เกณฑ์การประเมินโรงพยาบาลอัจฉริยะ
ด้านความปลอดภัยและธรรมภิบาล

นพ. จารุพล ตวงศิริทรัพย์
โรงพยาบาลกาฬสินธุ์

นายราชิ ปาลือชา
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

เกณฑ์การประเมินโรงพยาบาลอัจฉริยะ : ด้านความปลอดภัย

ความปลอดภัยพื้นฐาน

60 คะแนน

- ประกาศนโยบายด้านความมั่นคงปลอดภัย
- มีระเบียบปฏิบัติด้านความมั่นคงฯ และปรับปรุง อย่างน้อย ปีละ 1 ครั้ง
- ประเมินผลการปฏิบัติตามระเบียบอย่างน้อย ปีละ 1 ครั้ง
- risk management
- มีระบบ cyber security

เทคโนโลยีด้านความปลอดภัย

30 คะแนน

- username and password
- สร้างระบบการเข้าถึงข้อมูลผู้ป่วยให้รัดกุม
- การแยกระบบ network ให้เหมาะกับความปลอดภัยทางไซเบอร์

แผนตอบโต้ด้านความปลอดภัยไซเบอร์

50 คะแนน

- Service Desk
- Service Level Agreement
- Incident &Problem Management
- สถิติการให้บริการ สถิติอุบัติการณ์ และการรายงาน
- Capacity Management
- BCP & DRP

App หรือ Software พัฒนาเอง

15 คะแนน

- การพัฒนา App ที่มีหน่วยย่อยที่นำมาใช้ใหม่ร่วมกันได้/website รพ. ต้องมี domain .moph/.go.th
- การจัดสร้าง/ต่อเติม software/website รพ. ให้เป็นไปอย่างมีประสิทธิภาพ

ธรรมาภิบาล

75 คะแนน

- Information Security Management
- Application control
- ควบคุมคุณภาพข้อมูล
- พ.ร.บ. PDPA
- ประกาศ ศทส. แนวปฏิบัติการคุ้มครองฯ
- การจัดทำ ROPA
- แต่งตั้ง DPO

คกก.พัฒนาสุขภาพดิจิทัลระดับ รพ.

10 คะแนน

คกก. ความปลอดภัยทางไซเบอร์ระดับ รพ.

10 คะแนน

250 คะแนน

4.1 ความปลอดภัยพื้นฐาน 60 คะแนน

4.1.1 ประกาศนโยบายด้านความมั่นคงปลอดภัย 10 คะแนน (จำเป็น)

4.1.2 มีระเบียบปฏิบัติด้านความมั่นคงปลอดภัย และมีการทบทวน ระเบียบและปรับปรุง อย่างน้อย ปีละ 1 ครั้ง 10 คะแนน

4.1.3 ประเมินผลการปฏิบัติตามระเบียบอย่างน้อย ปีละ 1 ครั้ง วิเคราะห์ผลการประเมินและสรุป ประเด็นที่เรียนรู้และปรับปรุงต่อไป 10 คะแนน

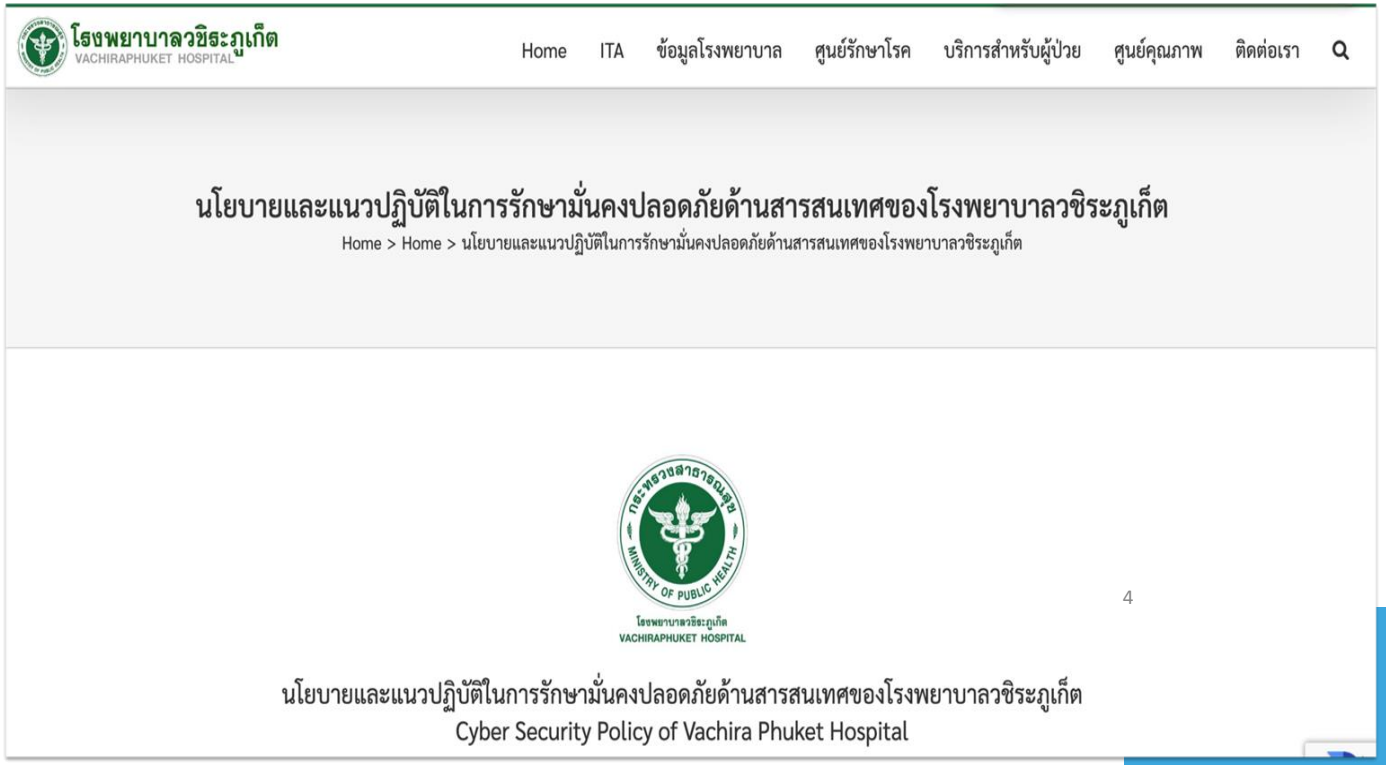
4.1.4 มีระบบบริหารความเสี่ยง (risk management) ในด้านต่าง ๆ ดังนี้ 10 คะแนน

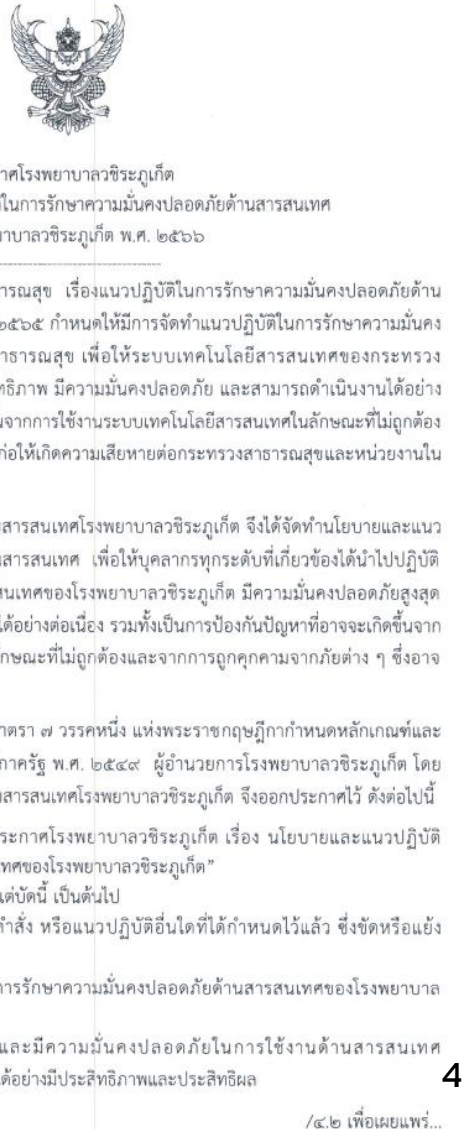
4.1.5 มีระบบความปลอดภัยป้องกันการโจมตีทางไซเบอร์ 20 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.1.4 ประกาศนโยบายด้านความมั่นคงปลอดภัย 10 คะแนน (จำเป็น)

การประกาศนโยบายในช่องทางต่างๆ เช่น ในหน้าเว็บไซด์ของหน่วยงาน หนังสือเวียน ฯลฯ





ประกาศโรงพยาบาลวชิระภูเก็ต
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลวชิระภูเก็ต พ.ศ. ๒๕๖๖

ตามประกาศกระทรวงสาธารณสุข เรื่องแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข เพื่อให้ระบบเทคโนโลยีสารสนเทศของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อกระทรวงสาธารณสุขและหน่วยงานในสังกัดนั้น

คณะกรรมการพัฒนาระบบสารสนเทศโรงพยาบาลวชิระภูเก็ต จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลวชิระภูเก็ต มีความมั่นคงปลอดภัยสูงสุดอย่างมีประสิทธิภาพ และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาล

อาศัยอำนาจตามความในมาตรา ๗ วรรคหนึ่ง แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ผู้อำนวยการโรงพยาบาลวชิระภูเก็ต โดยความเห็นชอบของคณะกรรมการพัฒนาระบบสารสนเทศโรงพยาบาลวชิระภูเก็ต จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑. ประกาศฉบับนี้เรียกว่า "ประกาศโรงพยาบาลวชิระภูเก็ต เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลวชิระภูเก็ต"

ข้อ ๒. ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลวชิระภูเก็ต มีวัตถุประสงค์ ดังต่อไปนี้

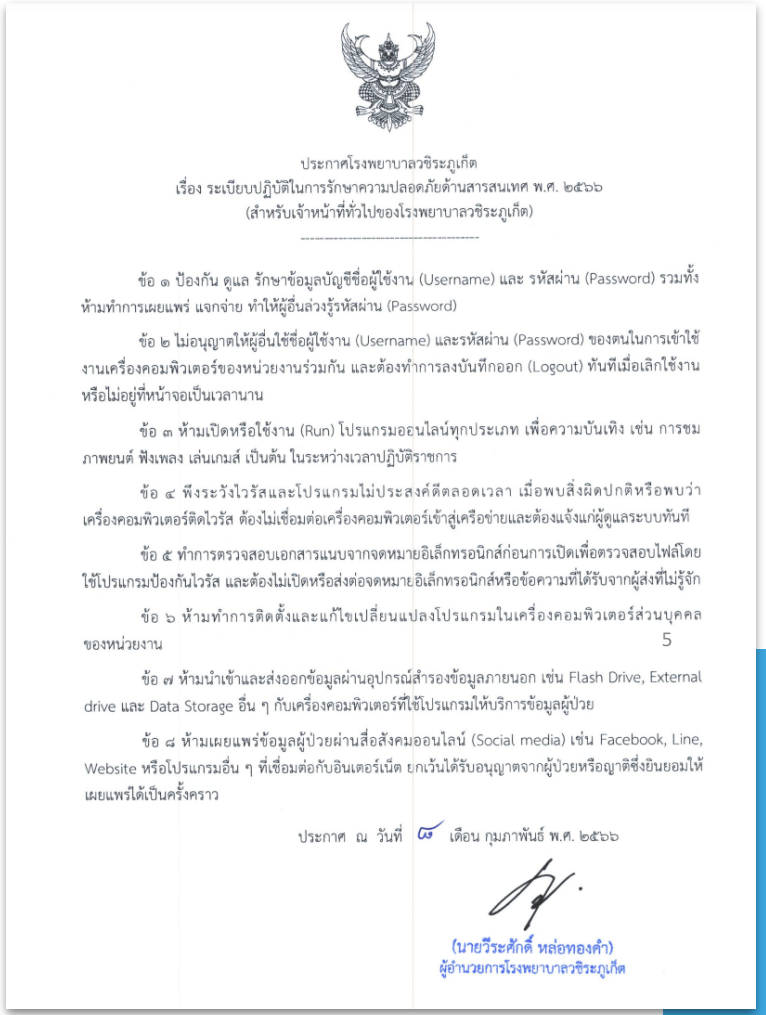
๔.๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลวชิระภูเก็ต ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

/๔.๒ เพื่อเผยแพร่...

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.1.2 ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยและมีการทบทวน ระเบียบและปรับปรุง อย่างน้อย ปีละ 1 ครั้ง 10 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน



ประกาศโรงพยาบาลวชิระภูเก็ต
เรื่อง ระเบียบปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖
(สำหรับเจ้าหน้าที่ทั่วไปของโรงพยาบาลวชิระภูเก็ต)

ข้อ ๑ ป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน และต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๓ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การชมภาพยนต์ ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๔ พึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา เมื่อพบสิ่งผิดปกติหรือพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบทันที

ข้อ ๕ ทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส และต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๖ ห้ามทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

5

ข้อ ๗ ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก เช่น Flash Drive, External drive และ Data Storage อื่น ๆ กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย

ข้อ ๘ ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social media) เช่น Facebook, Line, Website หรือโปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตจากผู้ป่วยหรือญาติซึ่งยินยอมให้เผยแพร่ได้เป็นครั้งคราว

ประกาศ ณ วันที่ ๑๗ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๖

(นายวีระศักดิ์ หล่อทองคำ)
ผู้อำนวยการโรงพยาบาลวชิระภูเก็ต

โรงพยาบาลวชิระภูเก็ต
VACHIRAPHUKET HOSPITAL

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลวชิระภูเก็ต พ.ศ. ๒๕๖๖

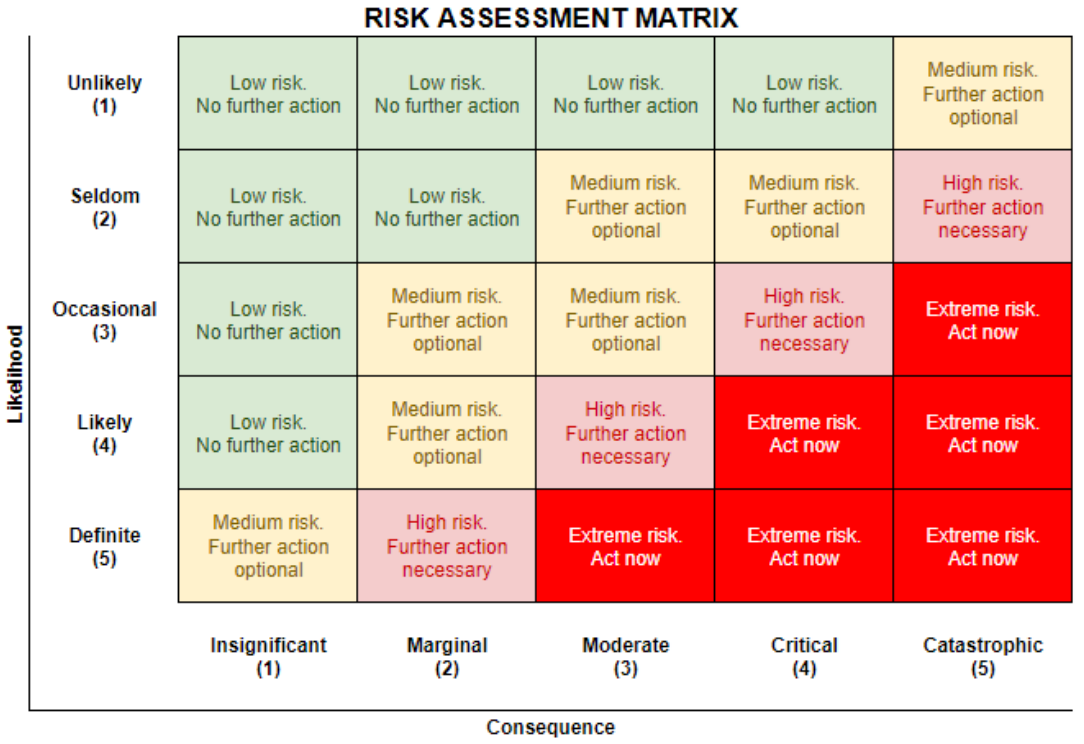
คณะกรรมการสารสนเทศโรงพยาบาลวชิระภูเก็ต

4.1.3 ประเมินผลการปฏิบัติตามระเบียบอย่างน้อยปีละ 1 ครั้ง วิเคราะห์ผลการประเมินและสรุปประเด็นที่เรียนรู้และปรับปรุงต่อไป 10 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.1.4 มีระบบบริหารความเสี่ยง (risk management) ในด้านต่าง ๆ

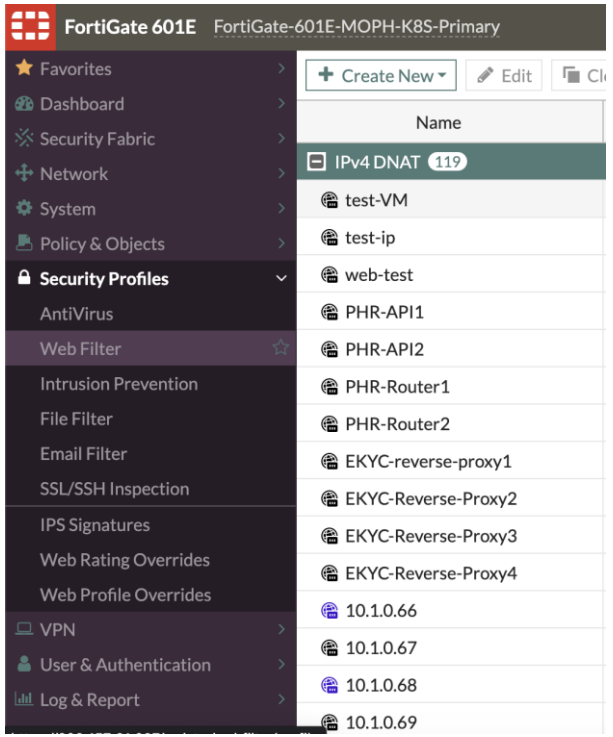
- ❑ ระบุประเด็นความเสี่ยงได้ครบ ทั้งความสี่ยงต่อระบบเทคโนโลยีสารสนเทศ และความเสี่ยงที่การใช้ เทคโนโลยีสารสนเทศจะทำให้เกิดอันตรายต่อผู้ป่วย — 4 คะแนน
- ❑ มีการทบทวนประเด็นความเสี่ยง การประเมินคะแนนความเสี่ยง อย่างน้อย ปีละ 1 ครั้ง — 2 คะแนน
- ❑ มีการจัดทำแผนกลยุทธ์ และแผนปฏิบัติการจัดการความเสี่ยงใหม่ ปีละ 1 ครั้ง — 2 คะแนน
- ❑ สามารถยกระดับการพัฒนาการจัดการความเสี่ยง ได้โดยประเมินจากความเสี่ยงทุกด้านลดลงอย่างต่อเนื่องในระยะเวลา 2-3 ปี — 2 คะแนน



มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

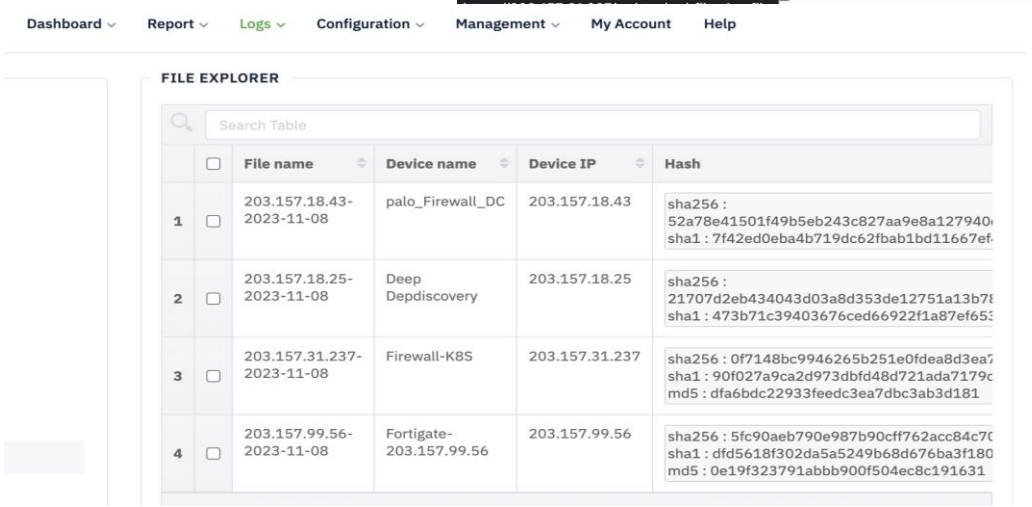
4.1.5 มีมีระบบความปลอดภัยป้องกันการโจมตีทางไซเบอร์

❑ มี Next Gen Fire wall ที่เปิด IPS และ IDS — 10 คะแนน (จำเป็น)
- ○ ชื่อ รุ่น ยี่ห้อ ของ Firewall ที่ติดตั้ง
- ○ Function IPS ที่เปิดใช้งาน
- ○ Network Diagram



❑ มี Antivirus — 5 คะแนน (จำเป็น)
- ○ ชื่อ รุ่น ยี่ห้อ ของ Antivirus

❑ มีการบันทึก Log ในการเข้าใช้งานระบบสารสนเทศโรงพยาบาลอย่างน้อย 90 วัน ตาม พรบ. Cyber crime — 5 คะแนน (จำเป็น)
- ○ จัดเก็บ Log File ของเครื่องคอมพิวเตอร์แม่ข่าย (ต้องจัดเก็บแยกออกมาจากเครื่อง)
- ○ จัดเก็บ Log File ของ Filewall



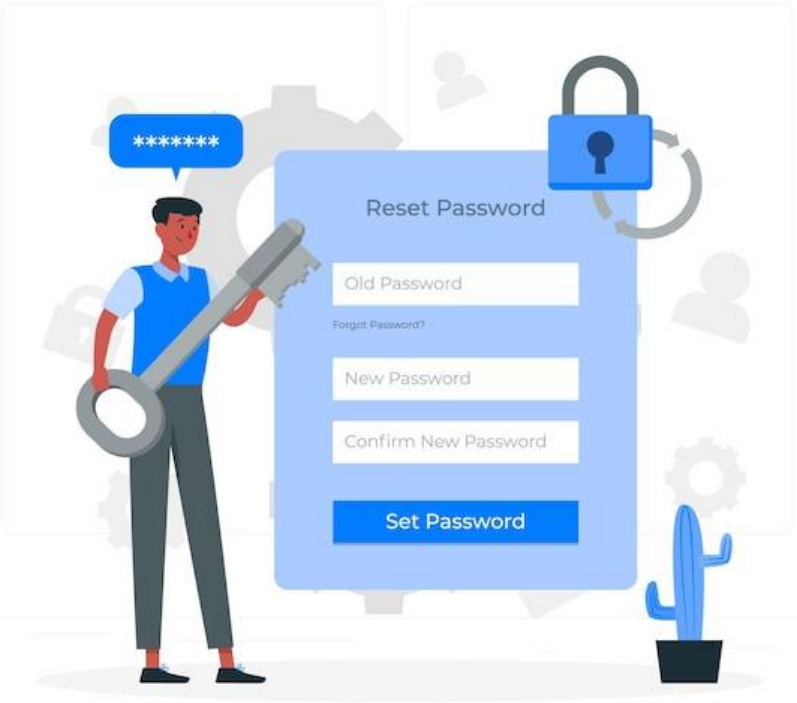
มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.2 จัดเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยและคุ้มครองความลับข้อมูลส่วนบุคคล และการเข้าถึงข้อมูลผู้ป่วย 30 คะแนน

4.2.1 ระบบมีบัญชีรายชื่อผู้ใช้งาน และรหัสผ่าน 10 คะแนน (จำเป็น)
(username and password)
และกลไกการยืนยันตัวบุคคล

4.2.2 สร้างระบบการเข้าถึงข้อมูลผู้ป่วยให้รัดกุม 10 คะแนน (จำเป็น)
(ใครสามารถเข้าถึงข้อมูลส่วนไหน
ด้วยวิธีใด เป็นต้น)

4.2.3 การแยกระบบ network ให้เหมาะกับ 10 คะแนน (จำเป็น)
ความปลอดภัยทางไซเบอร์ เช่น
ระบบ internet และระบบงานโรงพยาบาล
หรือการจัด private network



มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.3 มีแผนตอบโต้ด้านความปลอดภัยทางไซเบอร์ 50 คะแนน

4.3.1 มีการจัดตั้งจุดให้บริการแก่ผู้ใช้งานระบบ (Service Desk) 10 คะแนน (จำเป็น)

ช่องทางติดต่อประสานงาน 24/7
ตารางผู้รับผิดชอบ ช่องทางประสานงาน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.3.2 มีข้อตกลงระดับการให้บริการ (Service Level Agreement-SLA) 10 คะแนน (จำเป็น)

Service Level Agreement (SLA) 2023

โรงพยาบาลกาฬสินธุ์
KALASIN HOSPITAL

ข้อตกลงการแก้ปัญหาระบบ สารสนเทศการให้บริการ 3 ข้อ

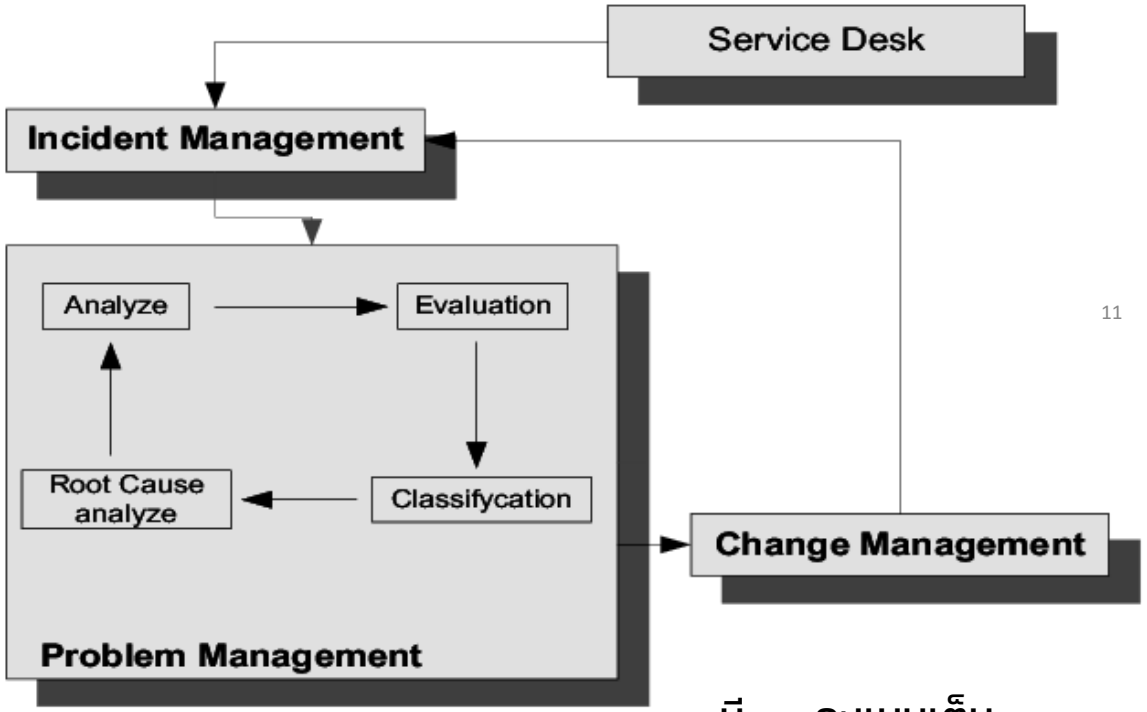
1 . การแก้ไขปัญหาเครื่องพิมพ์ ให้พร้อมใช้งาน ภายใน 15 นาที
2 . การแก้ไขปัญหาระบบ Internet ให้พร้อมใช้งาน ภายใน 15 นาที
3 . การแก้ไขปัญหาระบบคอมพิวเตอร์ขัดข้อง ณ จุดให้บริการด่านหน้า ให้พร้อมใช้งาน ภายใน 20 นาที

Service Level Agreement
งานบริการคลินิกจิตเวช โรงพยาบาลละหานทราย

การให้บริการ	ระยะเวลาประกันการให้บริการ	เงื่อนไขการให้บริการ
1.ชั่งน้ำหนัก/วัดส่วนสูง/รอบเอว/V/S	ไม่เกิน 5 นาที	ผู้รับผิดชอบ : พยาบาลวิชาชีพ / นักจิตวิทยา หน้าที่ความรับผิดชอบ : ลงบันทึกน้ำหนัก/ส่วนสูง/รอบเอว/สัญญาณชีพ
2.ซักประวัติ / ประเมินอาการ	ไม่เกิน 10 นาที	ผู้รับผิดชอบ : พยาบาลวิชาชีพ / นักจิตวิทยา หน้าที่ความรับผิดชอบ : ซักประวัติการเจ็บป่วย , ประวัติการใช้สารเสพติด , การแพ้ยา , โรคประจำตัว
3.ส่งพบจิตแพทย์	ไม่เกิน 40 นาที	ผู้รับผิดชอบ : จิตแพทย์ หน้าที่ความรับผิดชอบ : เพื่อวินิจฉัยรักษาทางจิตเวช
4.บริการหลังพบแพทย์	ไม่เกิน 10 นาที	ผู้รับผิดชอบ : พยาบาลวิชาชีพ / นักจิตวิทยา หน้าที่ความรับผิดชอบ : รับยา , ชำระเงิน(ถ้ามี), ให้คำแนะนำในการปฏิบัติตัว / การนัดครั้งต่อไป
5. ส่งต่อผู้ป่วยที่ต้อง Admitted (ถ้ามี)	ไม่เกิน 20 นาที	ผู้รับผิดชอบ : พยาบาลวิชาชีพ หน้าที่ความรับผิดชอบ :ปฏิบัติตามแนวทางการดูแลผู้ป่วย จิตเวช เช่น เตรียมเอกสาร / โทรประสานหน่วยงานที่เกี่ยวข้อง

4.3 มีแผนตอบโต้ด้านความปลอดภัยทางไซเบอร์ 50 คะแนน (ต่อ)

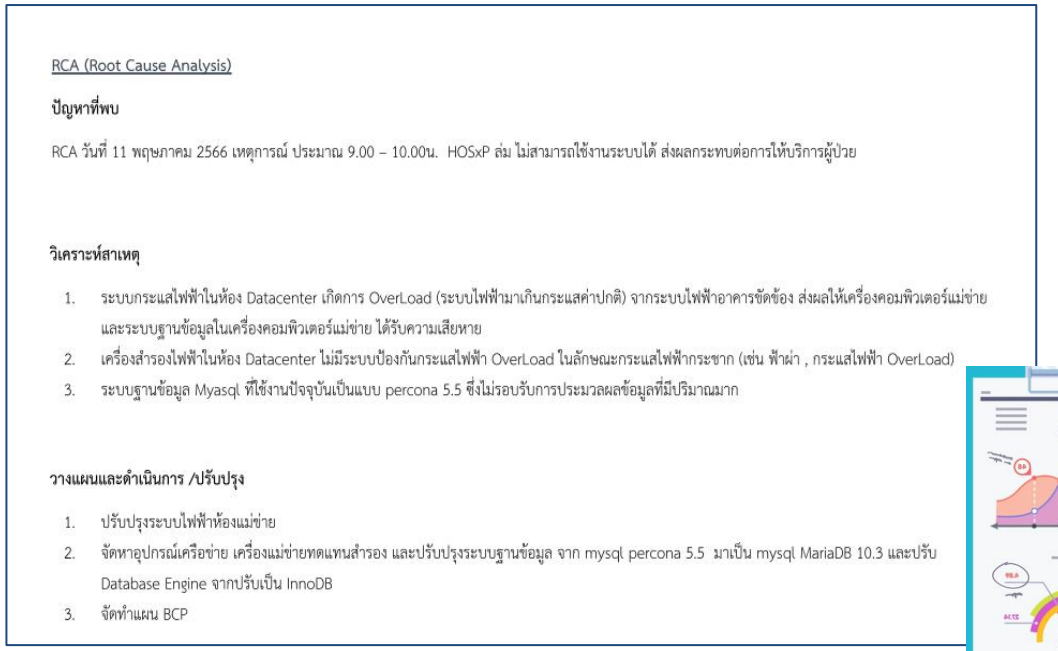
4.3.3 มีระบบการจัดการอุบัติการณ์ (Incident Management) และการจัดการปัญหา (Problem Management)
10 คะแนน (จำเป็น)



11

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.3.4 มีการจัดทำสถิติการให้บริการ สถิติอุบัติการณ์ และการรายงานการวิเคราะห์ปัญหา
10 คะแนน



RCA (Root Cause Analysis)

ปัญหาที่พบ

RCA วันที่ 11 พฤษภาคม 2566 เหตุการณ์ ประมาณ 9.00 – 10.00น. HOSxP ล่ม ไม่สามารถใช้งานระบบได้ ส่งผลกระทบต่อการให้บริการผู้ป่วย

วิเคราะห์สาเหตุ

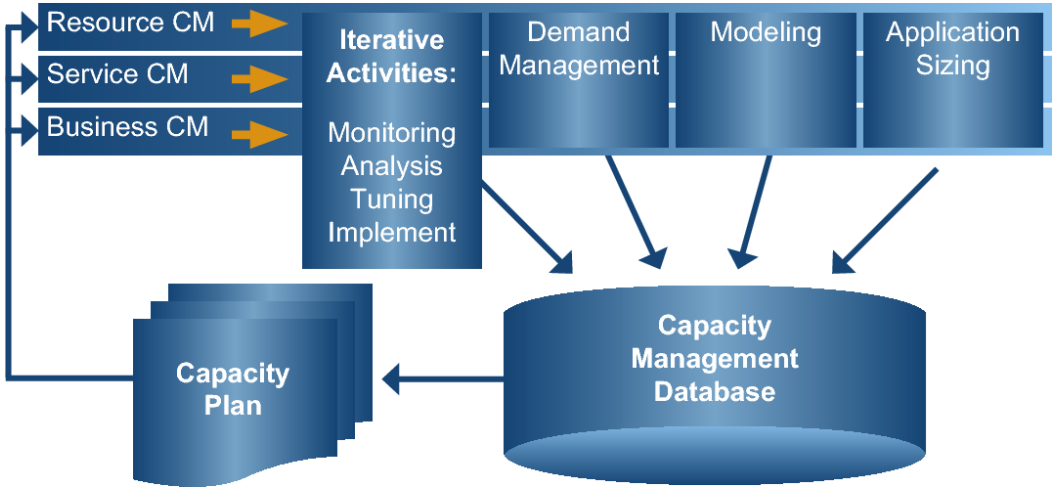
1. ระบบกระแสไฟฟ้าในห้อง Datacenter เกิดการ OverLoad (ระบบไฟฟ้ามาเกินกระแสค่าปกติ) จากระบบไฟฟ้าอาคารขัดข้อง ส่งผลให้เครื่องคอมพิวเตอร์แม่ข่าย และระบบฐานข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย ได้รับความเสียหาย
2. เครื่องสำรองไฟฟ้าในห้อง Datacenter ไม่มีระบบป้องกันกระแสไฟฟ้า OverLoad ในลักษณะกระแสไฟฟ้ากระชาก (เช่น ฟ้าผ่า , กระแสไฟฟ้า OverLoad)
3. ระบบฐานข้อมูล Myasql ที่ใช้งานปัจจุบันเป็นแบบ percona 5.5 ซึ่งไม่รอบรับการประมวลผลข้อมูลที่มีปริมาณมาก

วางแผนและดำเนินการ /ปรับปรุง

1. ปรับปรุงระบบไฟฟ้าห้องแม่ข่าย
2. จัดหาอุปกรณ์เครือข่าย เครื่องแม่ข่ายทดแทนสำรอง และปรับปรุงระบบฐานข้อมูล จาก mysql percona 5.5 มาเป็น mysql MariaDB 10.3 และปรับ Database Engine จากปรับเป็น InnoDB
3. จัดทำแผน BCP

4.3 มีแผนตอบโต้ด้านความปลอดภัยทางไซเบอร์ 50 คะแนน (ต่อ)

4.3.5 มีการจัดการและจัดสรรทรัพยากรที่เพียงพอ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ เหมาะสมกับปริมาณงาน (Capacity Management)
5 คะแนน



มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.3.6 มีการจัดทำแผนปฏิบัติงานเมื่อระบบล่ม (Business Continuity Plan -BCP) และแผนกู้คืน (Disaster Recovery Pian - DRP)
10 คะแนน (จำเป็น)

แผนการดำเนินงานกรณีระบบสารสนเทศล่ม
โรงพยาบาลกาฬสินธุ์ (Business Continuity Plan : BCP)

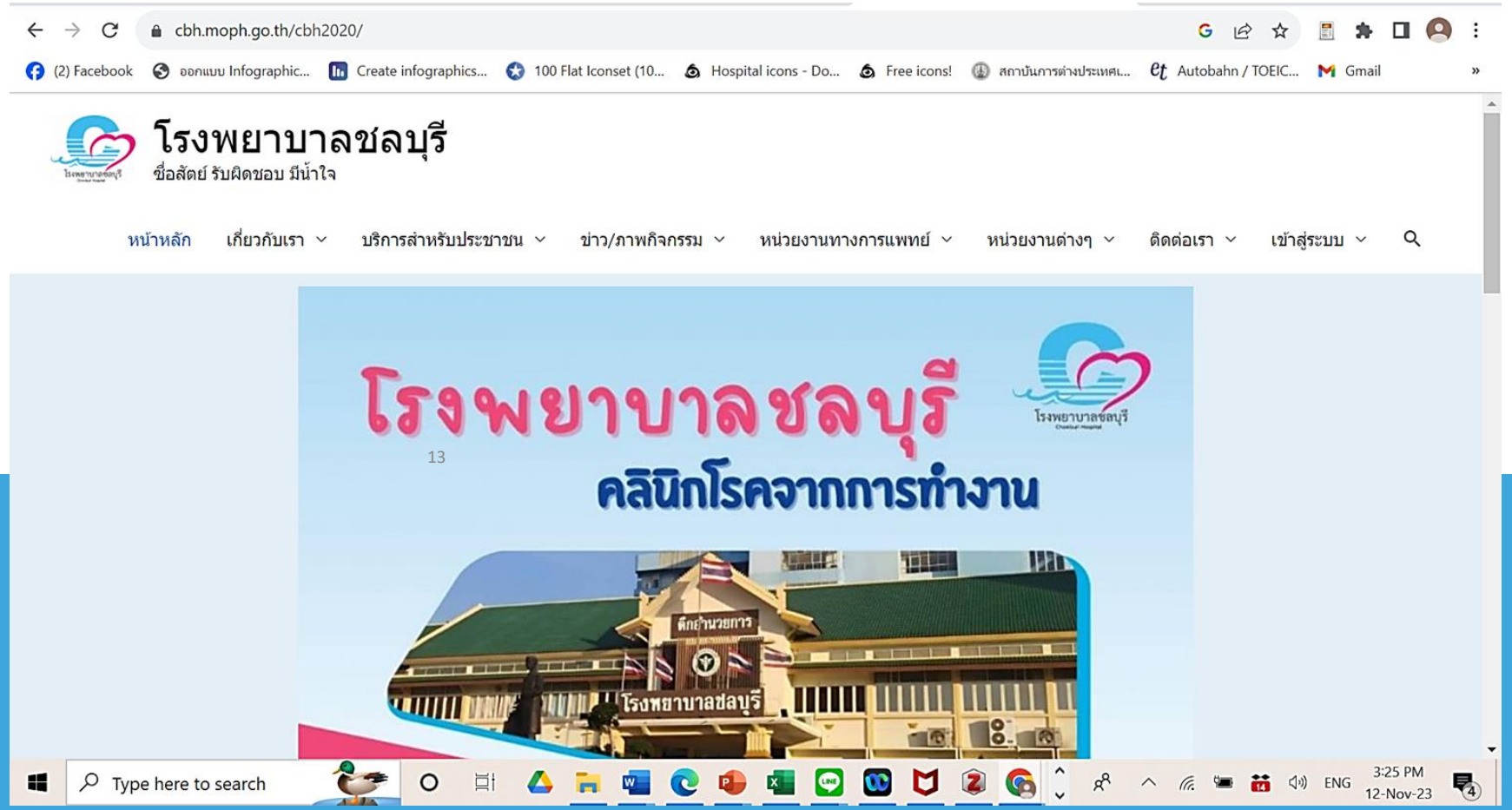
จัดทำโดย

กลุ่มงานสารสนเทศทางการแพทย์โรงพยาบาลกาฬสินธุ์

4.4 แอปพลิเคชั่นหรือ software พัฒนาเอง 15 คะแนน

4.4.1 การพัฒนา Application ที่มีองค์ประกอบส่วนใหญ่เป็นหน่วยย่อยที่นำมาใช้ใหม่ร่วมกันได้/website รพ. ต้องมี domain .moph/.go.th 5 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน



4.4 แอปพลิเคชั่นหรือ software พัฒนาเอง 15 คะแนน (ต่อ)

4.4.2 การจัดสร้าง/ต่อเติม software/website รพ. ให้เป็นไปอย่างมีประสิทธิภาพ รวมทั้งกำกับดูแล source code/version ของ software 10 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

```
static bool init(CURL *&conn, char *url)
{
  CURLcode code;

  conn = curl_easy_init();

  if (conn == NULL)
  {
    fprintf(stderr, "Failed to create CURL connection\n");

    exit(EXIT_FAILURE);
  }

  code = curl_easy_setopt(conn, CURLOPT_ERRORBUFFER,
errorBuffer);
  if (code != CURLE_OK)
  {
    fprintf(stderr, "Failed to set error buffer [%d]\n",
code);

    return false;
  }

  code = curl_easy_setopt(conn, CURLOPT_URL, url);
  if (code != CURLE_OK)
  {
    fprintf(stderr, "Failed to set URL [%s]\n", errorBuff-
er);

    return false;
  }

  code = curl_easy_setopt(conn, CURLOPT_FOLLOWLOCATION,
1L);
  if (code != CURLE_OK)
  {
    fprintf(stderr, "Failed to set redirect option [%s]\n",
errorBuffer);

    return false;
  }

  code = curl_easy_setopt(conn, CURLOPT_WRITEFUNCTION,
writer);
  if (code != CURLE_OK)
  {
    fprintf(stderr, "Failed to set writer [%s]\n",
errorBuffer);

    return false;
  }

  code = curl_easy_setopt(conn, CURLOPT_WRITEDATA,
&buffer);
  if (code != CURLE_OK)
  {
    fprintf(stderr, "Failed to set write data [%s]\n",
errorBuffer);

  return true;
```

```
static void startElement(void *voidContext,
                         const xmlChar *name,
                         const xmlChar **attributes)
{
  Context *context = (Context *)voidContext;

  if (COMPARE((char *)name, "TITLE"))
  {
    context->title = "";
    context->addTitle = true;
  }
  (void) attributes;
}

//
//  libxml end element callback function
//

static void EndElement(void *voidContext,
                       const xmlChar *name)
{
  Context *context = (Context *)voidContext;

  if (COMPARE((char *)name, "TITLE"))
    context->addTitle = false;
}

//
//  Text handling helper function
//

static void handleCharacters(Context *context,
                             const xmlChar *chars,
                             int length)
{
  if (context->addTitle)
    context->title.append((char *)chars, length);
}

//
//  libxml PCDATA callback function
//

static void Characters(void *voidContext,
                       const xmlChar *chars,
                       int length)
{
  Context *context = (Context *)voidContext;

  handleCharacters(context, chars, length);
}

static void cdata(void *voidContext,
                  const xmlChar *chars,
                  int length)
{
  Context *context = (Context *)voidContext;

  handleCharacters(context, chars, length);
```

4.5 ธรรมาภิบาล 75 คะแนน

4.5.1 ระบบควบคุมด้านความมั่น คงปลอดภัยสารสนเทศ (Information Security Management) มีกระบวนการควบคุมที่ทำให้แน่ใจได้ว่า ระบบและข้อมูลได้รับการปกป้องจากการเข้าถึงหรือโจมตีโดยผู้ไม่ประสงค์ดี การใช้งานที่ไม่ถูกต้องหรือไม่ได้รับอนุญาต ประกอบไปด้วย (PDPA ม. 37) — 30 คะแนน

4.5.2 มีระบบควบคุมด้วย application (Application control) เพื่อให้แน่ใจว่าข้อมูลสารสนเทศที่มีอยู่ในระบบเป็นข้อมูลที่ถูกต้อง ครบถ้วน เชื่อถือได้ทันเวลา โดยมีระบบควบคุมตรวจสอบดังนี้ — 10 คะแนน

4.5.3 มีระบบควบคุมคุณภาพข้อมูล ให้แน่ใจว่า ข้อมูลสำคัญที่บันทึก และจัดเก็บไว้ในระบบ มีคุณภาพที่ดีขึ้นอย่างต่อเนื่อง — 10 คะแนน

4.5.4 มีประกาศ Privacy Policy ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ — 10 คะแนน

ตามประกาศ ศทส. ที่ สธ.0212/ว 410 ลงวันที่ 25 พฤษภาคม 2565

4.5.5 มีประกาศ Privacy Noticeปฏิบัติตามประกาศ ศทส. แนวปฏิบัติการคุ้มครองฯ ที่ สธ. 0212/ว 11424 ลงวันที่ 25 พฤษภาคม และที่ สธ. 0212/ว 14039 ลงวันที่ 24 มิถุนายน 2565 — 5 คะแนน

4.5.6 หน่วยงานจัดทำรายการประมวลผลข้อมูลส่วนบุคคล (ROPA) ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ในการจัดทำ ROPA ตามหนังสือ ศทส. ที่ สธ. 0212.07/ว 2823 ลงวันที่ 3 กุมภาพันธ์ 2566 — 5 คะแนน

4.5.7 มีการแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (DPO) ของหน่วยบริการ — 5 คะแนน

4.5.1 ระบบควบคุมด้านความมั่น คงปลอดภัยสารสนเทศ (Information Security Management) มีกระบวนการควบคุมที่ทำให้แน่ใจได้ว่า ระบบและข้อมูลได้รับการปกป้องจากการเข้าถึงหรือโจมตี โดยผู้ไม่ประสงค์ดี การใช้งานที่ไม่ถูกต้องหรือไม่ได้รับอนุญาต ประกอบไปด้วย (PDPA ม. 37) 30 คะแนน

❑ มีทะบียนผู้ใช้งานการควบคุมการเข้าถึง (Access Control) การจัดการการเข้าถึงของผู้ใช้งาน (User access management) รวมถึงการทำบัญชีรายชื่อผู้ใช้งาน การกำหนดสิทธิผู้ใช้งานการรักษาความลับรหัสผ่านของผู้ใช้แต่ละบุคคล รวมถึงยืนยันตัวบุคคล (Authentication) (PDPA ม. 24)	5 คะแนน (จำเป็น)
❑ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) (PDPA ม. 24)	5 คะแนน (จำเป็น)
❑ มีระบบการควบคุมการเข้าถึงระบบงาน หรือโปรแกรม (System and application access control)	5 คะแนน (จำเป็น)
❑ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)	5 คะแนน
❑ การป้องกันการบุกรุกเครือข่าย จากการเชื่อมโยง Internet	5 คะแนน (จำเป็น)
❑ การบำรุงรักษาระบบโดยบุคคลภายนอก มีมาตรการควบคุม	5 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.5.2 มีระบบควบคุมด้วย application (Application control) เพื่อให้แน่ใจว่า ข้อมูลสารสนเทศที่มีอยู่ในระบบเป็นข้อมูลที่ถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลา 10 คะแนน

- ❑ การตรวจสอบความครบถ้วน (completeness check) มีระบบที่ทำให้แน่ใจว่ามีการบันทึกข้อมูลผู้รับบริการทุกรายที่เข้ามารับบริการในโรงพยาบาลอย่างครบถ้วน — 2 คะแนน
- ❑ ข้อมูลผู้รับบริการทุกคนที่มารับบริการ ถูกบันทึกข้อมูลไว้ในระบบอย่างเป็นระบบแบบแผน (input control) — 2 คะแนน
- ❑ การตรวจสอบความถูกต้อง (validity check) มีระบบที่ทำให้แน่ใจว่าข้อมูลต่างๆ ที่นำเข้าระบบสารสนเทศ มีความถูกต้อง เที่ยงตรง รวมทั้งมีระบบการเรียกดูข้อมูลผู้รับบริการ และตรวจสอบความครบถ้วนของข้อมูลผู้รับบริการอย่างสม่ำเสมอ โดยการเรียกดูแบบสุ่มตัวอย่าง ดำเนินการโดยแพทย์ พยาบาลและผู้เกี่ยวข้องที่มีอำนาจหน้าที่ในการนำข้อมูลเข้า หรือเรียกดูข้อมูลได้ การเรียกดูข้อมูลผู้รับบริการเน้นไปที่ความตรงต่อเวลา ความครบถ้วนของข้อมูล การเรียกดูข้อมูลครอบคลุมทั้งผู้ที่กำลังรับบริการอยู่และที่กลับไปแล้ว — 2 คะแนน
- ❑ การระบุเจ้าของข้อมูล (identification) มีการควบคุมที่ทำให้แน่ใจว่า มีการระบุบุคคลได้อย่างชัดเจน ไม่มีข้อมูลซ้ำ (ข้อมูลผู้ป่วย 2 ราย ถูกระบุเป็นคนเดียวกันในระบบ) และข้อมูลที่นำเข้าเป็นของผู้ป่วยรายนั้นจริง — 2 คะแนน
- ❑ การระบุตัวผู้เข้าใช้ระบบ และควบคุมให้ผู้มีสิทธิเท่านั้นที่เข้าใช้งานระบบได้ตามสิทธิ มีการบันทึกข้อมูลการเข้าใช้งาน — 2 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

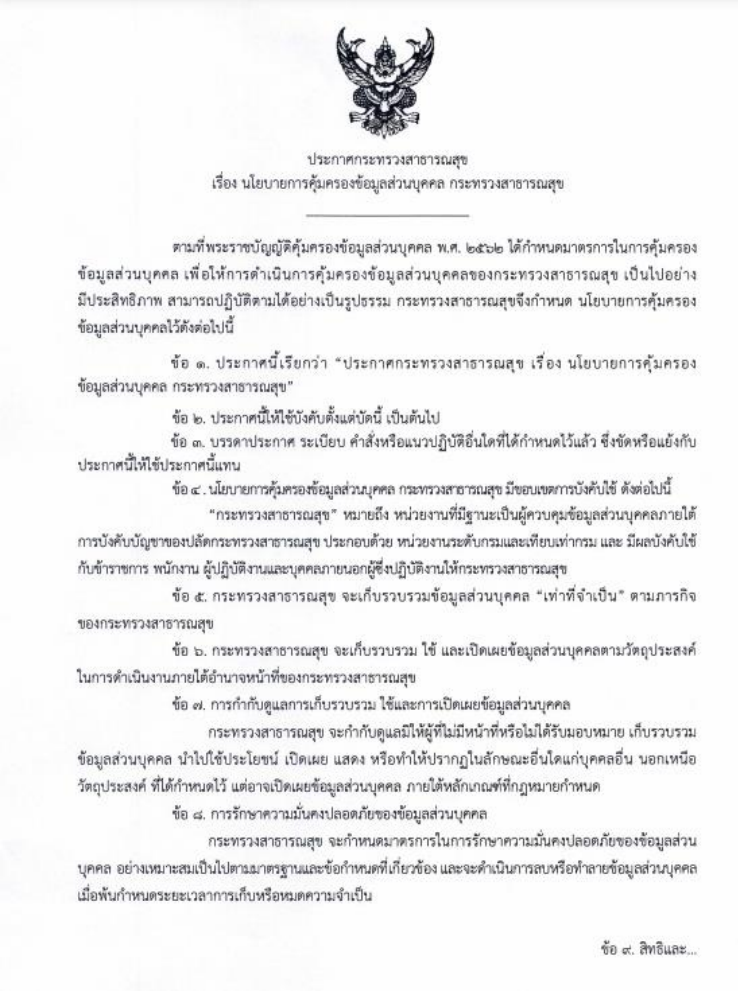
4.5.3 มีระบบควบคุมคุณภาพข้อมูล ให้แน่ใจว่า ข้อมูลสำคัญที่บันทึก และจัดเก็บไว้ในระบบ มีคุณภาพที่ดีขึ้นอย่างต่อเนื่อง 10 คะแนน (จำเป็น)

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.5.4 มีประกาศ Privacy Policy ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ตามประกาศ ศทส. ที่ สธ.0212/ว 410 ลงวันที่ 25 พฤษภาคม 2565

10 คะแนน (จำเป็น)

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน



ประกาศกระทรวงสาธารณสุข
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม กระทรวงสาธารณสุขจึงกำหนด นโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า "ประกาศกระทรวงสาธารณสุข เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข"

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข มีขอบเขตการบังคับใช้ ดังต่อไปนี้

"กระทรวงสาธารณสุข" หมายถึง หน่วยงานที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การบังคับบัญชาของปลัดกระทรวงสาธารณสุข ประกอบด้วย หน่วยงานระดับกรมและเทียบเท่ากรม และ มีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงานและบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้กระทรวงสาธารณสุข

ข้อ ๕. กระทรวงสาธารณสุข จะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" ตามภารกิจของกระทรวงสาธารณสุข

ข้อ ๖. กระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ในการดำเนินงานภายใต้อำนาจหน้าที่ของกระทรวงสาธารณสุข

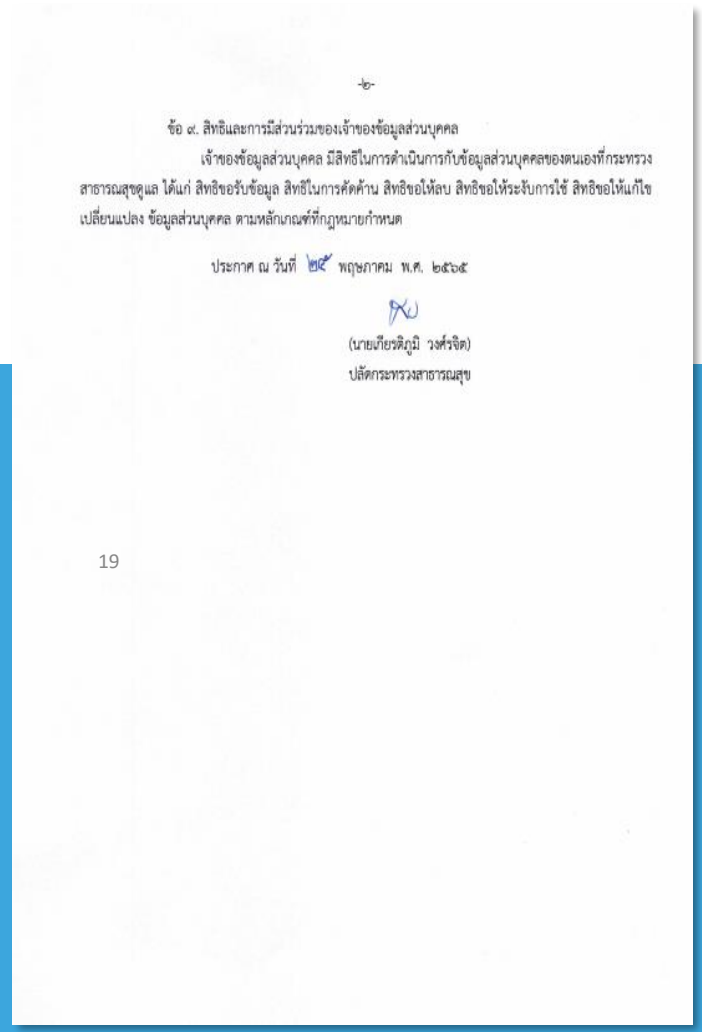
ข้อ ๗. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมาย เก็บรวบรวม ข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ ที่ได้กำหนดไว้ แต่อาจเปิดเผยข้อมูลส่วนบุคคล ภายใต้หลักเกณฑ์ที่กฎหมายกำหนด

ข้อ ๘. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล อย่างเหมาะสมเป็นไปตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง และจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็น

ข้อ ๙. สิทธิและ...



-๒-

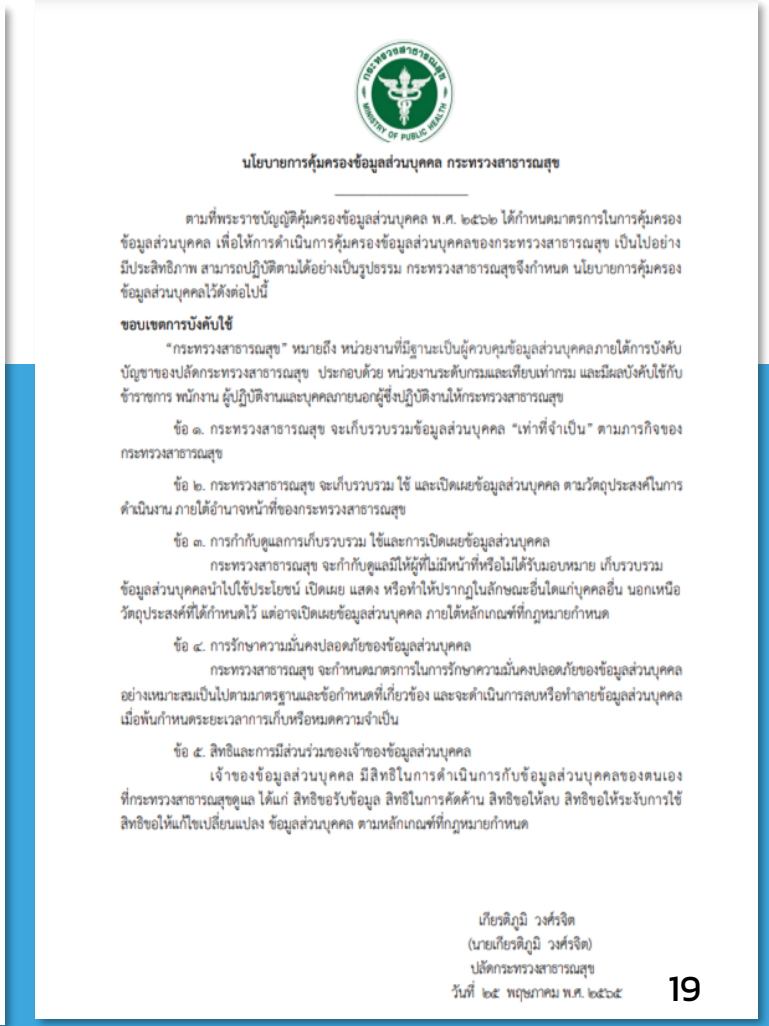
ข้อ ๙. สิทธิและการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการกับข้อมูลส่วนบุคคลของตนเองที่กระทรวงสาธารณสุขดูแล ได้แก่ สิทธิขอรับข้อมูล สิทธิในการคัดค้าน สิทธิขอให้ลบ สิทธิขอให้ระงับการใช้ สิทธิขอให้แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่กฎหมายกำหนด

ประกาศ ณ วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๕

(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข

19



นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม กระทรวงสาธารณสุขจึงกำหนด นโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ดังต่อไปนี้

ขอบเขตการบังคับใช้

"กระทรวงสาธารณสุข" หมายถึง หน่วยงานที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การบังคับบัญชาของปลัดกระทรวงสาธารณสุข ประกอบด้วย หน่วยงานระดับกรมและเทียบเท่ากรม และมีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงานและบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้กระทรวงสาธารณสุข

ข้อ ๑. กระทรวงสาธารณสุข จะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" ตามภารกิจของกระทรวงสาธารณสุข

ข้อ ๒. กระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ในการดำเนินงาน ภายใต้อำนาจหน้าที่ของกระทรวงสาธารณสุข

ข้อ ๓. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมาย เก็บรวบรวม ข้อมูลส่วนบุคคลนำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ที่ได้กำหนดไว้ แต่อาจเปิดเผยข้อมูลส่วนบุคคล ภายใต้หลักเกณฑ์ที่กฎหมายกำหนด

ข้อ ๔. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล อย่างเหมาะสมเป็นไปตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง และจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็น

ข้อ ๕. สิทธิและการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

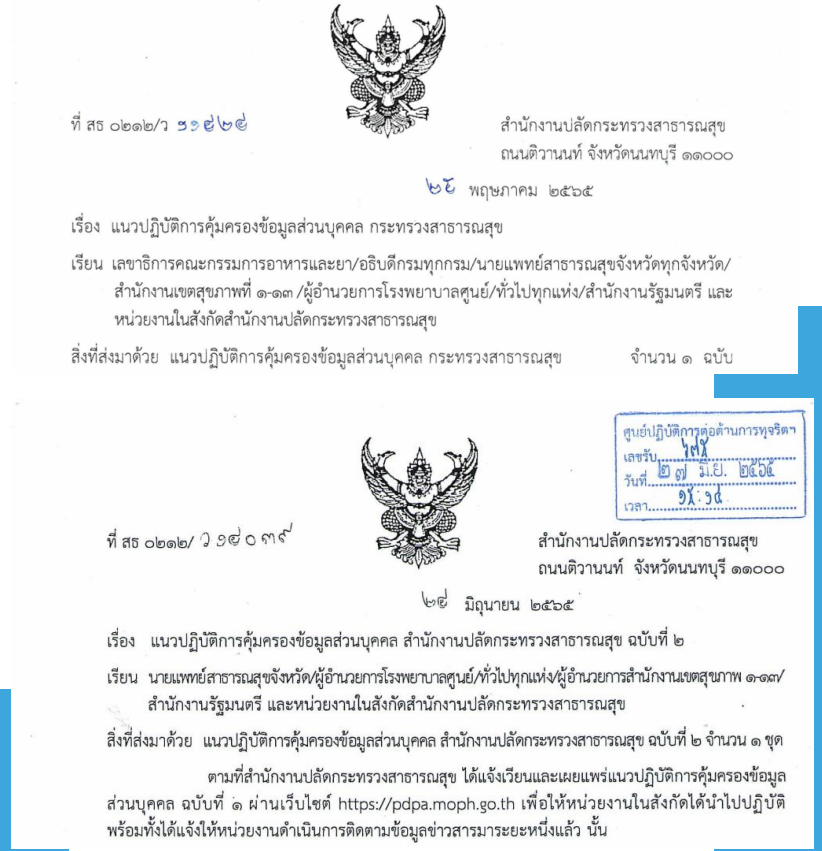
เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการกับข้อมูลส่วนบุคคลของตนเอง ที่กระทรวงสาธารณสุขดูแล ได้แก่ สิทธิขอรับข้อมูล สิทธิในการคัดค้าน สิทธิขอให้ลบ สิทธิขอให้ระงับการใช้ สิทธิขอให้แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่กฎหมายกำหนด

เกียรติภูมิ วงศ์รจิต
(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข
วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๕

19

4.5.5 มีประกาศ Privacy Noticeปฏิบัติตามประกาศ ศทส. แนวปฏิบัติการคุ้มครอง ฯ ที่ สธ. 0212/ว 11424 ลงวันที่ 25 พฤษภาคม และที่ สธ. 0212/ว 14039 ลง วันที่ 24 มิถุนายน 2565 5 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน



ที่ สธ ๐๒๑๒/ว ๑๑๔๒๔ สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๕ พฤษภาคม ๒๕๖๕

เรื่อง แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/สำนักงานเขตสุขภาพที่ ๑-๑๓ /ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง/สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข จำนวน ๑ ฉบับ

ศูนย์ปฏิบัติการต่อต้านการทุจริต เลขรับ ๑๙๖ วันที่ ๒๗ มิ.ย. ๒๕๖๕ เวลา ๑๖.๑๔

ที่ สธ ๐๒๑๒/ ว ๑๔๐๓๙ สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

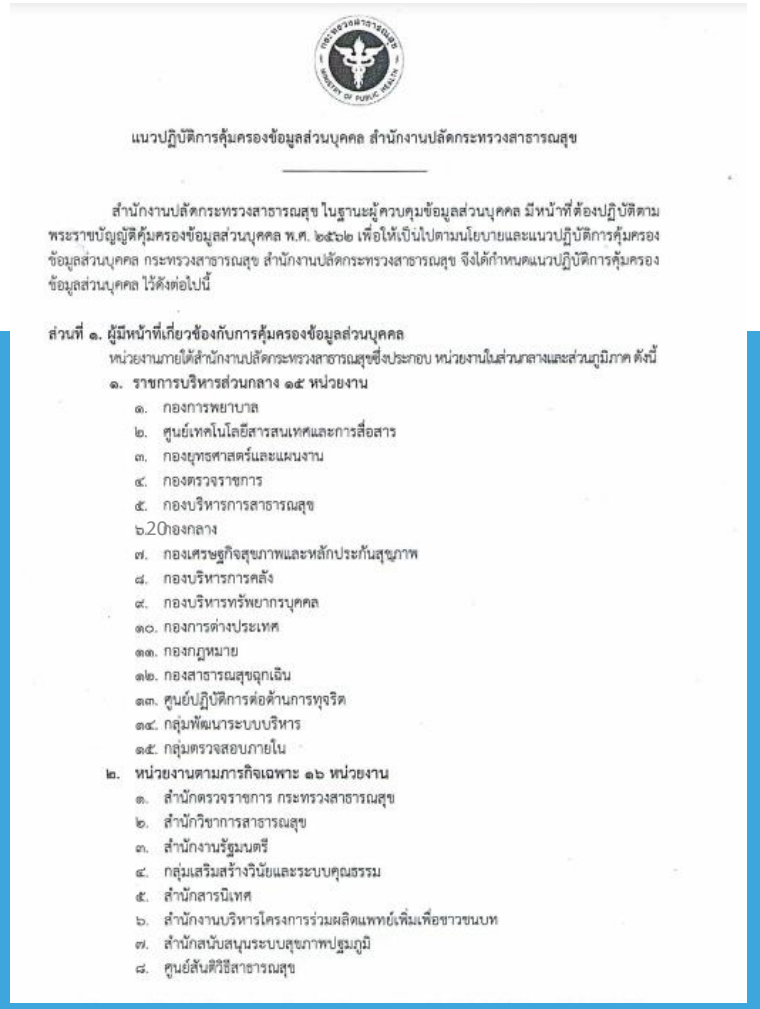
๒๔ มิถุนายน ๒๕๖๕

เรื่อง แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ฉบับที่ ๒

เรียน นายแพทย์สาธารณสุขจังหวัด/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง/ผู้อำนวยการสำนักงานเขตสุขภาพ ๑-๑๓/ สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ฉบับที่ ๒ จำนวน ๑ ชุด

ตามที่สำนักงานปลัดกระทรวงสาธารณสุข ได้แจ้งเวียนและเผยแพร่แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ฉบับที่ ๑ ผ่านเว็บไซต์ https://pdpa.moph.go.th เพื่อให้หน่วยงานในสังกัดได้นำไปปฏิบัติ พร้อมทั้งได้แจ้งให้หน่วยงานดำเนินการติดตามข้อมูลข่าวสารมาระยะหนึ่งแล้ว นั้น



แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข

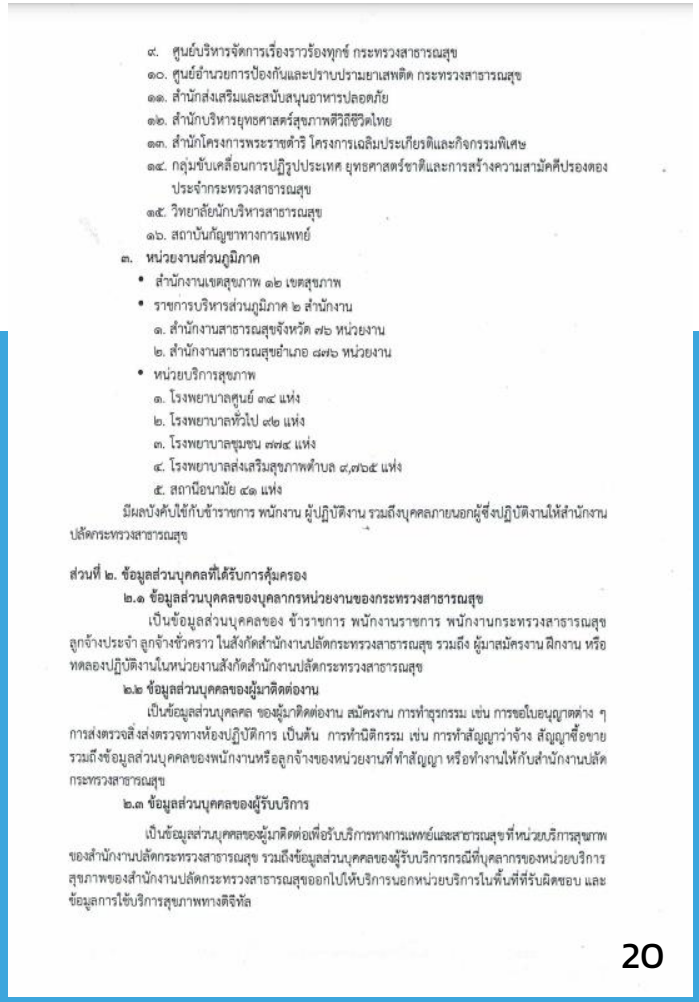
สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุข จึงได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ไว้ดังต่อไปนี้

ส่วนที่ ๑. ผู้มีหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานภายใต้สำนักงานปลัดกระทรวงสาธารณสุขซึ่งประกอบ หน่วยงานในส่วนกลางและส่วนภูมิภาค ดังนี้

๑. ราชการบริหารส่วนกลาง ๑๕ หน่วยงาน
- ๑. กองการพยาบาล
- ๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๓. กองยุทธศาสตร์และแผนงาน
- ๔. กองตรวจราชการ
- ๕. กองบริหารการสาธารณสุข
- ๖.20กองกลาง
- ๗. กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ
- ๘. กองบริหารการคลัง
- ๙. กองบริหารทรัพยากรบุคคล
- ๑๐. กองการต่างประเทศ
- ๑๑. กองกฎหมาย
- ๑๒. กองสาธารณสุขฉุกเฉิน
- ๑๓. ศูนย์ปฏิบัติการต่อต้านการทุจริต
- ๑๔. กลุ่มพัฒนาระบบบริหาร
- ๑๕. กลุ่มตรวจสอบภายใน

๒. หน่วยงานตามภารกิจเฉพาะ ๑๖ หน่วยงาน
- ๑. สำนักตรวจราชการ กระทรวงสาธารณสุข
- ๒. สำนักวิชาการสาธารณสุข
- ๓. สำนักงานรัฐมนตรี
- ๔. กลุ่มเสริมสร้างวินัยและระบบคุณธรรม
- ๕. สำนักสารนิเทศ
- ๖. สำนักงานบริหารโครงการร่วมผลิตแพทย์เพิ่มเพื่อชาวชนบท
- ๗. สำนักสนับสนุนระบบสุขภาพปฐมภูมิ
- ๘. ศูนย์สันติวิธีสาธารณสุข



- ๙. ศูนย์บริหารจัดการเรื่องราวร้องทุกข์ กระทรวงสาธารณสุข
- ๑๐. ศูนย์อำนวยการป้องกันและปราบปรามยาเสพติด กระทรวงสาธารณสุข
- ๑๑. สำนักส่งเสริมและสนับสนุนอาหารปลอดภัย
- ๑๒. สำนักบริหารยุทธศาสตร์สุขภาพศิวิลัยชีวิตไทย
- ๑๓. สำนักโครงการพระราชดำริ โครงการเฉลิมประเกียรติและกิจกรรมพิเศษ
- ๑๔. กลุ่มขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติและการสร้างความสามัคคีปรองดองประจำกระทรวงสาธารณสุข
- ๑๕. วิทยาลัยนักบริหารสาธารณสุข
- ๑๖. สถาบันกัญชาทางการแพทย์

๓. หน่วยงานส่วนภูมิภาค
- สำนักงานเขตสุขภาพ ๑๒ เขตสุขภาพ
- ราชการบริหารส่วนภูมิภาค ๒ สำนักงาน
  - ๑. สำนักงานสาธารณสุขจังหวัด ๗๖ หน่วยงาน
  - ๒. สำนักงานสาธารณสุขอำเภอ ๘๗๖ หน่วยงาน
- หน่วยบริการสุขภาพ
  - ๑. โรงพยาบาลศูนย์ ๑๔ แห่ง
  - ๒. โรงพยาบาลทั่วไป ๗๒ แห่ง
  - ๓. โรงพยาบาลชุมชน ๗๗๔ แห่ง
  - ๔. โรงพยาบาลส่งเสริมสุขภาพตำบล ๘,๗๖๕ แห่ง
  - ๕. สถานีอนามัย ๔๑ แห่ง

มีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงาน รวมถึงบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้สำนักงานปลัดกระทรวงสาธารณสุข

ส่วนที่ ๒. ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง

๒.๑ ข้อมูลส่วนบุคคลของบุคลากรหน่วยงานของกระทรวงสาธารณสุข

เป็นข้อมูลส่วนบุคคลของ ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างประจำ ลูกจ้างชั่วคราว ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข รวมถึง ผู้มาสมัครงาน ฝึกงาน หรือทดลองปฏิบัติงานในหน่วยงานสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

๒.๒ ข้อมูลส่วนบุคคลของผู้มาติดต่องาน

เป็นข้อมูลส่วนบุคคล ของผู้มาติดต่องาน สมัครงาน การทำธุรกรรม เช่น การขอใบอนุญาตต่าง ๆ การส่งตรวจสิ่งส่งตรวจทางห้องปฏิบัติการ เป็นต้น การทำนิติกรรม เช่น การทำสัญญาว่าจ้าง สัญญาซื้อขาย รวมถึงข้อมูลส่วนบุคคลของพนักงานหรือลูกจ้างของหน่วยงานที่ทำสัญญา หรือทำงานให้กับสำนักงานปลัดกระทรวงสาธารณสุข

๒.๓ ข้อมูลส่วนบุคคลของผู้รับบริการ

เป็นข้อมูลส่วนบุคคลของผู้มาติดต่อเพื่อรับบริการทางการแพทย์และสาธารณสุขที่หน่วยบริการสุขภาพของสำนักงานปลัดกระทรวงสาธารณสุข รวมถึงข้อมูลส่วนบุคคลของผู้รับบริการกรณีที่บุคลากรของหน่วยบริการสุขภาพของสำนักงานปลัดกระทรวงสาธารณสุขออกไปให้บริการนอกหน่วยบริการในพื้นที่ที่รับผิดชอบ และข้อมูลการใช้บริการสุขภาพทางดิจิทัล

4.5.6 หน่วยงานจัดทำรายการประมวลผลข้อมูลส่วนบุคคล (ROPA) ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ในการจัดทำ ROPA ตามหนังสือ ศทส. ที่ สธ. 0212.07/ว 2823 ลงวันที่ 3 กุมภาพันธ์ 2566 5 คะแนน

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

แบบฟอร์ม การบันทึกรายการประมวลผลข้อมูลส่วนบุคคลของ สป. (ROPA)

ประเภทของข้อมูลที่ทำการจัดเก็บ (Types of personal	Data	ฐานการประมวลผลตามมาตรา	ฐานการประมวลผลตามมาตรา
1.1 ชื่อ/นามสกุล	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.2 หมายเลขบัตรประจำตัวประชาชน	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.3 วัน/เดือน/ปีเกิด	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.4 เพศ	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.5 หมายเลขโทรศัพท์	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.6 รหัสประจำตัวทางสาธารณสุข	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.9 ที่อยู่ปัจจุบัน	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.7 หมายเลขหนังสือเดินทาง	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.8 ข้อมูลบุคคลใกล้ชิด	ข้อมูลส่วนบุคคลพื้นฐาน (Personal	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
1.1 อาการของโรค/ประวัติการรักษา	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว	เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์	เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์

วัตถุประสงค์การจัดเก็บ (Purpose of collection)	ผู้ใช้ข้อมูล (Data Owner)	รูปแบบการนำเข้าข้อมูล (Collection Source)	สื่อที่ใช้ในการจัดเก็บ (Collection Medium)	สถานที่เก็บทางกายภาพ (Physical	สถานที่เก็บอิเล็กทรอนิกส์ (Electronic Storage)	ฝ่ายอื่นที่ใช้ข้อมูล/วัตถุประสงค์การใช้ (Users of Personal	ฝ่ายอื่นที่เข้าถึง (Access to Perso	องค์กรอื่นที่มีการเปิดเผย (External Parties and	รูปแบบการโอน (Transfer	ระยะเวลาการจัดเก็บ (Retention Period	การทำลายข้อมูล (Disposal Meth	มาตรการเชิงเทคนิค	มาตรการเชิงองค์กร
เพื่อการดำเนินงานสุขภาพดิจิทัลให้สอดคล้องกับนโยบายกระทรวงสาธารณสุข	กลุ่มแพลตฟอร์มสุขภาพดิจิทัล สำนักสุขภาพดิจิทัล	เจ้าของข้อมูลส่วนบุคคลโดยตรง	Online Form	1. เอกสาร 2. Hardware	Share Drived, HRM, CRM	ไม่มี	นักพัฒนาระบบ	บริษัท (ผู้ประมวลผลข้อมูลส่วนบุคคล/	อิเล็คทรอนิกส์ (Database)	10 ปี นับตั้งแต่ผู้รับจ้างส่งมอบ	1. เครื่องย่อยกระดาษ	การเข้ารหัสข้อมูล	การกำหนดสิทธิการเข้าถึง
เพื่อการดำเนินงานสุขภาพดิจิทัลให้สอดคล้องกับนโยบายกระทรวงสาธารณสุข	ผู้ให้บริการ (รพ./คลินิก	ผู้ให้บริการโดยตรง	API Gateway	1. เอกสาร 2. Hardware	Share Drived, HRM, CRM	ไม่มี	สำนักงานหลักประกันสุขภาพแห่งชาติ	หน่วยบริการที่เกี่ยวข้อง	อิเล็คทรอนิกส์ (Database)	10 ปี นับตั้งแต่ผู้รับจ้างส่งมอบงาน	1. เครื่องย่อยกระดาษ 2. ลบ	VA Scan	ทำสัญญาการแบ่งปันข้อมูล (Data Sharing Agreement
เพื่อการดำเนินงานตามวัตถุประสงค์ของเจ้าของข้อมูลส่วนบุคคล	ผู้ประมวลผลข้อมูล (บริ	ผู้ประมวลผลข้อมูลโดยตรง	1. Role based access control 2. Data Sync 3. Security Gateway 4. Central Security Gateway	1. เอกสาร 2. Hardware	Share Drived, HRM, CRM	ไม่มี	ไม่มี	ไม่มี	อิเล็คทรอนิกส์ (Database)	10 ปี นับตั้งแต่ผู้รับจ้างส่งมอบงาน	1. เครื่องย่อยกระดาษ 2. ลบ Datab	Penetration Testing	1.ทำสัญญาการเก็บรักษาข้อมูลที่เป็นความลับ (Non-disclo sure

4.5.7 มีการแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (DPO) ของหน่วยบริการ 5 คะแนน

คำสั่งโรงพยาบาลธัญญารักษ์ขอนแก่น

ที่ ๑๓๑๒ / ๒๕๖๕

เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO : Data Protection Officer)

ประจำโรงพยาบาลธัญญารักษ์ขอนแก่น

ด้วย โรงพยาบาลธัญญารักษ์ขอนแก่น เป็นหน่วยงานที่มีการดำเนินกิจการที่เกี่ยวข้องกับการเก็บ 22
รวบรวมประมวลผล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO : Data Protection Officer)

สำเนาคู่ฉบับ

คำสั่งโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

ที่ ๑๙๙ /๒๕๖๕

เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

.....

ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนของตนในกรณี (๑) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (๒) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวมใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด และ (๓) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖ ซึ่งโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.6 จัดตั้งคณะกรรมการพัฒนาสุขภาพดิจิทัลระดับโรงพยาบาล 10 คะแนน (จำเป็น)

คำสั่งโรงพยาบาลเกาะสมุย
ที่ ๕๓๑ /๒๕๖๕
เรื่อง แต่งตั้งคณะกรรมการดิจิทัลการแพทย์โรงพยาบาลเกาะสมุย

.....

อาศัยอำนาจตามคำสั่งกระทรวงสาธารณสุข ที่ ๘๖๕/๒๕๖๕ ลงวันที่ ๒๑ กรกฎาคม ๒๕๖๕ เรื่อง มอบหมายให้ข้าราชการเป็นผู้บังคับบัญชา ด้วยสำนักงานปลัดกระทรวงสาธารณสุขมอบนโยบายและทิศทางการดำเนินงานกระทรวงสาธารณสุข โดยมุ่งเน้นผลักดันการบริการทางการแพทย์และสาธารณสุขสู่ยุคดิจิทัล ให้โรงพยาบาลบริการการแพทย์ทางไกล (Telemedicine) โดยให้โรงพยาบาลทุกแห่งมีหน่วยรับผิดชอบเพื่อขับเคลื่อนการใช้เทคโนโลยีทางการแพทย์ และจัดเตรียมบุคลากรสนับสนุนบริการดิจิทัลการแพทย์ในรูปแบบกลุ่มงานภายในหรือคณะกรรมการดิจิทัลการแพทย์โรงพยาบาล เพื่อปฏิบัติหน้าที่เร่งรัดการจัดบริการสุขภาพดิจิทัล

ดังนั้น เพื่อให้การดำเนินงานด้านดิจิทัลการแพทย์โรงพยาบาลเกาะสมุย เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ จึงขอแต่งตั้งคณะกรรมการ ดังรายชื่อต่อไปนี้

๑. รองผู้อำนวยการฝ่ายพัฒนาระบบบริการและสนับสนุนบริการสุขภาพ	ประธาน
๒. นายภัทรัช เวศพิศ	รองประธาน
๓. หัวหน้ากลุ่มงานผู้ป่วยนอก	กรรมการ
๔. หัวหน้ากลุ่มงานเวชกรรมสังคม	กรรมการ
๕. หัวหน้ากลุ่มงานอายุรกรรม	กรรมการ
๖. หัวหน้ากลุ่มงานการพยาบาลผู้ป่วยนอก	กรรมการ
๗. หัวหน้ากลุ่มงานการพยาบาลชุมชน	กรรมการ
๘. หัวหน้ากลุ่มงานเภสัชกรรม	กรรมการ
๙. หัวหน้ากลุ่มงานเทคนิคการแพทย์	กรรมการ
๑๐. หัวหน้ากลุ่มงานประกันสุขภาพ	กรรมการ
๑๑. หัวหน้ากลุ่มงานจิตเวชและยาเสพติด	กรรมการ
๑๒. หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์	กรรมการและเลขานุการ
๑๓. น.ส.กาญจนา เดโช	กรรมการและผู้ช่วยเลขานุการ

บทบาทหน้าที่

๑. พัฒนาการบริการสุขภาพดิจิทัลการแพทย์ทางไกล
๒. พัฒนาระบบการพิสูจน์ ยืนยันตัวตนสำหรับผู้ให้บริการและผู้รับบริการ
๓. เชื่อมข้อมูลระบบสารสนเทศของโรงพยาบาล (HIS) กับระบบ Telemedicine
๔. สื่อสารประชาสัมพันธ์ สร้างความเข้าใจให้ผู้รับบริการ ประชาชน อสม. และบุคลากร

ต่อ...../๕. สร้างเครือข่าย

๕. สร้างเครือข่ายการบริการสามหมอ เช่น อสม. หมอคนที่ ๑ ช่วยผู้สูงอายุเข้ารับบริการการแพทย์ทางไกลผ่าน Application Smart อสม. ที่เชื่อมโยงระบบ Telemedicine
๖. กำกับ ติดตาม การดำเนินงานการบริการสุขภาพดิจิทัลการแพทย์ทางไกลให้เป็นไปตามมาตรฐานของสภาวิชาชีพ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

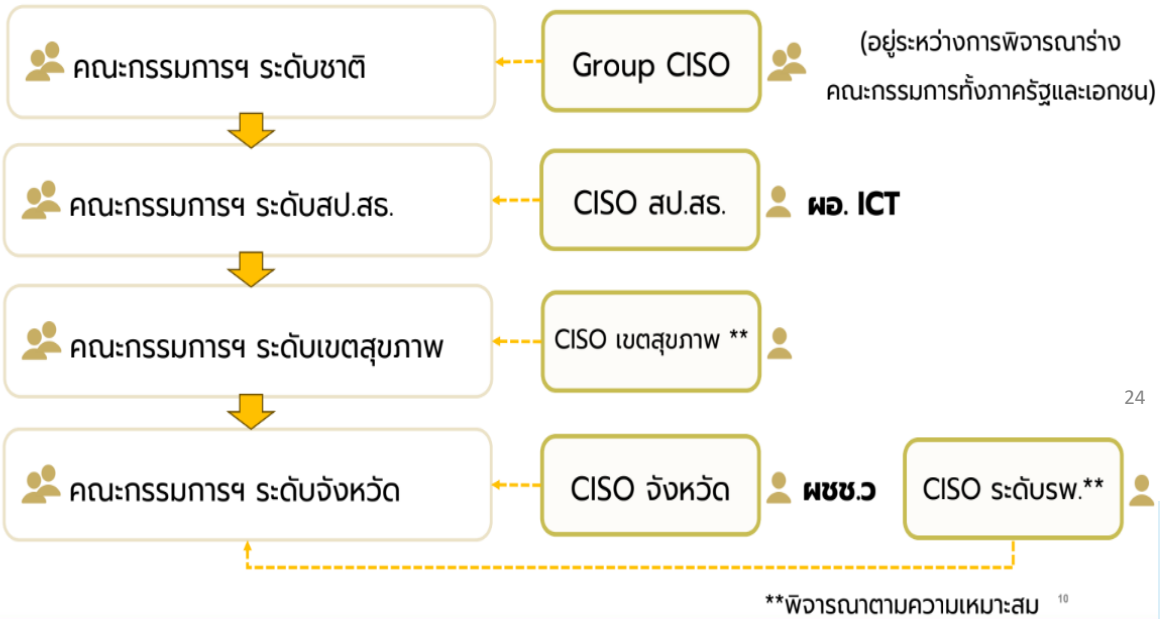
สั่ง ณ วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๖๕

(นายรัตนพล ล้อประเสริฐกุล)
ผู้อำนวยการโรงพยาบาลเกาะสมุย

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

4.7 จัดตั้งคณะกรรมการความปลอดภัยทางไซเบอร์ระดับโรงพยาบาล 10 คะแนน (จำเป็น)

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข



บทบาทและอำนาจหน้าที่ของผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)

1. เป็นจุดประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้คำแนะนำการสื่อสาร การรับรู้ และสนับสนุนการดำเนินงานของหน่วยบริการ
2. สนับสนุนหน่วยบริการในการควบคุมและสอบสวนเหตุการณ์ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยไวเบอร์ และพิจารณายกระดับการตอบโต้แก่กลุ่มผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศระดับสูง
3. สรุปรายงานด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งครอบคลุมเรื่องประสิทธิผล การประเมินความเสี่ยง การลดความเสี่ยง และควบคุมให้เกิดความเสี่ยงน้อยสุด
4. ควบคุมกำกับดูแล ว่าหน่วยบริการได้บริหารจัดการความเสี่ยง การปฏิบัติตามนโยบาย และสนับสนุนการดำเนินการตามมาตรฐานที่กำหนด

มี = คะแนนเต็ม
ไม่มี = 0 คะแนน

THANK YOU FOR YOUR ATTENTION