การพัฒนาแนวทางปฏิบัติเพื่อพัฒนาความมั่นคงปลอดภัย การป้องกันความลับและความเป็นส่วนตัวของข้อมูลส่วนบุคคล สำหรับโรงพยาบาล

วรรษา เปาอินทร์
สมาคมเวชสารสนเทศไทย

ในยุคดิจิทัล โรงพยาบาลทุกแห่งได้นำเทคโนโลยีดิจิทัลมาใช้ขับเคลื่อนบริการหลักของโรงพยาบาล เพื่อทำให้การทำงานมีประสิทธิภาพ ลดค่าใช้จ่าย ลดขั้นตอนซ้ำซ้อน เพิ่มความสะดวกสบายให้แก่ผู้รับบริการ อย่างไรก็ตามการใช้เทคโนโลยีดิจิทัลอาจทำให้เกิดความเสี่ยงเพิ่มขึ้นต่อการเกิดภัยร้ายและอาชญากรรมต่าง ๆ ที่มาทางช่องทางไซเบอร์ (Cybersecurity Risks) อาจเกิดกรณีข้อมูลส่วนบุคคลของผู้มารับบริการและเจ้าหน้าที่ของโรงพยาบาลรั่วไหลออกไปสู่ภายนอกได้ ดังเช่น กรณีการถูกโจมตีเรียกค่าไถ่ จาก ransomeware และการถูก hack แล้วนำข้อมูลออกไปขาย ตามข่าวที่ปรากฏในปี พ.ศ. 2563 - 2564

นอกจากนั้น ตั้งแต่ปี พ.ศ. 2562 ได้มีการประกาศบังคับใช้กฎหมายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โรงพยาบาลจึงควรมีแนวทางปฏิบัติเพื่อทำให้มั่นคงว่าเกิดความมั่นคงปลอดภัยในระบบเทคโนโลยีดิจิทัล และสามารถป้องกันความลับและการรั่วไหลของข้อมูลส่วนบุคคลได้เป็นอย่างดีและเป็นไปตามกฎหมายที่เกี่ยวข้อง

ในเดือนกันยายน พ.ศ. 2564 ราชกิจจานุเบกษา ได้เผยแพร่ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ถือว่าเป็นประกาศฉบับแรก ที่มีรายละเอียดสำหรับการปฏิบัติ ซึ่งได้สรุปไว้ตามลำดับต่อไป

ขั้นตอนที่ต้องปฏิบัติ ประกอบไปด้วยขั้นตอนต่าง ๆ ดังต่อไปนี้

1. การจัดทำทะเบียนทรัพย์สินดิจิทัล (Hardware, software, network) ทั้งหมด รวมถึงข้อมูลที่อยู่ในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล และการให้บริการดิจิทัลจากผู้ให้บริการภายนอก และมีการปรับปรุงบัญชีทะเบียนทุก ๆ 3-6 เดือน เพื่อให้มั่นใจว่าทะเบียนมีข้อมูลเป็นปัจจุบัน

ผู้นิพนธ์ประสานงาน: วรรษา เปาอินทร์, สมาคมเวชสารสนเทศไทย, อาคาร 4 ชั้น 4 ตึกสำนักงานปลัดกระทรวงสาธารณสุข ถ.ติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี 11000, E-mail: wansa@tmi.or.th

2. ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคล ของทรัพย์สินดิจิทัลและข้อมูลทุกรายการ ให้คะแนนความเสี่ยง จัดทำแผนกลยุทธ์จัดการความเสี่ยง จัดทำแผนปฏิบัติการจัดการความเสี่ยง แล้วดำเนินการตามผลประเมินผลการดำเนินการทุก ๆ 6 เดือน – 1 ปี แล้วนำผลการประเมินมาใช้ปรับการดำเนินการพัฒนารอบใหม่ทุก ๆ 1 ปี

3. ดำเนินทดสอบการเจาะระบบทุก ๆ 6 เดือน ถึง 1 ปี โดยใช้บุคคลภายนอกดำเนินการอย่างน้อยปีละ 1 ครั้ง

4. กำหนดแนวทางการให้บริการดิจิทัลจากผู้ให้บริการภายนอก ให้มีแนวทางป้องกันความมั่นคงปลอดภัย และป้องกันข้อมูลส่วนบุคคลในระดับสูงสุด

5. ดำเนินการสร้างความตระหนักรู้ ความเข้าใจด้านภัยไซเบอร์และความสำคัญในการจัดการด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคลให้กับบุคลากรทุกระดับทุกคนในโรงพยาบาล

6. จัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคล 3 ฉบับ สำหรับบุคลากรทั่วไป ผู้ดูแลระบบ และผู้บริหาร ประชาสัมพันธ์ระเบียบ ให้เกิดความรับรู้และความเข้าใจ ของบุคลากรทุกคน กำกับดูแลให้ทุกคน ทำตามระเบียบปฏิบัติอย่างเคร่งครัด กำหนดรางวัลและบทลงโทษอย่างชัดเจน

7. กำหนดให้มีกิจกรรมเฝ้าระวังและตรวจสอบภัยคุกคามทางไซเบอร์ การละเมิดแนวทางปกป้องข้อมูลส่วนบุคคลตลอดเวลา 24 ชั่วโมง ทุก ๆ วัน จัดทำรายการผลการตรวจสอบให้ผู้บริหารระดับสูงได้รับทราบและตอบสนอง ทุก 1 เดือน

8. จัดทำแผนรับมือเมื่อเกิดเหตุการณ์จากภัยไซเบอร์ Cybersecurity Incident Response Plan) รวมถึงแผนการสื่อสารในภาวะวิกฤติ แผนการดำเนินการอย่างต่อเนื่อง (Business Continuity Plan) และแผนกู้คืน (Disaster Recovery Plan) จัดให้มีการฝึกซ้อมแผนทุก ๆ แผน อย่างน้อย 1 ครั้งต่อปี

9. เมื่อมีการเพิ่มเติม ระบบดิจิทัลใหม่ เข้ามา ต้องมีการประเมินความเสี่ยง ช่องโหว่ และจัดการความเสี่ยงให้มั่นใจว่าระบบใหม่จะมีระดับความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคลในระดับสูงเท่ากับระบบเดิม

วันที่รับต้นฉบับ 10 มกราคม 2565, วันที่แก้ไข: 25 มีนาคม 2565, วันที่ตอบรับ: 1 พฤษภาคม 2565

1. การจัดทำทะเบียนทรัพย์สินดิจิทัล

การทำทะเบียน ควรเริ่มด้วยการสำรวจตำแหน่งที่ตั้ง รายละเอียดในแง่มุมต่าง ๆ ของทรัพย์สิน แยกเป็น Hardware, Software, Netware, Data โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าเราได้รับรู้และได้จัดการป้องกันจุดอ่อน ของทรัพย์สินทุกรายการโดยไม่ขาดตกบกพร่อง
(ตัวอย่างทะเบียนทรัพย์สิน)

นอกจากการจัดทำทะเบียนแล้ว ควรปรับปรุงทะเบียนให้ทันสมัยเป็นระยะ ๆ อย่างน้อยปีละ 2 ครั้ง เพื่อให้ทราบสถานะว่าในทะเบียนที่เปลี่ยนแปลงไป จะทำให้ความเสี่ยงเพิ่มขึ้นได้หรือไม่ และอาจทำให้ต้องเพิ่มการจัดการความเสี่ยงตามสถานะในทะเบียนที่เปลี่ยนไป

2. การจัดการความเสี่ยง

การจัดการความเสี่ยง (Risk Management) เป็นกลไกสำคัญ สำหรับการควบคุมคุณภาพระบบงานทุกระบบ เพราะหากเราต้องการให้ระบบงานมีคุณภาพ เราต้องประเมินและตรวจสอบความเสี่ยงที่จะให้ระบบงานของเราด้อยคุณภาพให้ครอบคลุมความเสี่ยงทุกด้าน แล้วจัดการป้องกันไม่ให้ความเสี่ยงเหล่านั้นมีโอกาสมารบกวนและทำให้ระบบงานของเราด้อยคุณภาพลงไปได้

ระบบเทคโนโลยีสารสนเทศโรงพยาบาลก็เป็นระบบหนึ่งที่ต้องใช้การจัดการความเสี่ยงเป็นกลไกสำคัญในการควบคุม เพื่อให้มั่นใจว่าระบบดำเนินไปได้อย่างมีคุณภาพ ดังนั้น ผู้บริหารและผู้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศโรงพยาบาลจึงต้องมีความเข้าใจวิธีการจัดการความเสี่ยงเป็นอย่างดี เพื่อให้สามารถดำเนินการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่ (Vulnerabilities)
2. ภัยคุกคาม (Threats)

จุดอ่อน (Vulnerabilities) หมายถึง ข้อบกพร่องทางด้านกายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคลากร การบริหารจัดการ ครุภัณฑ์ โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีการติดตั้งกุญแจประตูห้องเครื่องแม่ข่าย
- ไม่มีระบบดักจับควัน และระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบเครื่องแม่ข่าย
- ไม่กำหนดขั้นตอนมาตรฐานในการสำรองข้อมูล
- บุคลากรไม่ทำตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีเครื่องแม่ข่ายสำรอง
- ใช้โปรแกรมระบบงานสำคัญร่วมกับโปรแกรมส่วนตัว
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ
- ไม่มีการควบคุมการเข้าถึงข้อมูล สารสนเทศที่สำคัญ

ภัยคุกคาม (Threats) หมายถึง ภัยอันตรายต่างๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่น ๆ อันมีโอกาสจะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังตัวอย่างต่อไปนี้

- ไฟไหม้
- น้ำท่วม
- ขโมย
- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

ความเสี่ยง (Risk) คือความเป็นไปได้หรือโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบ โดยจุดอ่อนของระบบจะเพิ่มโอกาสให้ภัยคุกคามเข้ามาสร้างความเสียหายให้กับระบบเทคโนโลยีสารสนเทศได้ การจัดการความเสี่ยงจึงมีเป้าหมายสำคัญเพื่อ ลดโอกาส ที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบนั่นเอง

ขั้นตอนสำคัญในการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วยขั้นตอนดังต่อไปนี้

1. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)
2. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management Strategic Planning)
3. การดำเนินการจัดการความเสี่ยง (Risks Treatment)

1. การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป

มาตรฐาน ISO/IEC 27001 : 2013 [1] ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS) ได้กล่าวถึงความเสี่ยงในระบบเทคโนโลยีสารสนเทศไว้มากมาย ดังตัวอย่างเช่น

- acts of terrorism การก่อการร้าย
- air conditioning failure ระบบปรับอากาศหยุดทำงาน
- airborne particles/dust ฝุ่นละออง
- bomb attack การวางระเบิด
- breach of legislation or regulations การละเมิดนโยบายและระเบียบปฏิบัติด้านความปลอดภัย
- breaches of contractual obligations การละเมิดข้อตกลงหรือสัญญาที่ผูกพัน

- compromise of security ความย่อหย่อนในระบบรักษาความปลอดภัย
- damage caused by penetration tests ความเสียหายจากการทดลองเจาะเข้าระบบ
- damage caused by third parties ความเสียหายจากบุคคลที่สาม
- destruction of records ข้อมูลถูกทำลาย
- destruction of the business continuity plans แผนกู้คืนถูกทำร้าย
- deterioration of media สื่อที่เก็บข้อมูลเสื่อมสภาพ
- disasters (natural or man-made) ภัยพิบัติ (จากธรรมชาติ หรือจากมนุษย์)
- ฯลฯ

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจากการตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้แบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่พัฒนาโดย สมาคมเวชสารสนเทศไทย [2] (ดูแบบประเมินในหน้าถัดไป) โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

1. โอกาสที่จะเกิดความเสี่ยงนั้น (Probability)
2. ความเสียหายที่จะเกิดขึ้น (Impact)

การคำนวนคะแนนความเสี่ยง

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

ประเมินผลเสียหาย มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

คะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

การประเมินความเสี่ยง โอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1 ต่ำมาก มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก

2 ต่ำ มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี

3 ปานกลาง มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง

4 สูง มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง

5 สูงมาก มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆ สัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

1 ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก

2 ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด

3 ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1-2 แผนก

4 สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก

5 สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

Risk Value			**Probability**				
			Very Low	**Low**	**Medium**	**High**	**Very High**
			1	2	3	4	5
Impact	**Very High**	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล พัฒนาโดยสมาคมเวชสารสนเทศไทย ปี พ.ศ.2556

TMI Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware	1 2 3 4 5	1 2 3 4 5	
1.1 Servers Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.2 Network Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.3 Workstations Failure	1 2 3 4 5	1 2 3 4 5	
1.4	1 2 3 4 5	1 2 3 4 5	
2. IT – System Software	1 2 3 4 5	1 2 3 4 5	
2.1 Operating System Failure	1 2 3 4 5	1 2 3 4 5	
2.2	1 2 3 4 5	1 2 3 4 5	
3. IT – Applications	1 2 3 4 5	1 2 3 4 5	
3.1 Front Offices	1 2 3 4 5	1 2 3 4 5	
3.2 Back Offices	1 2 3 4 5	1 2 3 4 5	
3.3	1 2 3 4 5	1 2 3 4 5	
4. IT – Communications, Connectivity	1 2 3 4 5	1 2 3 4 5	
4.1 Intranet	1 2 3 4 5	1 2 3 4 5	
4.2 Internet	1 2 3 4 5	1 2 3 4 5	
4.3	1 2 3 4 5	1 2 3 4 5	
5. IT – Operational (Human) Error	1 2 3 4 5	1 2 3 4 5	
5.1 Backup Error	1 2 3 4 5	1 2 3 4 5	
5.2 Data Loss Error	1 2 3 4 5	1 2 3 4 5	
5.3	1 2 3 4 5	1 2 3 4 5	
6. IT –Project Failure	1 2 3 4 5	1 2 3 4 5	
6.1 Inappropriate System Analysis	1 2 3 4 5	1 2 3 4 5	
6.2 Inappropriate System Design	1 2 3 4 5	1 2 3 4 5	
6.3 Inadequate Resources	1 2 3 4 5	1 2 3 4 5	
6.4 Poor Project Management	1 2 3 4 5	1 2 3 4 5	
6.5	1 2 3 4 5	1 2 3 4 5	
7. IT –Future Development	1 2 3 4 5	1 2 3 4 5	
7.1 No Data Dictionary	1 2 3 4 5	1 2 3 4 5	
7.2 No System Blueprint	1 2 3 4 5	1 2 3 4 5	
7.3 No Program Document or Comments	1 2 3 4 5	1 2 3 4 5	
7.4	1 2 3 4 5	1 2 3 4 5	
8. IT – Vendor and Outsource Failure	1 2 3 4 5	1 2 3 4 5	
8.1 Vendor Stop Support	1 2 3 4 5	1 2 3 4 5	
8.2	1 2 3 4 5	1 2 3 4 5	
9. IT – Hacking, Unauthorized Intrusions	1 2 3 4 5	1 2 3 4 5	
10. Environment Factors	1 2 3 4 5	1 2 3 4 5	
10.1 Flooding – Internal	1 2 3 4 5	1 2 3 4 5	
10.2 Flooding – External	1 2 3 4 5	1 2 3 4 5	
10.3 Fire – Internal	1 2 3 4 5	1 2 3 4 5	
10.4 Fire – External	1 2 3 4 5	1 2 3 4 5	
10.5 Utilities – Electricity	1 2 3 4 5	1 2 3 4 5	
10.6 Criminal – Theft	1 2 3 4 5	1 2 3 4 5	
10.7 Criminal – Break-ins	1 2 3 4 5	1 2 3 4 5	
10.8 Civil Unrest – Protest, Mob	1 2 3 4 5	1 2 3 4 5	
10.9	1 2 3 4 5	1 2 3 4 5	
11. Other	1 2 3 4 5	1 2 3 4 5	
	1 2 3 4 5	1 2 3 4 5	

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย
เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15
เมื่อคำนวนคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยง

ดังนี้

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เราต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)

2. การวางแผนกลยุทธ์จัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

ความเสี่ยง	คะแนน	แถบสี	ความหมาย
ต่ำ	1 - 3		Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	4 - 9		Tolerable but caution or Management Discretion/Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	10 - 16		Intolerable or Attention Required/High Risk ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	17 - 25		Intolerable or Immediate Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ทันที

เมื่อเสร็จสิ้นขั้นตอนการประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปจะเป็นการวางแผนกลยุทธ์จัดการความเสี่ยง โดยเริ่มการจัดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยงดังนี้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยง เราจะสามารถเรียงลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้ โดย เหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูงมาก (17-25) จะถือว่ามีค่าความเสี่ยงในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้โดยทันที จึงต้องเขียนแผนจัดการความเสี่ยงเหตุการณ์ระดับนี้โดยกำหนดลำดับความสำคัญเป็นลำดับแรก ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูง และปานกลาง จะกำหนดลำดับความสำคัญไว้เป็นลำดับต่อมา

เมื่อกำหนดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้แล้ว ขั้นตอนต่อไป คือการกำหนดวิธีแก้ไขความเสี่ยง (Risk Treatment) ให้กับเหตุการณ์ต่าง ๆ โดยมีทางเลือกกลยุทธ์ในการแก้ไขความเสี่ยง [3] ทั้งหมด 4 กลยุทธ์ดังนี้

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง เป็นการกำหนดมาตรการควบคุมให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง และ/หรือ ร่วมกับมาตรการควบคุมให้ผลเสียหายลดลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. ไฟไหม้เครื่องแม่ข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งเครื่องตัดไฟอัตโนมัติเมื่อเกิดกระแสไฟรั่วหรือกระแสไฟเกินในห้องเครื่องแม่ข่าย 2. เปลี่ยนฝ้าเพดานและผนังห้องเครื่องแม่ข่ายให้เป็นวัสดุไม่ติดไฟ 3. ห้ามสูบบุหรี่ ห้ามนำวัสดุติดไฟง่ายเข้าใกล้เครื่องแม่ข่าย
	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ติดตั้งเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันทีเมื่อเครื่องแม่ข่ายจริงหยุดทำงาน โดยติดตั้งไว้อีกตึกหนึ่งของโรงพยาบาล 2. สำรองข้อมูลลงแถบแม่เหล็กทุกวัน นำแถบแม่เหล็กออกไปเก็บไว้นอกโรงพยาบาล 3. จัดทำแผนกู้คืนเครื่องแม่ข่าย และซ้อมแผนกู้คืนปีละ 2 ครั้ง
2. ไวรัสโจมตีระบบเครือข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. แยกระบบเชื่อมต่ออินเทอร์เน็ตออกจากระบบงานโรงพยาบาล 2. ติดตั้งโปรแกรมสำรวจ ป้องกันและกำจัดไวรัสในระบบเครือข่าย 3. ห้ามผู้ใช้งานระบบ นำ USB Drive มาถ่ายโอนข้อมูลกับเครื่องคอมพิวเตอร์ของโรงพยาบาล
	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ติดตั้งเครือข่ายสำรองที่สามารถกำหนดให้เป็นเครือข่ายจริงได้ทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้เป็นอิสระจากเครือข่ายจริง 2. ทำสัญญากับบริษัทผู้เชี่ยวชาญด้านระบบเครือข่าย ให้ส่งผู้เชี่ยวชาญมาแก้ปัญหาให้ภายใน 4 ชั่วโมง 3. จัดทำแผนดำเนินงานเมื่อระบบเครือข่ายล่ม ซ้อมแผนปีละ 2 ครั้ง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง เป็นการย้ายผลเสียหายที่เกิดขึ้นจากเหตุการณ์ที่ทำให้เกิดความเสี่ยงไปสู่บุคคลอื่น มักใช้ในกรณีที่องค์กรไม่สามารถลดความเสี่ยงได้ หรือไม่คุ้มค่าที่จะลงทุนลดความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. เครื่องคอมพิวเตอร์ถูกขโมย	ย้ายผลเสียหายไปอยู่ในความรับผิดชอบของบริษัทประกันภัย	ทำประกันภัยเครื่องคอมพิวเตอร์ทุกเครื่องจากภัยโจรกรรม
2. เครื่องแม่ข่ายชำรุด	ย้ายกระบวนการกู้คืนเครื่องแม่ข่ายไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญากับบริษัทขายเครื่องแม่ข่ายให้ต้องจัดเครื่องสำรองเตรียมไว้ให้ตลอด 24 ชม. ถ้าเครื่องเสียต้องยกเครื่องสำรองมาทดแทนทันที 2. ทำสัญญาจ้างบริษัทภายนอกให้รับผิดชอบกรณีเครื่องแม่ข่ายชำรุด ต้องรับดำเนินการกู้คืนให้สำเร็จภายใน 1 ชั่วโมง
3. เครื่องพิมพ์เสีย	ย้ายกระบวนการซ่อมและกระบวนการบริการเครื่องพิมพ์ให้พร้อมใช้ไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้บริษัทต้องตั้งเครื่องพิมพ์สำรองพร้อมทดแทนไว้ 5 เครื่อง ถ้ามีเครื่องเสียต้องยกเครื่องอื่นมาให้ใช้แทนได้ภายใน 24 ชั่วโมง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง เป็นการเปลี่ยนแปลงวิธีการทำงาน หรือกำหนดกิจกรรมเพิ่มเติมเพื่อให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. พัฒนาโปรแกรมเสร็จโดยเปล่าประโยชน์ (ผู้ใช้ไม่นำไปใช้งาน)	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ในขั้นตอนวิเคราะห์ความต้องการของผู้ใช้ เพิ่มการทำรายงานผลการวิเคราะห์ความต้องการให้ผู้ใช้ตรวจสอบและรับรอง 2. ในการออกแบบระบบ เพิ่มการทำเอกสารการออกแบบหน้าจอ ขั้นตอนการบันทึกข้อมูล และการทำรายงานให้ผู้ใช้ตรวจสอบ ปรับปรุงแก้ไข และรับรอง
2. เครื่องคอมพิวเตอร์ติดไวรัส	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ปิดการใช้งาน USB Drive 2. ตั้งเวลาให้โปรแกรมสแกนหาไวรัสในเครื่องทุก ๆ วัน ในช่วงเวลาพักรับประทานอาหารกลางวัน
3. เจ้าหน้าที่ลบข้อมูลผิดรายการ	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์ เปลี่ยนแปลงโปรแกรมโดยกำหนดให้ไม่สามารถลบข้อมูลออกจากฐานข้อมูลได้ โดยให้ใช้การยกเลิกข้อมูลที่ผิดพลาดและเพิ่มข้อมูลใหม่ที่ถูกต้องเข้าไปทดแทนได้

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง เป็นการบันทึกผลการวิเคราะห์และยอมรับความเสี่ยงในเรื่องที่มีโอกาสเกิดได้น้อยและ/หรือไม่คุ้มค่าที่จะลงทุนในการจัดการความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. การสูญเสียข้อมูลในฐานข้อมูลและข้อมูลที่สำรองไว้จนหมดในเวลาเดียวกัน	ยอมรับความเสี่ยง	ฐานข้อมูลของโรงพยาบาลและข้อมูลที่สำรองเก็บไว้ที่คนละตึกของโรงพยาบาล ที่ไม่ได้อยู่ในหมู่ตึกเดียวกัน มีระยะห่างกัน 800 เมตร โอกาสที่จะสูญเสียข้อมูลทั้งสองพร้อมกัน เช่น ไฟไหม้ทั้งสองตึก มีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง
2. สายเชื่อมต่ออินเทอร์เน็ตขาดการเชื่อมต่อพร้อมกันทั้ง 2 สาย	ยอมรับความเสี่ยง	การเชื่อมต่ออินเทอร์เน็ตของโรงพยาบาลมี 2 จุด เชื่อมต่อคือบริษัท A และบริษัท B โอกาสที่จุดเชื่อมต่อ 2 จุด จะขาดการเชื่อมต่อพร้อมกันมีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง

3. การดำเนินการจัดการความเสี่ยง

การดำเนินการจัดการความเสี่ยงเริ่มจากการจัดสรรทรัพยากร บุคคล เงิน และเวลา ที่ต้องใช้ในการจัดการความเสี่ยงแต่ละเรื่อง โดยอาจจัดทำเป็นโครงการ และใช้การจัดการโครงการ (Project Management) เป็นเครื่องมือช่วยให้การดำเนินการจัดการความเสี่ยงประสบผลสำเร็จต่อไป โดยอาจใช้แผนกิจกรรมจัดการความเสี่ยง ดังตัวอย่างในหน้าถัดไป เป็นเครื่องมือในการติดตามและควบคุมการดำเนินการจัดการความเสี่ยง

การประเมินผลและการพัฒนาคุณภาพอย่างต่อเนื่อง

เมื่อหน่วยงานดำเนินการจัดการความเสี่ยงไปแล้ว ควรมีการประเมินผลกิจกรรมจัดการความเสี่ยงที่ได้ดำเนินการไปแล้วว่าได้ผลหรือไม่ทุก ๆ 3-6 เดือน โดยการเก็บข้อมูลอุบัติการณ์ต่าง ๆ อันเป็นเหตุการณ์ที่ทำให้เกิดความเสี่ยงทุกรายการ ทำสถิติอุบัติการณ์ และวิเคราะห์แนวโน้มการเปลี่ยนแปลงว่ามีการเปลี่ยนแปลงไปในทางที่ดีขึ้นหรือไม่ โดยต้องประเมินคะแนนความเสี่ยงใหม่ เพื่อตรวจสอบว่าคะแนนความเสี่ยงลดลงหรือไม่ ถ้าพบว่าแนวโน้มดีขึ้น ย่อมแสดงว่ากิจกรรมจัดการ

ความเสี่ยงที่ได้ดำเนินมาแล้วเป็นไปอย่างถูกต้องสมควร แต่หากแนวโน้มความเสี่ยงใดไม่ลดลง หรือเพิ่มขึ้น ก็สมควรปรับแก้ไขหรือเพิ่มกิจกรรมจัดการความเสี่ยง ให้ดีขึ้นกว่าเดิมอย่างต่อเนื่อง

3. ดำเนินทดสอบการเจาะระบบทุก ๆ 6 เดือน ถึง 1 ปี โดยใช้บุคคลภายนอกดำเนินการอย่างน้อยปีละ 1 ครั้ง

การทดสอบการเจาะระบบ (Penetration Test) เป็นการใช้ทีมงานผู้ชำนาญการเจาะระบบทดลองเจาะเข้าสู่ระบบเทคโนโลยีสารสนเทศของโรงพยาบาล โดยเฉพาะระบบที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) โดยการทดสอบการเจาะระบบครอบคลุมระบบของเครื่องแม่ข่าย เครือข่าย และโปรแกรมระบบบริการที่สำคัญของโรงพยาบาล

การทดสอบการเจาะระบบ อาจดำเนินการโดยทีมผู้ตรวจสอบภายใน โดยกำหนดให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือดำเนินการเมื่อมีการปรับเปลี่ยนระบบใหม่ เช่น การเพิ่มโมดูลใหม่ การปรับเปลี่ยนเทคโนโลยี และต้องจัดให้มีการทดสอบการเจาะระบบจากผู้ทดสอบภายนอก ที่ได้รับการรับรองและได้รับประกาศนียบัตรอันเป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบของโรงพยาบาล

การทดสอบการเจาะระบบทั้งหมดต้องดำเนินการภายใต้การดูแลของเจ้าหน้าที่โรงพยาบาลโดยเคร่งครัด และเมื่อทราบผลการทดสอบเจาะระบบแล้ว ก็ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

4. กำหนดแนวทางการให้บริการดิจิทัลจากผู้ให้บริการภายนอกให้มีแนวทางป้องกันความมั่นคงปลอดภัย และป้องกันข้อมูลส่วนบุคคลในระดับสูงสุด

ในบางกรณี โรงพยาบาลอาจต้องใช้บริการจากผู้ให้บริการภายนอก เช่น การเช่าใช้ระบบ PACS (Picture Archiving and Communication System) จากบริษัทภายนอก กรณีนี้ โรงพยาบาลต้องรับผิดชอบและดูแลให้มั่นใจว่าบริษัทภายนอกมีการรักษาความมั่นคงปลอดภัยของระบบในระดับสูงสุด

ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บการสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของบริษัทภายนอก ไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement)

ข้อกำหนดที่ตกลงในเงื่อนไขสัญญากับบริษัทภายนอกจะต้องมีรายละเอียดอย่างน้อยได้แก่ ประเภทของบริษัทภายนอกและโปรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัย ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการจากภัยคุกคามทางไซเบอร์ ความเสี่ยงที่เกี่ยวข้องกับบริการ และสิทธิของโรงพยาบาลในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของบริษัทภายนอก

5. ดำเนินการสร้างความตระหนักรู้ ความเข้าใจด้านภัยไซเบอร์และความสำคัญในการจัดการด้านความมั่นคงปลอดภัย และการปกป้องข้อมูลส่วนบุคคลให้กับบุคลากรทุกระดับ ทุกคนในโรงพยาบาล

ในโรงพยาบาลแต่ละแห่ง มีบุคลากรจำนวนมาก และมีงานในภาระหน้าที่ในการดูแลรักษาผู้ป่วยเป็นหลัก บุคลากรเหล่านี้ส่วนใหญ่จะไม่ค่อยตระหนักรู้และเข้าใจด้านภัยไซเบอร์และความสำคัญในการจัดการด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคล จึงต้องมีกิจกรรมสร้างความตระหนักรู้ให้กับบุคลากรทุกคน

ทีมพัฒนาคุณภาพของโรงพยาบาลจึงควรจัดทำแผนงานในการสร้างความตระหนักรู้ แล้วจัดกิจกรรมประชาสัมพันธ์ให้กับบุคลากรทุกคน และวางแผนจัดกิจกรรมให้กับบุคลากรที่เข้าใหม่ทุก ๆ ปี ปีละอย่างน้อย 1 ครั้ง กิจกรรมประชาสัมพันธ์นี้ควรรวมการให้ความรู้เกี่ยวกับระเบียบปฏิบัติต่าง ๆ ด้วย

6. จัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคล 3 ฉบับ สำหรับบุคลากรทั่วไป ผู้ดูแลระบบและผู้บริหาร ประชาสัมพันธ์ระเบียบ ให้เกิดความรับรู้ และความเข้าใจ ของบุคลากรทุกคน กำกับดูแลให้ทุกคน ทำตามระเบียบปฏิบัติอย่างเคร่งครัด กำหนดรางวัลและบทลงโทษอย่างชัดเจน

นโยบายด้านความมั่นคงปลอดภัย เป็นแนวทางที่ผู้บริหารระดับสูงกำหนดทิศทางการดำเนินงานเพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศนโยบายฉบับนี้จึงเป็นการแสดงเจตจำนงค์ให้ทุกฝ่ายที่เกี่ยวข้องกับโรงพยาบาล ไม่ว่าจะเป็นผู้ป่วย ญาติผู้ป่วย เจ้าหน้าที่ทุกฝ่ายในโรงพยาบาล ตลอดจนคู่สัญญาภายนอกของโรงพยาบาลได้รับรู้แนวทางและจุดยืนของโรงพยาบาล

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล ได้แก่

- โรงพยาบาล จะดำเนินการจัดการเพื่อป้องกันความลับและความเป็นส่วนตัวของผู้ป่วยอย่างเคร่งครัด
- โรงพยาบาลมีนโยบายใช้ซอฟท์แวร์ที่ไม่ละเมิดลิขสิทธิ์เท่านั้น
- การใช้ทรัพยากรเทคโนโลยีสารสนเทศของโรงพยาบาลต้องเป็นไปเพื่อการดำเนินกิจกรรมตามพันธกิจและภารกิจของโรงพยาบาลเท่านั้น

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัย เป็นข้อกำหนดที่ให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตาม เพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศระเบียบปฏิบัติจึงเป็นสิ่งที่เจ้าหน้าที่ทุกคนต้องรับรู้ และปฏิบัติตามโดยเคร่งครัด โดยหากไม่ปฏิบัติตามควรมีมาตรฐาน

ตักเตือนหรือลงโทษตามสมควร

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

- (เจ้าหน้าที่ทุกคน) ต้องเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
- ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลเพื่อความบันเทิง เช่น ดูหนัง ฟังเพลง เล่นเกมส์ ฯลฯ
- ห้ามติดตั้งโปรแกรมใดๆเพิ่มเติมลงในเครื่องคอมพิวเตอร์ของโรงพยาบาล หากมีความจำเป็นให้ขออนุมัติจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายหน้าที่จากผู้อำนวยการเท่านั้น

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลสามารถแบ่งกลุ่มตามลักษณะผู้ใช้ได้ 3 กลุ่มดังนี้

1. ระเบียบปฏิบัติสำหรับผู้บริหาร (ระดับสูง ระดับกลาง ระดับต้น)
2. ระเบียบปฏิบัติสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ
3. ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน

ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน เป็นระเบียบที่สำคัญที่สุด เพราะต้องบังคับใช้กับบุคคลหมู่มาก จึงต้องเขียนโดยใช้ข้อความที่ชัดเจน ไม่กำกวม เข้าใจได้ง่าย ไม่ตีความบิดเบือนเป็นอย่างอื่นได้

ทั้งนโยบายและระเบียบปฏิบัติ ควรจัดทำเป็นประกาศของโรงพยาบาล โดยผู้อำนวยการลงนามและประกาศให้ผู้ที่เกี่ยวข้องทุกคนได้รับรู้โดยทั่วกัน โดยเมื่อประกาศใช้งานไปแล้ว สามารถทบทวนและปรับปรุงแก้ไขให้ทันสมัยหรือเหมาะสมต่อสถานการณ์ในอนาคตได้ต่อไป

การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติไปสู่ผู้ใช้ระบบทุกคน

เมื่อมีการประกาศนโยบายและระเบียบปฏิบัติออกมาแล้ว ต้องมีการประชาสัมพันธ์ให้มั่นใจว่า ผู้ใช้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลทุกคน ได้รับรู้ระเบียบปฏิบัติฉบับที่สำคัญที่สุด คือระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน กิจกรรมประชาสัมพันธ์เป็นกิจกรรมที่สำคัญมาก เพราะการประกาศเรื่องราวใด ๆ ในโรงพยาบาลตามช่องทางปกติมักจะไม่สามารถสื่อสารไปสู่บุคลากรหมู่มากของโรงพยาบาลได้ โรงพยาบาลหลายแห่งใช้ช่องทางเครือข่ายภายใน (Intranet) เพื่อนำประกาศต่าง ๆ ไปใส่ไว้ แต่เรามักจะพบว่า เจ้าหน้าที่โรงพยาบาลส่วนใหญ่จะไม่สนใจอ่านประกาศต่าง ๆ เหล่านั้น ดังนั้น หากนำระเบียบปฏิบัติที่สำคัญนี้ไปประกาศไว้ในช่องทางปกติ เจ้าหน้าที่ส่วนใหญ่จะยังคงไม่รับรู้ว่ามีระเบียบนี้ให้ปฏิบัติตาม

การประชาสัมพันธ์ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสำหรับผู้ใช้งานระบบทุกคน ควรใช้ช่องทางประชาสัมพันธ์หลายช่องทาง โดยช่องทางประชาสัมพันธ์ที่อาจเลือกใช้ ได้แก่

1. ประกาศตามช่องทางประชาสัมพันธ์ปกติของโรงพยาบาล เช่น บอร์ดติดประกาศ Intranet ฯลฯ
2. จัดทำเป็นโปสเตอร์ ทำไปติดไว้ในสถานที่ที่เจ้าหน้าที่ของโรงพยาบาลมองเห็นได้โดยง่าย
3. จัดอบรมเจ้าหน้าที่ นำเสนอระเบียบปฏิบัติ เปิดโอกาสให้ซักถาม อภิปรายร่วมกัน
4. มอบหมายให้หัวหน้าหน่วยงาน นำระเบียบไปแจ้งในที่ประชุมหน่วยงานให้เจ้าหน้าที่ทุกคนทราบ

ในกรณีที่ ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคนมีข้อปฏิบัติมากเกินกว่า 1 หน้ากระดาษ เช่น มีข้อปฏิบัติ 30-50 ข้อ ควรคัดเลือกระเบียบปฏิบัติที่สำคัญที่สุด มาจัดทำเป็นหน้าเดียวดังตัวอย่างในภาพที่ 1

ประกาศโรงพยาบาล[redacted]
เรื่อง ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐
(ฉบับผู้ใช้งานทั่วไป)

.....

ข้อ ๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

ข้อ ๒ ผู้ใช้งานห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก เช่น Flash Drive , External Drive , CD-Rom เป็นต้น กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย HOSxP, X-Ray และ Lab ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานห้ามทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔ ห้ามผู้ใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๕ ผู้ใช้งานห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖ ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook), ไลน์ (Line), เว็บไซต์ (Website) หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยหรือญาติซึ่งยินยอมเผยแพร่ได้เป็นครั้งคราว

ข้อ ๗ ผู้ใช้งานต้องรับผิดชอบป้องกันความเสียหาย ที่อาจจะเกิดขึ้น กับเครื่องคอมพิวเตอร์ , ปริ้นเตอร์, ปลั๊กไฟ หรืออุปกรณ์อิเลคทรอนิกส์ เช่น ไม่วางอาหารหรือน้ำดื่ม บนเครื่องคอมพิวเตอร์ ,ไม่ใช้งานปลั๊กที่ไฟชำรุด เป็นต้น

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศใช้ ณ วันที่ พฤศจิกายน พ.ศ.๒๕๖๐

ภาพที่ 1 ตัวอย่าง ระเบียบปฏิบัติฉบับคัดเลือกข้อปฏิบัติให้เหลือเนื้อหาอยู่ในหน้าเดียว

การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประชาสัมพันธ์ระเบียบปฏิบัติไปสู่ผู้ใช้ระบบแล้ว ต้องมีกระบวนการประเมินความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน เพื่อให้ทราบว่า การประชาสัมพันธ์ระเบียบนั้นได้ผลมากน้อยเพียงใด โดยก่อนการประเมินจะต้องรวบรวมข้อมูลจากผู้ดูแลระบบมาให้ครบถ้วนเสียก่อนว่าผู้ใช้งานระบบมีทั้งหมดกี่คน ทำงานอยู่ในหน่วยงานใดบ้าง เพื่อจะได้ดำเนินการประเมินได้ครบทุกคน

วิธีการประเมินความรับรู้ระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์หรือการให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความรับรู้เสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความรับรู้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 499 คน คิดเป็นร้อยละ 99.80

การรับรู้ระเบียบ

ข้อที่ 1	รู้ 400 คน ไม่รู้ 99 คน	การรับรู้คิดเป็นร้อยละ 80.16
ข้อที่ 2	รู้ 450 คน ไม่รู้ 49 คน	การรับรู้คิดเป็นร้อยละ 90.18
ข้อที่ 3	รู้ 420 คน ไม่รู้ 79 คน	การรับรู้คิดเป็นร้อยละ 84.17
ข้อที่ 4	รู้ 350 คน ไม่รู้ 149 คน	การรับรู้คิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่รับรู้มากที่สุดคือข้อที่ 2 ข้อที่ไม่รับรู้มากที่สุดคือข้อที่ 4

สาเหตุที่ไม่รู้ระเบียบ เป็นเพราะไม่ได้อ่านโดยละเอียด อ่านแล้วจำไม่ได้ ขาดสมาธิตอนเข้ารับการอบรม หรือ เข้ารับการอบรมไม่ครบทุกหัวข้อ

เสนอแนะแนวทางแก้ไข

เพิ่มการให้ความรู้แก่บุคลากรที่ยังขาดความรู้ด้านระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การรับรู้ทุกหัวข้อ มีสัดส่วนการรับรู้ไม่ต่ำกว่า ร้อยละ 95

การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประเมินความรับรู้แล้ว ต้องมีกระบวนการประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน ด้วย เพื่อให้ทราบว่าผู้ใช้ระบบเข้าใจระเบียบแต่ละข้ออย่างถูกต้องหรือไม่ เพราะบางครั้ง ผู้ใช้อาจจะเข้าใจความหมายของระเบียบปฏิบัติแต่ละข้อไม่ถูกต้อง วิธีการประเมินความเข้าใจระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือการให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความเข้าใจเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความเข้าใจระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100

ความเข้าใจระเบียบ

ข้อที่ 1	เข้าใจ 400 คน ไม่เข้าใจ 99 คน	ความเข้าใจคิดเป็นร้อยละ 80.16
ข้อที่ 2	เข้าใจ 450 คน ไม่เข้าใจ 49 คน	ความเข้าใจคิดเป็นร้อยละ 90.18
ข้อที่ 3	เข้าใจ 420 คน ไม่เข้าใจ 79 คน	ความเข้าใจคิดเป็นร้อยละ 84.17
ข้อที่ 4	เข้าใจ 350 คน ไม่เข้าใจ 149 คน	ความเข้าใจคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่เข้าใจมากที่สุดคือข้อที่ 2 ข้อที่ไม่เข้าใจมากที่สุดคือข้อที่ 4

สาเหตุที่ไม่เข้าใจระเบียบ เป็นเพราะอ่านไม่รู้เรื่อง ไม่เข้าใจศัพท์ที่ใช้ ความหมายกำกวม

เสนอแนะแนวทางแก้ไข

ปรับปรุงแก้ไขข้อความที่ทำให้อ่านไม่รู้เรื่อง เพิ่มการอธิบายแก่บุคลากรที่ยังไม่เข้าใจระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้ความเข้าใจทุกหัวข้อ มีสัดส่วนความเข้าใจไม่ต่ำกว่า ร้อยละ 95

การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

ถ้าผลการประเมินการรับรู้และความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน ยังไม่เป็นที่น่าพอใจ ต้องพิจารณาว่าสาเหตุที่ทำให้ผู้ใช้ระบบไม่รับรู้หรือไม่เข้าใจระเบียบเกิดจากอะไร เพื่อจะได้ดำเนินการแก้ไขให้ถูกทาง เช่น ระเบียบที่ประกาศใช้ไปแล้วมีบางข้อที่ผู้ใช้อ่านไม่รู้เรื่อง ก็ควรปรับปรุงข้อความให้อ่านแล้วเข้าใจได้โดยง่าย หรือ ผู้ใช้ระบบจำระเบียบไม่ได้เพราะการอบรมมีเนื้อหามากเกินไป ก็ควรปรับปรุงวิธีการอบรมให้ดีขึ้นกว่าเดิม

การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติ ทำได้หลายวิธี เช่น การให้ความรู้ซ้ำหลายๆครั้ง เปลี่ยนช่องทางการให้ข้อมูล หรือเพิ่มช่องทางการให้ข้อมูล กำหนดมาตรการให้รางวัลแก่ผู้ที่สนใจและรับรู้ระเบียบได้อย่างดี ฯลฯ

การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อมั่นใจว่าผู้ใช้ระบบทุกคน มีความรู้และความเข้าใจระเบียบปฏิบัติเป็นอย่างดีแล้ว ก็ควรติดตามประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย เพราะถึงแม้จะมีความรู้และความเข้าใจเรื่องระเบียบแล้ว แต่บางคนก็ยังคงไม่ปฏิบัติตามระเบียบ ทีมงานพัฒนาคุณภาพจึงต้องสร้างระบบตรวจสอบประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย

วิธีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศของโรงพยาบาล สามารถดำเนินการได้หลายวิธี ได้แก่

1. แบบประเมินตนเอง ให้ผู้ใช้ระบบตอบคำถามว่า ระเบียบข้อใดบ้างที่ปฏิบัติตาม ระเบียบข้อใดที่ไม่ปฏิบัติ สาเหตุที่ทำให้ไม่ปฏิบัติตามระเบียบคืออะไร ฯลฯ การให้ตอบแบบประเมินตนเองนี้ มีข้อดีตรงที่ทำได้โดยง่าย และใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่นได้ แต่ข้อเสียของการประเมินด้วยวิธีนี้คือ การที่ผู้ประเมินตนเองอาจประเมินไม่ตรงตามการปฏิบัติจริง

2. การสังเกตโดยตรงจากผู้ประเมิน วิธีนี้ผู้ประเมินจะเข้าไปสังเกตวิธีปฏิบัติงานของผู้ใช้ระบบโดยตรง โดยอาจไม่บอกให้รู้ล่วงหน้าว่าจะมีการเข้าประเมิน การประเมินแบบนี้มีข้อดีตรงที่ได้ข้อมูลเหตุการณ์การละเมิดระเบียบปฏิบัติที่เกิดขึ้นจริง ส่วนข้อเสียคืออาจไม่สามารถประเมินด้วยวิธีนี้ได้ทุกหัวข้อของระเบียบที่ประกาศไป

3. การจำลองสถานการณ์ เป็นการสร้างสถานการณ์เพื่อทดสอบว่า ผู้ใช้ระบบปฏิบัติตามระเบียบปฏิบัติได้ตรงตามที่กำหนดไว้ เช่น มีระเบียบปฏิบัติให้ผู้ใช้ระบบต้อง log off จากระบบเมื่อไม่ได้ใช้งาน ก็อาจจะลองโทรศัพท์เรียกใช้ผู้ใช้ระบบให้ออกไปจากหน้าจอแล้วสังเกตดูว่า ผู้ใช้ระบบ log off จากระบบหรือไม่ การจำลองสถานการณ์มีข้อดี คือ ใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่น ๆ แต่มีข้อเสียคือต้องใช้บุคลากรในการประเมินหลายคน และเสียเวลาในการประเมินมาก

การประเมินผลการปฏิบัติตามระเบียบปฏิบัตินี้ ควรกำหนดให้มีการประเมินโดยสม่ำเสมอ เช่น ทุก ๆ 1 - 3 เดือน เพื่อคอยติดตามสถานการณ์ว่า เกิดการละเมิดระเบียบปฏิบัติมากน้อยแค่ไหน หากเกิดการละเมิดระเบียบปฏิบัติเป็นจำนวนมาก ควรค้นหาสาเหตุและหาทางแก้ไขปัญหาโดยเร่งด่วน

เมื่อประเมินการปฏิบัติตามระเบียบปฏิบัติเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100
ความปฏิบัติตามระเบียบ

ข้อที่ 1	ปฏิบัติ 400 คน ไม่ปฏิบัติ 99 คน	การปฏิบัติตามคิดเป็นร้อยละ 80.16
ข้อที่ 2	ปฏิบัติ 450 คน ไม่ปฏิบัติ 49 คน	การปฏิบัติตามคิดเป็นร้อยละ 90.18
ข้อที่ 3	ปฏิบัติ 420 คน ไม่ปฏิบัติ 79 คน	การปฏิบัติตามคิดเป็นร้อยละ 84.17
ข้อที่ 4	ปฏิบัติ 350 คน ไม่ปฏิบัติ 149 คน	การปฏิบัติตามคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่ปฏิบัติตามมากที่สุดคือข้อที่ 2 ข้อที่ละเมิดมากที่สุดคือข้อที่ 4

สาเหตุที่ละเมิดระเบียบ เป็นเพราะไม่สนใจที่จะทำตาม ไม่ตระหนักถึงความสำคัญที่จะต้องดำเนินการตามระเบียบ

เสนอแนะแนวทางแก้ไข

ให้รางวัลแก่บุคลากรที่สามารถปฏิบัติตามระเบียบปฏิบัติได้เป็นอย่างดี กำหนดมาตรการลงโทษผู้ที่ละเมิดระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การปฏิบัติตามระเบียบทุกหัวข้อ มีสัดส่วนการปฏิบัติไม่ต่ำกว่า ร้อยละ 95

7. กำหนดให้มีกิจกรรมเฝ้าระวังและตรวจสอบภัยคุกคามทางไซเบอร์ การละเมิดแนวทางปกป้องข้อมูลส่วนบุคคล ตลอดเวลา 24 ชั่วโมง ทุก ๆ วัน จัดทำรายการผลการตรวจสอบให้ผู้บริหารระดับสูงได้รับทราบและตอบสนอง ทุก 1 เดือน

ทีมพัฒนาคุณภาพต้องกำหนดให้มีกิจกรรมเฝ้าระวังและตรวจสอบภัยคุกคามทางไซเบอร์ สร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และการละเมิดแนวทางปกป้องข้อมูลส่วนบุคคลทั้งหมด เช่น ระบบรายการอุบัติการณ์ (Incident Report) และต้องนำอุบัติการณ์ที่เกิดขึ้นมาวิเคราะห์ จัดประเภท เพื่อนำมาปรับปรุงกระบวนการให้ดีขึ้น และรายการผลการตรวจสอบนำเสนอให้ผู้บริหารระดับสูงได้รับทราบและตอบสนองทุกเดือน

ต้องดำเนินการทบทวนกลไกและกระบวนการตรวจจับและเฝ้าระวังดังกล่าว อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

8. จัดทำแผนรับมือเมื่อเกิดเหตุการณ์จากภัยไซเบอร์ (Cybersecurity Incident Response Plan) รวมถึงแผนการสื่อสารในภาวะวิกฤต แผนการดำเนินการอย่างต่อเนื่อง (Business Continuity Plan) และแผนกู้คืน (Disaster Recovery Plan) จัดให้มีการฝึกซ้อมแผนทุก ๆ แผน อย่างน้อย 1 ครั้งต่อปี

ต้องมีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ แล้วสื่อสารแผนฝึกซ้อม อย่างน้อยปีละ 1 ครั้ง ประเมินผลการฝึกซ้อม แล้วนำผลการประเมินมาทบทวนปรับปรุง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จัดตั้งทีมสื่อสารในภาวะวิกฤต ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง ระบุกลุ่มเป้าหมาย ผู้มีส่วนได้ส่วนเสีย โฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของโรงพยาบาลเมื่อกล่าวแถลงกับสื่อมวลชนและระบุช่องทางการเผยแพร่ที่เหมาะสม

ต้องจัดทำแผนการดำเนินการอย่างต่อเนื่อง และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ จัดให้มีการซ้อมการดำเนินงานตามแผน ประเมินผลการซ้อม แล้วนำผลมาทบทวน ปรับปรุงแผนและกระบวนการให้ดีขึ้นอย่างน้อยปีละ 1 ครั้ง

9. เมื่อมีการเพิ่มเติม ระบบดิจิทัลใหม่ เข้ามา ต้องมีการประเมินความเสี่ยง ช่องโหว่ และจัดการความเสี่ยงให้มั่นใจว่าระบบใหม่จะมีระดับความมั่นคงปลอดภัยและการปกป้องข้อมูลส่วนบุคคลในระดับสูงเท่ากับระบบเดิม

ต้องจัดทำกระบวนการจัดการการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเพิ่มเติมระบบใหม่เข้ามา และต้องมีการประเมินช่องโหว่และจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมให้เรียบร้อยเสียก่อนที่จะทำการเพิ่มเติมระบบใหม่เข้ามา

เอกสารอ้างอิง

[1.] ISO/IEC 27001:2013, Information technology -- Security techniques – Information security management systems – Requirements. (2013). Retrieved November 2, 2013, from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[2.] สมาคมเวชสารสนเทศไทย. (2556). แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล. นนทบุรี. สมาคมเวชสารสนเทศไทย.

[3.] จิรพร สุเมธีประสิทธิ์, มัทธนา พิพิธเนาวรัตน์ และ กิตติพันธ์ คงสวัสดิ์เกียรติ. (2556). การบริหารความเสี่ยงอย่างมืออาชีพ. กรุงเทพ. สำนักพิมพ์แมคกรอ-ฮิล.

[4.] Brown, Carol. (2012). Managing Information Technology, 7th Edition. New Jersey: Prentice Hall.

[5.] ราชกิจจานุเบกษา (2564) เล่ม 138 ตอนพิเศษ 208 ง หน้า 9. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

[6.] ชุษณะ มะกรสาร, วรรษา เปาอินทร์ บรรณาธิการ. (2561). แนวทางการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลตาม Thai Medical Informatics – TMI Hospital IT Maturity Model. สมาคมเวชสารสนเทศไทย