การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ (Hospital IT Risk Management)
โรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

กระบวนการบริหารความเสี่ยง เป็น กระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกลุ่มงานสารสนเทศทางการแพทย์ มีขั้นตอนหรือกระบวนการบริหารความเสี่ยง ๖ ขั้นตอนหลัก ดังนี้

การระบุความเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงาน ร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยง โดยต้องคำนึงถึงความเสี่ยงที่มีสาเหตุมาจากปัจจัยทั้งภายในและภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายขององค์กร หรือผลการปฏิบัติงานทั้งในระดับองค์กรและกิจกรรม ในการระบุปัจจัยเสี่ยงจะต้องพิจารณาว่ามีเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาด ความเสียหายและไม่บรรลุวัตถุประสงค์ที่กำหนด รวมทั้งมีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา ดังนั้นจึงจำเป็นต้องเข้าใจในความหมายของ “ความเสี่ยง (Risk)” “ปัจจัยเสี่ยง (Risk Factor)” และ “ประเภทความเสี่ยง” ก่อนที่จะดำเนินการระบุความเสี่ยงได้อย่างเหมาะสม

๑.๑ ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักขององค์กร และเป้าหมายตามแผนปฏิบัติงาน

๑.๒ ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นตอ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง โดยปัจจัยเสี่ยงแบ่งได้ ๒ ด้าน ดังนี้

- ปัจจัยเสี่ยงภายนอก คือ ความเสี่ยงที่ไม่สามารถควบคุมการเกิดได้โดยองค์กร เช่น เศรษฐกิจสังคม การเมือง กฎหมาย คู่แข่ง เทคโนโลยี ภัยธรรมชาติ สิ่งแวดล้อม

- ปัจจัยเสี่ยงภายใน คือ ความเสี่ยงที่สามารถควบคุมได้โดยองค์กร เช่น กฎระเบียบ ข้อบังคับภายในองค์กร วัฒนธรรมองค์กร นโยบายการบริหารและการจัดการ ความรู้/ความสามารถของบุคลากรกระบวนการ ท างาน ข้อมูล/ระบบสารสนเทศ เครื่องมือ/อุปกรณ์

๑.๓ ประเภทความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา สามารถแยกประเภทความเสี่ยงเป็น ๕ ประเภท ดังนี้

- ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ Hardware, Software, Network, Data

- ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการรักษาผู้ป่วย ทำให้ข้อมูลผิดพลาดไม่ถูกต้องตรงกัน ข้อมูลที่สำคัญไม่อยู่ระบบ ข้อมูลที่จำเป็นและสำคัญไปถึงผู้ป่วยหรือผู้ให้บริการล่าช้าจนทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง, ข้อมูลไม่ครบถ้วน ขาดหาย, ข้อมูลไปถึงผู้ป่วยล่าช้า, ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน, การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น

- ความเสี่ยงด้นความเป็นส่วนตัวของผู้ป่วย เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยี

สารสนเทศของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษาเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศ ได้รับความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

- ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

- ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ

ขั้นตอนการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วย ขั้นตอนดังต่อไปนี้

๑. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)

๒. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management Strategic Planning)

๓. การดำเนินการจัดการความเสี่ยง (Risks Treatment)

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป มาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ [๑] ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS)

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจาก การตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้แบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

๑. โอกาสที่จะเกิดความเสี่ยงนั้น (Probability)

๒. ความเสียหายที่จะเกิดขึ้น (Impact)

การคำนวณคะแนนความเสี่ยง

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่า ๑ (ต่ำมาก) ๒ (ต่ำ) ๓ (ปานกลาง) ๔ (สูง) ๕ (สูงมาก)

ประเมินผลเสียหาย มีค่า ๑ (ต่ำมาก) ๒ (ต่ำ) ๓ (ปานกลาง) ๔ (สูง) ๕ (สูงมาก)

คะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = ๓ ผลเสียหาย = ๕ ดังนั้น คะแนนความเสี่ยง = ๓x๕ = ๑๕
การประเมินความเสี่ยง โอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ ๑-๕ ดังนี้
ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

๑ ต่ำมาก มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้หรือมีโอกาสเกิดได้น้อยมาก
๒ ต่ำ มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ ๑ ปี
๓ ปานกลาง มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ ๑ ครั้ง
๔ สูง มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
๕ สูงมาก มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์
ประเมินผลเสียหาย มีค่าได้เป็น
๑ ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
๒ ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
๓ ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน ๑-๒ แผนก
๔ สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล ๓-๔ แผนก
๕ สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

การประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล (Risk analysis worksheet)

แบบประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ ปี ๒๕๖๕			
สถานการณ์	โอกาส/ความถี่ (P)	ผลกระทบ (I)	PxI=Risk
๑. Hard Ware			
๑.๑ Server' Crash or Failure	๒	๕	๑๐
๑.๒ Network Switches Crash or Failure	๒	๓	๖
๑.๓ Workstations Failure	๒	๔	๘
๒. Soft Ware			
๒.๑ Operating System Failure	๓	๕	๑๕
๓. Application			
๓.๑ Front Offices	๒	๓	๖๖
๓.๒ Back Offices	๑	๕	๕
๔. Communication, Connectivity			
๔.๑ Intranet	๕	๔	๒๐
๔.๒ Internet	๕	๔	๒๐
๕. Operational (Human) Error			
๕.๑ Backup Error	๒	๔	๘
๕.๒ Data Loss Error	๒	๔	๘
๖. Project Failure			
๖.๑ Inappropriate System Analysis	๒	๓	๖
๖.๒ Inappropriate System Design	๒	๓	๖
๖.๓ Inadequate Resources	๓	๓	๙
๖.๔ Poor Project Management	๒	๒	๔
๗. Future Development			
๗.๑ No Data Dictionnary	๓	๒	๖
๗.๒ No System Blueprint	๔	๒	๘
๗.๓ No Program Document or Comments	๓	๒	๖
๘ Vender and Outsource Failure			
๘.๑ Vender stop support	๑	๔	๔
๙ Hacking	๓	๕	๑๕
๑๐. Environment Factors			
๑๐.๑ Utiltities	๓	๕	๑๕

เมื่อคำนวณคะแนนความเสี่ยงแล้ว ได้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยง (IT Risk Matrix) ดังนี้

Risk value			Probability				
			Vary Low	Low	Medium	High	Vary high
			๑	๒	๓	๔	๕
Impact	Vary high	๕				๔.๑, ๔.๒	
	High	๔	๗.๒				
	Medium	๓	๗.๑, ๗.๓	๖.๓			๒.๑
	Low	๒	๖.๔	๑.๒,๓.๑,๖.๑,๖.๒	๑.๓, ๕.๑, ๕.๒		๑.๑
	Very Low	๑					๓๒., ๑๐.๑

จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยง เราจะสามารถเรียงลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้โดย เหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูงมาก (๑๗-๒๕) จะถือว่ามีค่าความเสี่ยงในระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้โดยทันทีจึงต้องเขียนแผนจัดการความเสี่ยงเหตุการณ์ระดับนี้โดยกำหนดลำดับความสำคัญเป็นลำดับแรก ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูง และปานกลาง จะกำหนดลำดับความสำคัญไว้เป็นลำดับต่อมา

เมื่อกำหนดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้แล้ว ขั้นตอนต่อไป คือการกำหนดวิธีแก้ไขความเสี่ยง (Risk Treatment) ให้กับเหตุการณ์ต่างๆ โดยมีทางเลือกกลยุทธ์ในการแก้ไข ความเสี่ยงทั้งหมด ๔ กลยุทธ์ดังนี้

กลยุทธ์ที่ ๑ การลดความเสี่ยง
กลยุทธ์ที่ ๒ การย้ายความเสี่ยง
กลยุทธ์ที่ ๓ การหลีกเลี่ยงความเสี่ยง
กลยุทธ์ที่ ๔ การยอมรับความเสี่ยง

การวางแผนกลยุทธ์จัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ (IT Risk Action)

เหตุที่ทำให้เกิดความเสี่ยง	Risk Value	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
เครื่องพิมพ์เสีย	๑๕	ย้ายกระบวนการซ่อมและกระบวนการบริการเครื่องพิมพ์ให้พร้อมใช้ไปอยู่ในความรับผิดชอบของบริษัท	ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้บริษัท ต้องตั้งเครื่องพิมพ์สำรองพร้อมทดแทนไว้ ๕ เครื่อง ถ้ามีเครื่องเสียต้องยกเครื่องอื่นมาให้ใช้แทนได้ภายใน ๒๔ ชั่วโมง	อับดุลวาเฮบ สานิ
เครื่องคอมพิวเตอร์ติดไวรัส	๑๕	เปลี่ยนแปลงวิธีการทำงานเพื่อลด โอกาสที่จะเกิดเหตุการณ์	๑. ปิดการใช้งาน USB Drive ๒. ตั้งเวลาให้โปรแกรมสแกนหาไวรัสใน เครื่องทุกๆ วัน ในช่วงเวลาพักรับประทาน อาหารกลางวัน	มูฮำมัด อาแซ
เจ้าหน้าที่ลบข้อมูลผิดรายการ ในโปรแกรม Hos-XE	๑๐	เปลี่ยนแปลงวิธีการทำงานเพื่อลด โอกาสที่จะเกิดเหตุการณ์	เปลี่ยนแปลงโปรแกรมโดยกำหนดให้ไม่สามารถลบข้อมูลออกจากฐานข้อมูลได้ โดยให้ใช้การยกเลิกข้อมูลที่ผิดพลาดและเพิ่มข้อมูลใหม่ที่ถูกต้องเข้าไปทดแทนได้	แอนซอรี อาลี

การวางแผนกลยุทธ์จัดการความเสี่ยง (ต่อ)

เหตุที่ทำให้เกิดความเสี่ยง	Risk Value	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
ไม่มีการบันทึกข้อมูลราคาในรายการยา ข้อมูลรายการยาไม่ครบ ๒๔ หลัก	๑๖	ลดโอกาสที่จะเกิดเหตุการณ์	๑. ทำกลุ่มไลน์ Data๔๓ file เพื่อตรวจสอบความสมบูรณ์ ๒. ติดตามข้อมูลเป็นรายสัปดาห์ทุกวันจันทร์จะส่งข้อมูลที่ไม่สมบูรณ์	บาฮารี แม
เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ ระบบล่ม/ มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	๑๕	ลดโอกาสที่จะเกิดเหตุการณ์	๑. จัดทำระบบ Back up ข้อมูลใน HOS แบบรายวันและ ๒ สัปดาห์ครั้ง ๒. ใช้ CAT Fiber Optic ๓. จัดทำห้อง Server เพิ่มความสะดวกในการเชื่อมต่อข้อมูล ๔. แยก server Hos-XE/X-ray แยก server Hos-office ๕. จัดทำระบบ One HN oneTambon ตามมาตรฐาน HA	อับดุลวาเฮบ สานิ
ถูกโจมตีด้วยเครือข่ายคอมพิวเตอร์สาธารณะ (Cyber)	๑๘	ลดโอกาสที่จะเกิดเหตุการณ์	๑. จัดซื้อ Server เพิ่ม ในการสำรองข้อมูลที่สำคัญ ๒. จัดซื้ออุปกรณ์ตรวจจับและป้องกันการโจมตี ๓. จัดทำแผนดำเนินการเมื่อระบบเครือข่ายล่ม ซ้อมแผนปีละ ๒ ครั้ง	อับดุลวาเฮบ สานิ
Hardware เช่น ไม่มีแผนบริหารจัดการ/ ไม่เพียงพอ/ ไม่พร้อมใช้/ ใช้ไม่ตรงวัตถุประสงค์/ ใช้ผิดวิธี-เทคนิค	๑๕	เปลี่ยนแปลงวิธีการทำงานเพื่อลด โอกาสที่จะเกิดเหตุการณ์	๑. สำรวจอุปกรณ์ทั้งหมด ๒. ทำQR Code ควบคุมแต่ละเครื่อง ๓. วางแผนการซ่อมบำรุงและจัดซื้อ	ณัฐพงศ์ อินทองคำ
ข้อมูลสารสนเทศไม่ถูกต้อง/ ไม่ครบถ้วน/ ไม่น่าเชื่อถือ/ ไม่เป็นปัจจุบัน	๑๐	เปลี่ยนแปลงวิธีการทำงานเพื่อลด โอกาสที่จะเกิดเหตุการณ์	๑. จัดทำ Dash board ลงบันทึกข้อมูลให้ถูกต้องดูง่าย ๒. ตรวจสอบ update ข้อมูลให้เป็นปัจจุบัน	ซอลาฮุดเดน เบ็นโน
ระบบจัดเก็บฐานข้อมูล(Drive Y)มีปัญหา ปัญหาที่พบ - เครื่อง ฮาร์ดดิสค์ นอก ที่เก็บข้อมูลการดำเนินงานใน รพ เสีย - ข้อมูลไม่สามารถกู้ได้	๑๕	ลดโอกาสที่จะเกิดเหตุการณ์	๑. เปลี่ยน ฮาร์ดดิสค์ ใหม่ ๒. เพิ่มช่องทางในการเข้าถึงข้อมูล เช่น Dash board ๓. จัดระบบการเข้าถึงข้อมูล	อับดุลวาเฮบ สานิ

การรวบรวมข้อมูลรายงานอุบัติการณ์ (IT Risk incidents)

IT Components	จำนวน
๑. Hardware	๑๖
๒. Software	๑๔
๓. Aplication Internet-Intranet	๓๒
๔. Comnuni cation ,connect Internet-Intranet	๔๔
๕. Operation (Human) Error	๗
๖. Project Failure	๑
๗. Future Development	๐
๘. Vender and Outsource Failure	๐
๙. Hacking	๓
๑๐. Environment Factors	๖

แผนดำเนินการจัดการความเสี่ยง ในระบบสารสนเทศ

- ความเสี่ยงที่รุนแรง ได้แก่ ด้าน Hacking

เหตุการณ์ที่เกิดความเสี่ยง	แนวทางการแก้ไขระยะสั้น	แนวทางการแก้ไขระยะยาว	งบประมาณ	ช่วงเวลาดำเนินการ
ระบบสำรองข้อมูลหลักของโรงพยาบาล (Server) ถูกโจมตีด้วยเครือข่ายคอมพิวเตอร์สาธารณะ (Cyber) ในระหว่าง Update รับปฏิบัติการป้องกันไฟล์ Firewall โดยถูกโจมตีด้วยการยิง Ddos ทำให้อุปกรณ์ Router switch เสียหายและทำการ Downgrade อุปกรณ์ต่างๆ ก่อให้เกิดเสียหาย ทำให้ผู้ดูแลระบบไม่สามารถควบคุมได้	๑. ผู้ดูแลระบบปรึกษาทีมเชี่ยวชาญเฉพาะให้ช่วยดูแลและวินิจฉัยปัญหาที่เกิดขึ้น ๒. Upgrade ระบบป้องกันใหม่	๑. จัดซื้อ Server เพิ่ม ในการสำรองข้อมูลที่สำคัญ ๒. จัดซื้ออุปกรณ์ตรวจจับและป้องกันการโจมตี	โครงการ จัดหาระบบคัดกรองและเครื่องตรวจคลื่นไฟฟ้าหัวใจสำหรับให้บริการเชื่อมโยงและจัดเก็บในฐานข้อมูลโรงพยาบาลแบบอัตโนมัติ กิจกรรม จัดซื้อเครื่องคอมพิวเตอร์แม่ข่าย (Server)ราคา ๔๙๐,๐๐๐ บาท ***งบมูลนิธิเทพรัตนเวชานุกูล	พ.ค.-มิ.ย. ๖๕

แผนดำเนินการจัดการความเสี่ยง ในระบบสารสนเทศ (ต่อ)

- ความเสี่ยงที่พบมาก ได้แก่ ด้าน Communication, Connectivity

เหตุการณ์ที่เกิดความเสี่ยง	แนวทางการแก้ไขระยะสั้น	แนวทางการแก้ไขระยะยาว	งบประมาณ	ช่วงเวลาดำเนินการ
Hos-XE, Hos-office ล่ม สายข้างนอกมีปัญหา, ถูกตัดสาย, เกิดจากภัยทางธรรมชาติ	๑. จัดทำระบบ Back up ข้อมูลใน HOS แบบรายวัน และ ๒ สัปดาห์ครั้ง ๒. แยก server Hos-XE/X-ray แยก server Hos-office ๓. จัดทำระบบ One HN oneTambon ตามมาตรฐาน HA	๑. ใช้ CAT Fiber Optic ๒. จัดทำห้อง Server เพิ่มความสะดวกในการเชื่อมต่อข้อมูล	โครงการ พัฒนาระบบการให้บริการ Smart Hospital เดินสายระบบอินเตอร์เน็ตและ Fiber Optic พร้อมติดตั้ง ราคา ๒๐๕,๐๐๐ บาท ***งบประมาณรายจ่ายประจำปีกิจกรรมสนับสนุนการการดำเนินงานตามโครงการพระราชดำริและเฉลิมพระเกียรติ และงบเงินบำรุงโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา	ต.ค.๖๔-ม.ค. ๖๕