคลภายนอกใช้วัสดุหรือครุภัณฑ์คอมพิวเตอร์นอกเหนือจากที่ได้จัดสถานที่ให้บริการ เช่น การจัดการประชุม

๙. นโยบายการเข้าถึงข้อมูลระยะไกลผ่านอินเตอร์เน็ต(remote access service)

๙.๑ ห้ามมิให้บุคคลภายนอก หรือผู้ไม่มีส่วนเกี่ยวข้องทำการติดตั้งโปรแกรมรีโมทควบคุมเครื่อง

๙.๒ กำหนดให้ผู้รับผิดชอบงานระบบสารสนเทศ คือ นักวิชาการคอมพิวเตอร์ เป็นผู้ได้รับอนุญาตรีโมทเข้ามาแก้ไขข้อผิดพลาดของระบบแม่ข่าย ลูกข่ายและฐานข้อมูลแก้ไขกรณีเกิดปัญหาระบบเท่านั้น

๑๐. นโยบายความปลอดภัยของห้องแม่ข่ายคอมพิวเตอร์

๑๐.๑ ต้องปิดล๊อกประตูห้องแม่ข่ายคอมพิวเตอร์ตลอดเวลา

๑๐.๒ การเข้า-ออก ต้องมีการลงลายมือชื่อ ภารกิจ และเก็บบันทึกการตรวจสอบไว้เป็นหลักฐาน

๑๐.๓ กรณีบุคคลภายนอกมีความจำเป็นต้องเข้าออกพื้นที่ฯ จะต้องมีเจ้าหน้าที่คอยควบคุมติดตามอยู่ด้วยตลอดเวลา และหากต้องการ Access อุปกรณ์ใดจะต้องได้รับอนุญาตจากเจ้าของระบบหรือผู้มีสิทธิ์อนุญาต

นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ จัดเป็นมาตรการด้านความปลอดภัยในการใช้งานระบบสารสนเทศของโรงพยาบาล ซึ่งเจ้าหน้าที่ของโรงพยาบาลนาเยีย จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ เดือน ตุลาคม พ.ศ. ๒๕๖๒

(นายลิต แสงแก้ว)
นายแพทย์ชำนาญการพิเศษ
ผู้อำนวยการโรงพยาบาลนาเยีย