บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ โรงพยาบาลมหาสารคาม โทร ๒๗๐ ,๒๗๑

ที่ มค ๐๐๓๒.๒๐๒/๙๑ **วันที่** ๑๒ มิถุนายน ๒๕๖๒

เรื่อง ประกาศนโยบายและระเบียบปฏิบัติทั่วไปด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เรียน ผู้อำนวยการโรงพยาบาลมหาสารคาม

สืบเนื่องจากมาตรฐานความมั่นคงปลอดภัยของข้อมูลผู้ป่วย พ.ศ. ๒๕๕๙ ของสำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Privacy) ดังกล่าวไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ กำหนดให้สถานพยาบาลควรมีแนวทางปฏิบัติเกี่ยวกับการเก็บรวบรวมการใช้และการเปิดเผยข้อมูลข่าวสารส่วนบุคคลด้านสุขภาพที่สอดคล้องกับกฎหมายต่างๆและสื่อสารให้บุคคลทราบทั่วกัน

ดังนั้น ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ จึงได้ประกาศนโยบายและระเบียบปฏิบัติทั่วไปด้านการรักษาความมั่นคงของระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับบุคลากรที่มีโอกาสเข้าถึงข้อมูลผู้ป่วยเพื่อให้บุคลากรทุกคนถือปฏิบัติ ซึ่งได้ดำเนินการประกาศไปแล้ว ณ วันที่ ๑๔ สิงหาคม ๒๕๖๑ และได้มีการปรับปรุงแก้ไขและเพิ่มเติมบางข้อเพื่อให้ครอบคลุมในทุกด้านและให้ถือปฏิบัติอย่างเคร่งครัด

จึงเรียนมาเพื่อโปรดพิจารณาลงนามตามประกาศที่แนบมาพร้อมหนังสือนี้

(นางสาวกาญจนาภรณ์ ตาราไต)
เภสัชกรชำนาญการ
หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

(นางสุภาภรณ์ คณะเวทย์)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
รักษาการในตำแหน่ง รองผู้อำนวยการฝ่ายบริหาร

-เรียน ผอ.รพ.มค.
เพื่อโปรดพิจารณาลงนาม

(นายสุนทร ยนต์ตระกูล)

นายสุนทร ยนต์ตระกูล
ผู้อำนวยการโรงพยาบาลมหาสารคาม
16 มิ.ย. 2562

ประกาศโรงพยาบาลมหาสารคาม

เรื่อง นโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลมหาสารคามเป็นไปอย่างเหมาะสม มีประสิทธิภาพปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดจากการใช้อย่างไม่ถูกต้อง ซึ่งอาจก่อให้เกิดความเสียหายและเป็นความผิดตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นๆที่เกี่ยวข้อง ดังนั้น จึงขอประกาศนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้บุคลากรถือปฏิบัติอย่างเคร่งครัด ดังรายละเอียดต่อไปนี้

หมวดที่ ๑ คำนิยาม

โรงพยาบาล หมายถึง โรงพยาบาลมหาสารคาม

ส่วนราชการ หมายถึง กระทรวงสาธารณสุข

ผู้บังคับบัญชา หมายถึง ผู้อำนวยการหรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลมหาสารคาม

ผู้บริหารระบบเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายถึง ผู้บริหารระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม โดยมีบทบาทหน้าที่ในการกำหนดนโยบายและแนวทางปฏิบัติการใช้งานระบบเทคโนโลยีสนเทศ

หน่วยงาน หมายถึง หน่วยงานต่างๆที่อยู่ในเครือข่ายของโรงพยาบาลมหาสารคาม

ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ หมายถึง หน่วยงานที่ทำหน้าที่ให้บริการและพัฒนาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม

หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ หมายถึง หัวหน้าที่ทำหน้าที่ดูแล บริหารจัดการศูนย์เทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม

ผู้ดูแลระบบ (System Administrator) หมายถึง บุคลากรที่ได้รับมอบหมายจาก CIO หรือหัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ ให้มีหน้าที่รับผิดชอบในการดูแลและเข้าถึงระบบคอมพิวเตอร์เครือข่ายของโรงพยาบาลมหาสารคาม

เครื่องคอมพิวเตอร์เครือข่าย หมายถึง ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาล ทั้งที่อยู่ภายในโรงพยาบาล และเครือข่ายโรงพยาบาลมหาสารคาม รวมทั้งอุปกรณ์ต่อพ่วงต่างๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่างๆ ตลอดจนโปรแกรมและข้อมูลต่างๆที่มิได้จัดให้เป็นสื่อสาธารณะ

ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานกระทรวงสาธารณสุข ลูกจ้างชั่วคราวของโรงพยาบาลมหาสารคาม หรือผู้ที่โรงพยาบาลมหาสารคามอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และเครือข่ายได้

นโยบายด้านความมั่นคงปลอดภัย คือ แนวทางที่ผู้บริหารระดับสูงกำหนดทิศทางการดำเนินงานเพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะมีความมั่นคงปลอดภัย

ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย คือ ข้อกำหนดที่ให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตามเพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย

บทลงโทษ หมายถึง บทลงโทษที่ส่วนราชการเป็นผู้กำหนด หรือบทลงโทษตามกฎหมาย

หมวดที่ ๒ นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. โรงพยาบาลจะดำเนินการจัดการเพื่อคุ้มครองข้อมูลส่วนบุคคลอันเป็นความลับและเป็นข้อมูลส่วนตัวของผู้ป่วยอย่างเคร่งครัด

๒. การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ต้องเป็นไปเพื่อดำเนินกิจกรรมตามพันธกิจเพื่อให้บรรลุวิสัยทัศน์ของโรงพยาบาล

หมวดที่ ๓ ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นพื้นที่ควบคุม โดยกำหนดเฉพาะผู้ที่ใช้งานที่ได้รับอนุญาตให้เข้าปฏิบัติให้เข้าปฏิบัติงานในพื้นที่ควบคุม

๒. ผู้ดูแลระบบเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ห้ามบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าใช้งาน หากมีหน่วยงานภายนอกต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายมาใช้งานในพื้นที่ควบคุมจะต้องลงบันทึกขออนุญาตใช้งานจาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

๓. ห้ามผู้ใช้งานทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หากจำเป็นให้ประสานศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

หมวดที่ ๔ ระเบียบปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. ผู้ดูแลระบบต้องเป็นผู้กำหนดสิทธิในการเข้าถึงระบบข้อมูลต่างๆให้เหมาะสมกับการใช้งานของผู้ใช้งานโดยทำการลงทะเบียนการใช้งานและทำการเก็บประวัติการเข้าถึงข้อมูลและข้อมูลจราจรทางคอมพิวเตอร์

๒. ผู้ดูแลระบบ เป็นผู้ทำหน้าที่บริหารจัดการและทำการตรวจสอบเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เครือข่ายทั้งภายในและภายนอก โดยมีการแสดงตัวตน (User Authentication) ของผู้ใช้งาน

๓. ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (User Authentication) และรหัสผ่าน (Password) ไว้เป็นความลับ ห้ามปิดประกาศไว้ในที่เปิดเผยหรือมอบให้ผู้อื่นใช้งานแทนและต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน

หมวดที่ ๕ ระเบียบปฏิบัติด้านความปลอดภัยและระบบคอมพิวเตอร์เครือข่ายและเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องทำการควบคุมตรวจสอบ และจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ตามแนวทางปฏิบัติ เพื่อให้เกิดความปลอดภัย และสามารถระบุถึงตัวบุคคลได้

๒. หากมีบุคคลภายนอกต้องการสิทธิในการเข้าถึงระบบคอมพิวเตอร์เครือข่าย จะต้องทำบันทึกเพื่อขออนุญาตเข้าใช้จาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

๓. ผู้ดูแลระบบ เป็นผู้ติดตั้งและวาง Access point ในตำแหน่งที่เหมาะสมและกำหนดรหัสผ่านและสิทธิผู้ใช้งาน ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองโดยไม่ได้รับอนุญาต

หมวดที่ ๖ ระเบียบปฏิบัติใช้เครื่องคอมพิวเตอร์และคอมพิวเตอร์พกพา

๑. กำหนดให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดเป็นสมบัติของโรงพยาบาล และมอบให้ผู้ใช้งานสามารถใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายได้ตามหน้าที่รับผิดชอบที่กำหนดจากผู้ดูแลระบบ และห้ามผู้ใช้งานติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๒. ห้ามผู้ใช้งานหรือบุคคลภายนอก นำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายด้านคอมพิวเตอร์ทุกชนิดมาเชื่อมต่อระบบเครือข่ายของโรงพยาบาลมหาสารคาม ยกเว้นทำบันทึกและได้รับอนุญาตจาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์เท่านั้น

๓. กำหนดให้ผู้ใช้งาน ต้องทำการ Scan Virus ในอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy drive) ทุกครั้งก่อนใช้งานเชื่อมต่อกับอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลมหาสารคาม

หมวดที่ ๗ ระเบียบปฏิบัติการใช้อินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑. ผู้ใช้งานต้องทำการลงทะเบียน บัญชีผู้ใช้งานเครือข่ายอินเตอร์เน็ต ที่ศูนย์เทคโนโลยีสารสนเทศ และก่อนใช้งานต้องใส่ Username และ Password เพื่อยืนยันตัวตน (Authentication) ทุกครั้ง

๒. ผู้ใช้งานต้องรับผิดชอบบัญชีผู้ใช้งาน (User Account) ของตนเอง จะโอน จำหน่าย หรือจ่ายแลกสิทธิให้กับผู้อื่นไม่ได้ หากผู้อื่นได้ใช้บัญชีผู้ใช้งานของตน ผู้ใช้งานจึงต้องเป็นผู้รับผิดชอบผลต่างๆที่อาจจะเกิดขึ้น

๓. ผู้ดูแลระบบจะต้องทำระบบรักษาความปลอดภัยของข้อมูล และสามารถเก็บประวัติการใช้งานของผู้ใช้งานเพื่อตรวจสอบและป้องกันภัยคุกคาม

๔. กรณีบุคคลภายนอก เช่น วิทยากร ผู้เข้าร่วมประชุม จำเป็นต้องใช้อินเตอร์เน็ตต้องให้หน่วยงานผู้รับผิดชอบติดต่อผู้ดูแลระบบเพื่อดำเนินการกำหนดบัญชีผู้ใช้งานและรหัสผ่านทุกครั้ง

หมวดที่ ๘ ระเบียบปฏิบัติในการรักษาความลับของผู้ป่วย

๑. ผู้ใช้งานทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูลในระบบคอมพิวเตอร์และเอกสารเวชระเบียนของผู้ป่วย

๒. ผู้ใช้งานห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ หรือ CIO

๓. การส่งข้อมูลผู้ป่วยผ่านช่องทาง Social Media ต้องปฏิบัติตามระเบียบปฏิบัติด้านการส่งข้อมูลผู้ป่วยผ่าน Social Media

๔. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเทอร์เน็ตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่อ

อินเทอร์เน็ตพร้อมกันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ หรือ CIO

๕. ห้ามมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใด เข้าถึงข้อมูลผู้ป่วยรายนั้น

หมวดที่ ๙ ระเบียบปฏิบัติด้านการส่งข้อมูลผู้ป่วย Social Media

๑. ผู้ใช้งานต้องหลีกเลี่ยงการระบุ ชื่อ, สกุล, HN, เลข ๑๓ หลัก, เตียง, ใบหน้า หรือข้อมูลที่ระบุตัวตนผู้ป่วยได้

๒. ผู้ใช้งานต้องหลีกเลี่ยงการส่งข้อมูลผู้ป่วยผ่าน Social Media แบบกลุ่ม

๓. เมื่อส่งข้อมูลผ่าน Social Media แล้ว หากใช้ข้อมูลนั้นแล้ว ให้ทำการลบออกจาก Social Media ที่ทำการส่งทันที

ประกาศ ณ วันที่ ๒๖ มิถุนายน พ.ศ. ๒๕๖๒

ลงชื่อ

นายสุนทร ยนต์ตระกูล
ผู้อำนวยการโรงพยาบาลมหาสารคาม

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

Don't 1

การใช้งาน โปรแกรมโรงพยาบาล

ห้ามบุคคลภายนอกหรือผู้ไม่เกี่ยวข้องใช้งานระบบคอมพิวเตอร์ของโรงพยาบาลและผู้ใช้ทำการ Logout ออกทุกครั้งเมื่อไม่ใช้งาน

Don't 2

เครือข่ายและการใช้งาน

ห้ามผู้ใช้งานเคลื่อนย้ายคอมพิวเตอร์ และอุปกรณ์เครือข่ายก่อนได้รับอนุญาตจากศูนย์คอมพิวเตอร์

Don't 3

การปลอดภัยของข้อมูล

ห้ามผู้ใช้งาน ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

Don't 4

การป้องกันผู้ไม่มีสิทธิใช้งาน

ห้ามมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใด เข้าถึงข้อมูลผู้ป่วยรายนั้น

Don't 5

การเชื่อมต่ออุปกรณ์

ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล ก่อนได้รับอนุญาต และลงทะเบียนกับศูนย์คอมพิวเตอร์

Don't 6

การรักษาความลับของผู้ป่วย

ห้ามผู้ใช้งาน ส่งข้อมูลผู้ป่วยผ่านสื่อ Social Mediaและต้องปฏิบัติตามระเบียบการใช้อย่างเคร่งครัด

Do 7

การป้องกันไวรัส

ผู้ใช้งานต้องทำการ Scan ไวรัสจากอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy Drive)ทุกครั้งก่อนใช้งาน

Do 8

การเก็บรักษา User& Password

ผู้ใช้งานต้องเก็บรักษาUser &Passwordไว้เป็นความลับและต้องเปลี่ยนทุก 6 เดือน