

๒.

การบริหารความเสี่ยงด้าน
ระบบเทคโนโลยีสารสนเทศ
(IT RISK MANAGEMENT)

คำนำ

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลอุดรธานี ประจำปี ๒๕๖๖ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศในการระบุความเสี่ยงวิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงโดยมุ่งหวังให้บรรลุผลตามเป้าประสงค์ของหน่วยงาน เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่องค์กรสามารถรองรับได้และทำให้การปฏิบัติงานมีประสิทธิภาพมากยิ่งขึ้นโรงพยาบาลอุดรธานี หวังเป็นอย่างยิ่งว่าแผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

ทั้งนี้โรงพยาบาลอุดรธานีจะนำแผนการจัดการความเสี่ยงไปใช้เพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ต่อไป

สารสนเทศทางการแพทย์ (ศูนย์คอมพิวเตอร์)

หน้า

การจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

๑. แผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

- ๑.๑. หลักการและเหตุผล
- ๑.๒. วัตถุประสงค์
- ๑.๓. ผลที่คาดว่าจะได้รับ
- ๑.๔. ความหมายของการบริหารความเสี่ยง
- ๑.๕. ขอบเขตการดำเนินการ
- ๑.๖. ระยะเวลาการดำเนินการ

๒. สถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการในปัจจุบัน

๓. การประเมินความเสี่ยง

- ๓.๑. ผลการวิเคราะห์ความเสี่ยง
- ๓.๒. รายงานผลการวิเคราะห์ความเสี่ยง

๔. การจัดการความเสี่ยง

๕. ภาคผนวก

ส่วนที่ ๑

แผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

เนื่องจากแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดให้มีการปรับเปลี่ยนบริการของภาครัฐ เพื่อตอบสนองการบริการประชาชน ผู้ประกอบการ ทุกภาคส่วนให้มีความสะดวก รวดเร็ว และแม่นยำมีโครงสร้างการจัดเก็บและบริหารฐานข้อมูลที่เป็นบูรณาการ ไม่ซ้ำซ้อน สามารถรองรับการเชื่อมโยงการทำงาน ระหว่างหน่วยงาน และให้บริการประชาชนได้อย่างทั่วถึงและมีประสิทธิภาพ การบริหารจัดการความเสี่ยง จึงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้องงานตามภารกิจของหน่วยงานให้รอดพ้นจากความ เสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ซึ่งขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการ สื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน มีกระบวนการในการบริหารจัดการความเสี่ยงด้าน เทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่ อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อให้การดำเนินการตามภารกิจของหน่วยงานบรรลุผลตามวัตถุประสงค์ไม่ใช่แค่เพียงการปกป้องสินทรัพย์ เทคโนโลยีสารสนเทศหรือหน่วยงานเท่านั้น การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่า ด้วยการบริหารกิจการบ้านเมืองที่ดีพ.ศ. ๒๕๕๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการ บริหารเชิงกลยุทธ์เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุวัตถุประสงค์ตามภารกิจที่ตั้งไว้และเป็นการ พัฒนาการปฏิบัติงานของหน่วยงาน เพื่อนำไปสู่การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

หลักการและเหตุผล

๑. เพื่อให้การจัดการภายในหน่วยงานมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการ เปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหาย ต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเลย

๒. เพื่อให้มีการวางแผนการควบคุมแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม

๓. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในโรงพยาบาลเลย

ผลที่คาดว่าจะได้รับ

เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในโรงพยาบาลเลย

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของหน่วยงาน เช่น ไวรัสมาทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต

ระดับความเสี่ยงที่ยอมรับได้(Risk appetite หรือ Acceptable level of risk) หมายถึง ความความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชา

แผนการลดความเสี่ยง (Treatment Plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยง สำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับ ความเสี่ยงที่ยอมรับได้ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติดำเนินการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้เกิดวัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็น สาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยง ในภายหลังได้อย่างถูกต้อง

ขอบเขตการดำเนินการ

บริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของโรงพยาบาลอุดรธานี

ระยะเวลาดำเนินการ

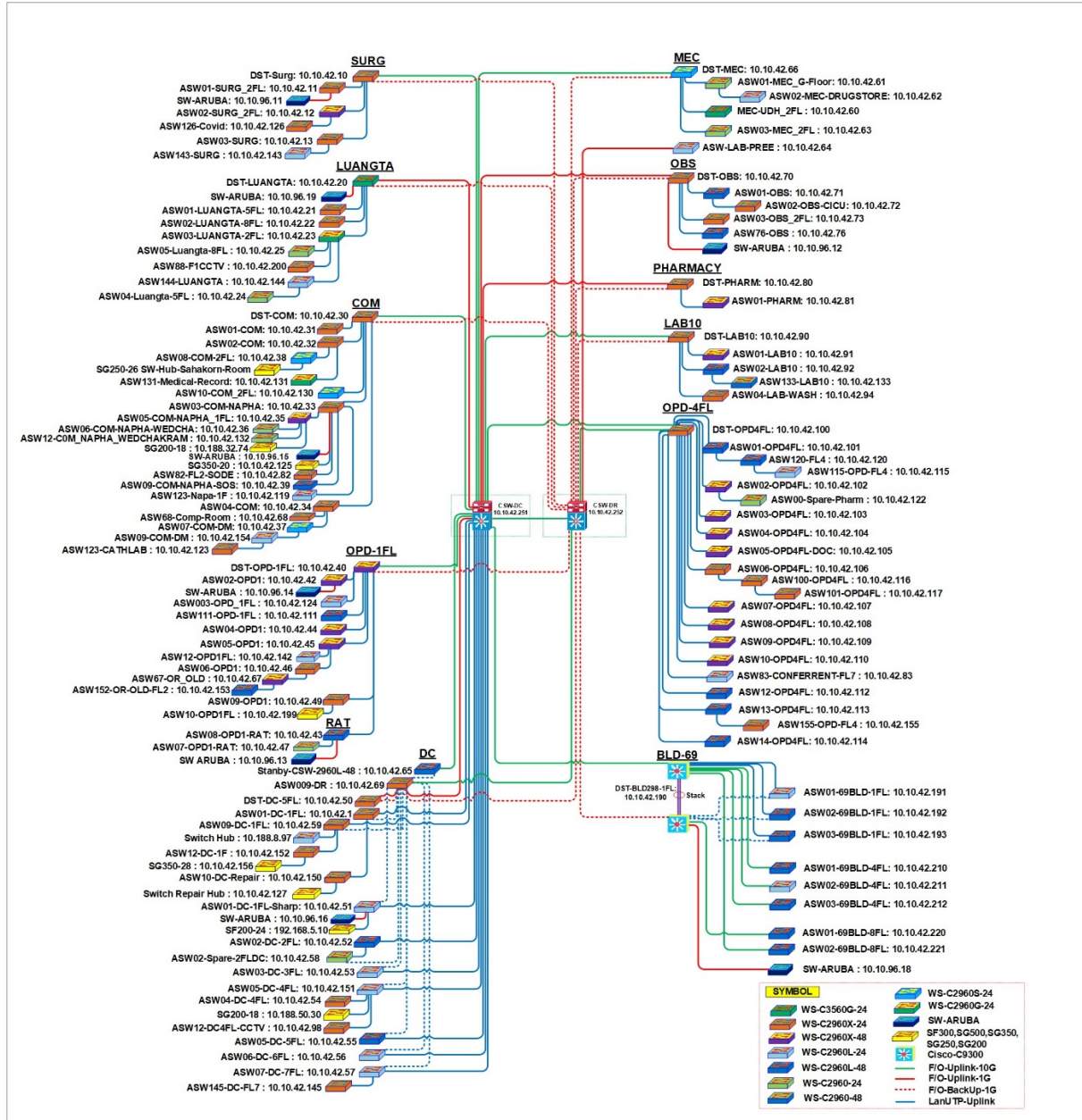
ลำดับที่	กิจกรรม	ปีงบประมาณ ๒๕๖๖						หน่วยงานรับผิดชอบ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑	ศึกษาข้อมูลในการจัดทำ แผนบริหารการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ							สารสนเทศทางการแพทย์
๒	วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดทำ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ							ศูนย์คอมพิวเตอร์
๓	วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดทำ แผนบริหารจัดการความเสี่ยงด้านเวชระเบียน							เวชระเบียน
๔	สรุปผลการประเมิน							สารสนเทศทางการแพทย์

ตารางที่ ๑ ตารางแสดงระยะเวลาดำเนินการ

ส่วนที่ ๒

สถานภาพและสภาพแวดล้อมของโรงพยาบาล

ระบบเครือข่ายคอมพิวเตอร์



จำนวนคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

กิจกรรม	จำนวนเครื่อง(ร้อยละ)
คอมพิวเตอร์เพื่อให้บริการ(เครื่อง)	๑,๐๐๐
โน้ตบุ๊ก	๑๕๐
แท็บเล็ต	๒๐
คอมพิวเตอร์ประมวลผล	๕
รวม	๑,๒๗๕
ข้อมูล ณ ปีงบประมาณ ๒๕๖๕ หมายเหตุ ประมาณร้อยละ ๗๐ มีอายุการใช้งานมากกว่า ๑๐ ปี	

ตารางที่ ๒ จำนวนคอมพิวเตอร์เพื่อให้บริการ

ส่วนที่ ๓

การประเมินความเสี่ยง (Risk Assessment)

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสำนักงานจังหวัด สามารถแยกประเภทความเสี่ยงด้านเป็น ๔ ประเภท ดังนี้

๑. ความเสี่ยงด้านเทคนิคเป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือและอุปกรณ์เองอาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีถูกก่อวินาศกรรมจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงจากผู้ปฏิบัติงานเป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดการ ความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่าง ๆ ของสำนักงานจังหวัดเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการวางแผนนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ

การประเมินความเสี่ยงโอกาสที่จะเกิดความเสี่ยงและผลเสียหาย

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

๑. ต่ำมาก ไม่น่าจะเกิดเหตุการณ์นี้ได้หรือมีโอกาสเกิดได้น้อยมาก
๒. ต่ำมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ ๑ ปี
๓. ปานกลาง มีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ ๑ ครั้ง
๔. สูง มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
๕. สูงมาก มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกสัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

๑. ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
๒. ต่ำมีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
๓. ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน ๑ - ๒ แผนก
๔. สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล ๓ - ๔ แผนก
๕. สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นได้ประเมินคะแนนความเสี่ยง คำนวณได้จาก คะแนนโอกาส บวก กับ คะแนนผลเสียหาย (สูตร คำนวณนี้เป็นตามข้อกำหนดของงาน HA โรงพยาบาลเลย) เช่น โอกาสเกิดความเสี่ยง = ๓ ผลเสียหาย = ๕ ดังนั้น คะแนนความเสี่ยง = ๓ + ๕ = ๘ เมื่อคำนวณคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมา พิจารณาตามแผนผังประเมินความเสี่ยงดังนี้

ผลกระทบ	๕	๖	๗	๘	๙	๑๐
	๔	๕	๖	๗	๘	๙
	๓	๔	๕	๖	๗	๘
	๒	๓	๔	๕	๖	๗
	๑	๒	๓	๔	๕	๖
		๑	๒	๓	๔	๕
		โอกาสที่จะเกิด/ความถี่				

ตารางที่ ๓ ตารางคำนวณความเสี่ยง

ผลการวิเคราะห์ความเสี่ยง

ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลอุดรธานี มีดังนี้

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
ฮาร์ดแวร์ Hardware	ฮาร์ดแวร์ใช้งานเกิน ๕ ปีอาจเกิดการชำรุด/เสียหาย				
	ฮาร์ดแวร์มีประสิทธิภาพการประมวลผลต่ำไม่สามารถประมวลผลได้ทันเวลา				
	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ				
	อุปกรณ์เกิดความเสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี				
	ถูกทำลายด้วยผู้บุกรุก				
	การถูกโจรกรรม				
	ไฟไหม้				
	ไฟฟ้าลัดวงจร				
	ไม่มีระบบป้องกันไฟฟ้ากระชาก/ไฟฟ้าดับ				
	ขาดอุปกรณ์ทดแทนเมื่อเกิดการชำรุด/สูญหาย				
	สายไฟหรือสายอุปกรณ์ขาดชำรุด				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
ซอฟต์แวร์ Software	ขาดโปรแกรมตรวจสอบไวรัส				
	มีการติดตั้งซอฟต์แวร์ที่อาจมีการฝังไวรัส				
	ระบบปฏิบัติการเสียหาย				
	ถูกไวรัสโจมตีจากอินเทอร์เน็ต				
	ติดตั้งซอฟต์แวร์ที่ไม่มีแหล่งที่มาที่เชื่อถือได้				
	ซอฟต์แวร์ไม่เข้ากับฮาร์ดแวร์				
	ไม่ตอบสนองความต้องการของผู้ใช้งาน				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
อุปกรณ์เครือข่าย Network	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ				
	ระบบเครือข่ายเสียหาย/ขัดข้อง				
	ถูกโจรกรรม				
	ไฟไหม้				
	ขาดอุปกรณ์ทดแทนเมื่อเกิดการชำรุด/สูญหาย				
	อุปกรณ์เกิดความเสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี				
	ถูกทำลายด้วยผู้บุกรุก				
	ไฟฟ้าลัดวงจร				
	ไม่มีระบบป้องกันไฟฟ้ากระชาก/ไฟฟ้าดับ				
	อายุการใช้งานของอุปกรณ์เกิน ๕ ปี อาจเกิดการชำรุด/เสียหาย				
	ประสิทธิภาพการส่งข้อมูลต่ำ ไม่สามารถส่งข้อมูลได้ทันเวลา				
	สายไฟหรือสายอุปกรณ์ขาดชำรุด				
	ถูกเจาะระบบจากภายนอก				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
บุคลากรและ หน่วยงาน Department	เจ้าหน้าที่เกิดอุบัติเหตุขณะปฏิบัติงาน				
	ขาดความรู้/ความเข้าใจ ในการใช้งานโปรแกรมหรืออุปกรณ์				
	มีการเปิดเผยรหัสผ่าน/ไม่มีการรักษารหัสผ่านไว้เป็นความลับ				
	ไม่มีการออกจากระบบ(logout)เมื่อไม่ได้อยู่ที่โต๊ะทำงาน				
	สำเนาข้อมูลให้บุคคลภายนอกซึ่งอาจเป็นความลับ				
	บันทึกข้อมูลผิดพลาด/ไม่ครบถ้วน				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
อาคารสถานที่และ ระบบสนับสนุน ในห้องคอมพิวเตอร์ เครื่องแม่ข่าย Environment	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ				
	เครื่องปรับอากาศไม่ทำงาน/ไม่เย็น				
	การแอบ/ลักลอบ เข้าห้อง Server หรือไม่มีการควบคุมการเข้า				
	ไฟไหม้				
	ไม่มีระบบป้องกันไฟฟ้ากระชาก/ไฟฟ้าดับ				
	ไฟฟ้าลัดวงจร				
	ถูกทำลายด้วยผู้บุกรุก				
	อุปกรณ์เกิดความเสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี				
	ขาดอุปกรณ์ทดแทนเมื่อเกิดการชำรุด/สูญหาย				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
ระบบฐานข้อมูล/ เครื่องแม่ข่าย Data Center	ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดการเสียหาย				
	ข้อมูลสูญหายเกิดจากอุปกรณ์บันทึกข้อมูล (Hard disk) ชำรุด				
	ขาดการทดสอบการกู้ข้อมูล				
	ขาดการสำรองข้อมูล				
	ข้อมูลสูญหายเกิดจากความผิดพลาดของเจ้าหน้าที่				
	ถูกเจาะระบบจากภายนอก				
	ระบบช้า/หน่วง เนื่องจากการมีกรดิงรายงานที่ต้องใช้เวลานาน				
	Server หยุดทำงานโดยไม่ทราบสาเหตุ				
	ตารางในฐานข้อมูลเสียหาย				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
รับบัตร	ทำบัตรผิดคน (ญาติยื่นทำบัตรแทนผู้ป่วย ยื่นเอกสารผิดคน เจ้าหน้าที่พิมพ์ประวัติผู้ป่วยผิด ชักประวัติผู้ป่วยในการทำบัตรไม่ครบถ้วน)				
	มีการสวมสิทธิ์ผู้ป่วย				
	ไม่พึงพอใจ (รอทำบัตรนาน ไม่มีที่นั่งรอ จนท.พูดไม่เพราะ)				
การออกรายการส่ง ตรวจ	ส่งตรวจผิดแผนก				
	ส่งตรวจผิดคน				
	ให้สิทธิ์ผิดพลาด				
ค้นบัตร	ค้นบัตรผิดคน				
	ค้นบัตรล่าช้า				
	หาประวัติเก่าไม่พบ				
	ตามประวัติadmit ล่าช้า				
ส่งบัตรตามห้องตรวจ	ส่งบัตรล่าช้า				
	ส่งบัตรผิดแผนก				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
ส่งบัตรตามห้องตรวจ	ส่งบัตรล่าช้า				
	ส่งบัตรผิดแผนก				
เก็บบัตรจากห้องตรวจ	บัตรไม่ครบ				
	เก็บบัตรล่าช้า				
เก็บบัตรคืน	เก็บบัตรผิดที่				
	เก็บบัตรช้า/บัตรไม่เข้าชั้นตามเวลาที่กำหนด				
	เก็บบัตรล่าช้า				
	เก็บบัตรไม่ครบ				
ส่งบัตรตามห้องตรวจ	ส่งบัตรล่าช้า				
	ส่งบัตรผิดแผนก				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
เวชระเบียนผู้ป่วยใน	คั่นประวัติผิดคน				
	ชาร์ตเข้าระบบโดยไม่ผ่านการบันทึกรหัสลงในคอมพิวเตอร์				
	ตึกผู้ป่วยในยืมประวัติแล้วไม่คืนตามเวลาที่กำหนด				
	ห้องตรวจยืมประวัติผู้ป่วยไปแล้วไม่คืนในวัน/คืนไม่ครบ				
	ตึกผู้ป่วยในส่งประวัตินานเกินเวลาที่กำหนด				
	การเข้าถึงเวชระเบียนจากบุคคลภายนอกหน่วยงาน				
	ข้อร้องเรียนเกี่ยวกับพฤติกรรมบริการ				
	ไฟฟ้าดับ				
แยกประเภทเอกสาร	แยกเอกสารผิดคน(Lab x-ray Echo EKG และเอกสารอื่นๆที่ทำกิจกรรมเกี่ยวกับผู้มารับบริการ)				
จัดเก็บเอกสาร	เก็บเอกสารผิดวัน				

ประเภท	รายการความเสี่ยง	โอกาส/ ความถี่	ผลกระทบ	ระดับ ความเสี่ยง	Plot Value
แสกนชาร์ต	แสกนเอกสารผิดประเภท				
	แสกนผิดคน				
	แสกนไม่ครบในHN นั้น				
	แสกนไม่ทันเวลา				
	ตึกผู้ป่วยในส่งประวัตินานเกินเวลาที่กำหนด				
อื่น ๆ	ข้อร้องเรียนเกี่ยวกับพฤติกรรมบริการ				
	ไฟฟ้าดับ				
	การเข้าถึงเวชระเบียนจากบุคคลภายนอกหน่วยงาน				
	ICD ๑๐ ผิดพลาด				
	บันทึกเวชระเบียนไม่ครบถ้วน สมบูรณ์				
	การเข้าถึงเวชระเบียนจากบุคคลภายนอกหน่วยงาน				
	ข้อร้องเรียนเกี่ยวกับพฤติกรรมบริการ				

รายงานผลการวิเคราะห์ความเสี่ยง

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	โอกาส	ผลกระทบ	ระดับ
ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	๑.ระบบกระแสไฟฟ้าขัดข้อง/ไฟดับ	- เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิด โดยไม่สมบูรณ์อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ - ทำความเสียหายระยะยาวต่ออุปกรณ์คอมพิวเตอร์ - เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว			
ความเสี่ยงด้านบริหาร จัดการ	๒.ไม่ออกจากระบบ(Log out) เมื่อไม่ใช้งาน HomeC	- ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ทำให้ข้อมูลและระบบการทำงานของคอมพิวเตอร์ถูกแก้ไข เปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิแก่บุคคลที่มีหน้าที่รับผิดชอบให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ส่งผลให้ไม่สามารถปฏิบัติงานได้			
ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	๓.เปิดเผยรหัสผ่าน/รหัสผ่านไม่เป็นความลับ	- ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ทำให้ข้อมูลและระบบการทำงานของคอมพิวเตอร์ถูกแก้ไข เปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิแก่บุคคลที่มีหน้าที่รับผิดชอบให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ส่งผลให้ไม่สามารถปฏิบัติงานได้			

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	โอกาส	ผลกระทบ	ระดับ
ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	๔.ถูกไวรัสโจมตีจากอินเทอร์เน็ต	- ทำให้ระบบคอมพิวเตอร์ในโรงพยาบาลไม่สามารถทำงานต่อได้			
	๕.เครื่องปรับอากาศไม่ทำงาน/ไม่เย็น	- ทำให้อุณหภูมิห้องแม่ข่ายสูง ส่งผลให้อุปกรณ์ห้องแม่ข่ายเสียหาย ส่งผลให้ไม่สามารถให้บริการได้			
ความเสี่ยงด้านบริหารการจัดการ	๖.เวชระเบียนขาดความถูกต้องสมบูรณ์ครบถ้วน	- ทำให้ข้อมูลในเวชระเบียนไม่น่าเชื่อถือ เกิดความผิดพลาดในการรักษา เกิดความเสียหายต่อทรัพย์สิน			
	๗.ให้CD๑๐ ผิดพลาด	- ทำให้ข้อมูลในเวชระเบียนไม่น่าเชื่อถือ เกิดความผิดพลาดในการรักษา เกิดความเสียหายต่อทรัพย์สิน			
ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องใน การดูแลรักษาผู้ป่วย	๘.ให้สิทธิ์ผิดพลาด	- ทำให้ผู้ป่วยได้รับสิทธิ์การรักษาที่ไม่ตรงตามสิทธิ์ที่มีและส่งผลให้โรงพยาบาลสูญเสียค่ารักษาที่ควรจะได้รับตามสิทธิ์ของผู้ป่วยนั้น			
	๙.ทำบัตรผิดคน	- ทำให้เกิดการรักษาผิดพลาด ผิดคน ส่งผลให้โรงพยาบาลสูญเสียทรัพย์สินและความน่าเชื่อถือ			
	๑๐.มีการสวมสิทธิ์	- ทำให้ผู้ป่วยไม่สามารถใช้สิทธิ์ที่ตัวเองมีและถูกบุคคลอื่นสวมสิทธิ์แทน			
	๑๑.ข้อร้องเรียน	- ทำให้เสียภาพลักษณ์ที่ดีของโรงพยาบาล			

การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์โรงพยาบาลเลยระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ 5 กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 6 ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า 6 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ซึ่งการดำเนินการจัดการความเสี่ยงเป็นดังที่กล่าวมาข้างต้น

๑. หลีกเลี่ยงความเสี่ยง (Risk Avoidance = RA) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง ๑ ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของ ไวรัสอย่างหนัก องค์กรอาจมีเลือกกระบังไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

๒. การโอนย้ายความเสี่ยง (Risk Transfer = RF) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่าย ไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือ สัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

๓. การยอมรับความเสี่ยง (Risk Acceptance = RC) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ Id/Password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้การให้ผู้ใช้ชีวมาตร (Biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่าโรงพยาบาล อาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

๔. การลดความเสี่ยง (Loss Reduction = LR) ได้แก่การมีมาตรการควบคุมมากขึ้นหรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (Biometrics) เพื่อใช้ในการพิสูจน์ตัวจริง นอกเหนือไปจากการใช้ Id/Password ที่มีอยู่เดิม

การเลือกการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจัยเสี่ยง	วิธีการจัดการปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๑.ระบบ กระแสไฟฟ้า ขัดข้อง/ไฟดับ	หลีกเลี่ยง ยอมรับ ควบคุมถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียมาก - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) - แจ้งความเสี่ยงให้ENV รับทราบและมีการเตรียมการปรับปรุงระบบ GEN ในปีงบประมาณ ๒๕๖๒	- เกิดต้นทุนในการจัดหาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) - เกิดต้นทุนในการปรับปรุงระบบGEN	- เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	ควบคุมถ่ายโอน
๒.ไม่ออกจาก ระบบ(Log out) เมื่อไม่ใช้งาน HomC	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียมาก - จัดทำและประกาศใช้นโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ - จัดทำระเบียบการดูแลและการใช้งาน ข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ - ไม่สามารถถ่ายโอนให้ผู้อื่นได้	- เกิดค่าใช้จ่ายใน การจัดทำระบบป้องกัน ความปลอดภัยของข้อมูล - เกิดค่าใช้จ่ายในการจัดอบรมให้ความรู้แก่เจ้าหน้าที่	- เพื่อป้องกันปัญหาซึ่งอาจสร้างความเสียหาย แก่ระบบสารสนเทศและระบบคอมพิวเตอร์	ควบคุม

ปัจจัยเสี่ยง	วิธีการจัดการปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๓.เปิดเผยแพร่ผ่าน/รหัสผ่านไม่เป็นความลับ	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียมาก - จัดทำและประกาศใช้นโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ - จัดทำระเบียบการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศ ให้แก่เจ้าหน้าที่ทุกระดับ - ไม่สามารถถ่ายโอนให้ผู้อื่นได้	- เกิดค่าใช้จ่ายในการจัดทำระบบป้องกันความปลอดภัยของข้อมูล - เกิดค่าใช้จ่ายในการจัดอบรมให้ความรู้แก่เจ้าหน้าที่	- เพื่อป้องกันและแก้ไขปัญหาจากระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	ควบคุม
๔.ถูกไวรัสโจมตีจากอินเทอร์เน็ต	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียมาก - ติดตั้งระบบป้องกันไวรัสบนคอมพิวเตอร์ระบบงานในโรงพยาบาล - ไม่สามารถถ่ายโอนให้ผู้อื่นได้	- เกิดค่าใช้จ่ายในการจัดทำระบบป้องกันไวรัส	- ป้องกันไม่ให้ระบบคอมพิวเตอร์ถูกไวรัสโจมตี	ควบคุม
๕.เครื่องปรับอากาศไม่ทำงาน/ไม่เย็น	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียมาก - ติดตั้งระบบแจ้งเตือนอุณหภูมิห้องแม่ข่ายหลักและ DR-site - จัดหาเครื่องปรับอากาศทดแทนของเดิมที่ใช้งานเกิน ๗ ปี - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดหาอุปกรณ์และติดตั้งระบบแจ้งเตือนและค่าใช้จ่ายในการจัดหาเครื่องปรับอากาศใหม่	- ป้องกันไม่ให้ห้องแม่ข่ายหลักและ DR-site มีอุณหภูมิสูงเกินไปจนทำให้อุปกรณ์ห้องแม่ข่ายและ DR-site เสียหาย	ควบคุม

ปัจจัยเสี่ยง	วิธีการจัดการปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๖.เวชระเบียนขาดความครบถ้วนสมบูรณ์	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียค่อนข้างมาก - ทำการตรวจสอบความสมบูรณ์ของเวชระเบียน โดยคณะกรรมการตรวจสอบเวชระเบียน(สหวิชาชีพ) - อบรมการบันทึกเวชระเบียนที่ถูกต้องแก่เจ้าหน้าที่ - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อให้การบันทึกข้อมูลในเวชระเบียนและ ICD ๑๐ ถูกต้อง ครบถ้วน สมบูรณ์	ควบคุม
๗.ให้ ICD ๑๐ ผิดพลาด	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียค่อนข้างมาก - ทำการตรวจสอบความสมบูรณ์ของเวชระเบียน โดยคณะกรรมการตรวจสอบเวชระเบียน(สหวิชาชีพ) - อบรมการบันทึกเวชระเบียนที่ถูกต้องแก่เจ้าหน้าที่ - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อให้การบันทึกข้อมูลในเวชระเบียนและ ICD ๑๐ ถูกต้อง ครบถ้วน สมบูรณ์	ควบคุม
๘.ให้สิทธิผิดพลาด	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียค่อนข้างมาก - ให้ความรู้แก่เจ้าหน้าที่ เกี่ยวกับขั้นตอนการตรวจสอบความถูกต้องของการให้สิทธิ และการทำบัตรให้ถูกคน - จัดทำ แนวทางการตรวจสอบสิทธิ การทำ บัตรที่ตรวจสอบได้ - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อป้องกันไม่ให้เกิดความผิดพลาดในการให้สิทธิ และการทำบัตรผิดคน และการเสียชื่อเสียงขององค์กร	ควบคุม
๙.ทำบัตรผิดคน	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียค่อนข้างมาก - ให้ความรู้แก่เจ้าหน้าที่ เกี่ยวกับขั้นตอนการตรวจสอบความถูกต้องของการให้สิทธิ และการทำบัตรให้ถูกคน - จัดทำ แนวทางการตรวจสอบสิทธิ การทำ บัตรที่ตรวจสอบได้ - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อป้องกันไม่ให้เกิดความผิดพลาดในการให้สิทธิ และการทำบัตรผิดคน และการเสียชื่อเสียงขององค์กร	

ปัจจัยเสี่ยง	วิธีการจัดการปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๑๐.การสวมสิทธิ์	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้เนื่องจากมีผลเสียค่อนข้างมาก - ให้ความรู้แก่เจ้าหน้าที่ เกี่ยวกับขั้นตอนการตรวจสอบความถูกต้องของการตรวจสอบสิทธิ์ และการให้สิทธิ์ให้ถูกคน - จัดทำแนวทางการตรวจสอบสิทธิ์ที่ตรวจสอบได้และเป็นขั้นตอนชัดเจน - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อป้องกันการสวมสิทธิ์ของบุคคลที่ไม่ใช่เจ้าของสิทธิ์นั้น ๆ - ป้องกันการสูญเสียทรัพย์สินขององค์กร	ควบคุม
๑๑.ข้อร้องเรียน	หลีกเลี่ยง ยอมรับ ควบคุม ถ่ายโอน	- ไม่สามารถยกเลิกระบบนี้ได้ - ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียค่อนข้างมาก - อบรมเจ้าหน้าที่บริการด้านหน้าให้มีพฤติกรรมบริการที่ดี - อบรม Lean concept แก่เจ้าหน้าที่งานด้านหน้า - ไม่สามารถถ่ายโอนได้	- เกิดค่าใช้จ่ายในการจัดอบรม	- เพื่อป้องกันการร้องเรียนซึ่งจะทำให้องค์กรเสียภาพลักษณ์ที่ดี	ควบคุม

การเลือกการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นโยบายของโรงพยาบาลเลกระดับความเสี่ยงคงเหลือที่ยอมรับได้ < ๖ ทางศูนย์คุณภาพโรงพยาบาลเลย กำหนดให้ความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๗ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๖ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงดังตารางต่อไปนี้

ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ระดับความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ช่วงเวลาดำเนินการ	ผลลัพธ์/ความก้าวหน้า
๑.ระบบกระแสไฟฟ้าขัดข้อง/ไฟดับ	- เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดโดยไม่สมบูรณ์อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบาง ประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ - ทำความเสียหายระยะยาวต่ออุปกรณ์คอมพิวเตอร์ - เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว	๘	- จัดหาเครื่องสำรองไฟฟ้าและ ปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) - ปรับปรุงระบบGEN	- อยู่ระหว่างดำเนินการ (แผนงบปี๒๕๖๔) - ENV ปรับปรุงระบบ Genเมื่อ ๒ พ.ค. ๒๕๖๓ - เพิ่มแหล่งจ่ายไฟเป็น ๒แหล่งจ่าย ATS เมื่อ ส.ค.๒๕๖๓	- อยู่ระหว่างดำเนินการหลังปรับปรุงระบบ GENแล้วไฟฟ้ามาตามข้อกำหนดภายใน ๑๐ วินาที - ติดตั้งระบบ ATS หลังใช้งานมีการสลับแหล่งจ่ายได้ยังไม่พบอุบัติเหตุการณ์ATS ไม่ทำงาน
๒ .ไม่ออกจากระบบ (Log out) เมื่อไม่ใช้งาน HomC	- ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ทำให้ข้อมูลและระบบการทำงานของคอมพิวเตอร์ถูกแก้ไข เปลี่ยนแปลงทำลาย หรืออาจกระทำการแก้ไขสิทธิแก่บุคคลที่มีหน้าที่รับผิดชอบให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ ส่งผลให้ไม่สามารถปฏิบัติงานได้	๙	- จัดทำและประกาศใช้นโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ - จัดทำระเบียบการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ	- ทำ RCA ๓๑ พ.ค ๒๕๖๒	- จัดทำนโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ อยู่ระหว่างดำเนินการประกาศใช้และรอเผยแพร่

ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ระดับความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ช่วงเวลาดำเนินการ	ผลลัพธ์/ความก้าวหน้า
๓.เปิดเผยแพร่รหัสผ่าน/รหัสผ่านไม่เป็นความลับ	- ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ทำให้ข้อมูลและระบบการทำงานของคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงทำลาย หรืออาจกระทำการแก้ไขสิทธิแก่บุคคลที่มีหน้าที่รับผิดชอบให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ ส่งผลให้ไม่สามารถปฏิบัติงานได้	๙	- จัดทำและประกาศใช้นโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ - จัดทำระเบียบการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ	- ทำ RCA ๓๑ พ.ค ๒๕๖๒	จัดทำนโยบายและระเบียบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอยู่ระหว่างดำเนินการประกาศใช้และรอเผยแพร่
๔.ถูกไวรัสโจมตีจากอินเทอร์เน็ต	- ทำให้ระบบคอมพิวเตอร์ในโรงพยาบาลไม่สามารถทำงานต่อได้	๗	- ติดตั้งระบบป้องกันไวรัสบนคอมพิวเตอร์ระบบงานในโรงพยาบาล	- ทำ RCA ๓๑ พ.ค ๒๕๖๒ - อยู่ระหว่างจัดซื้อโปรแกรม - ป้องกันไวรัส ปิงบ ๒๕๖๓	
๕.เครื่องปรับอากาศไม่ทำงาน/ไม่เย็น	- ทำให้อุณหภูมิห้องแม่ข่ายสูงส่งผล - ให้อุปกรณ์ห้องแม่ข่ายเสียหายทำให้ - ไม่สามารถให้บริการได้	๗	- ติดตั้งระบบแจ้งเตือนอุณหภูมิห้อง - แม่ข่ายหลักและ DR site - จัดหาเครื่องปรับอากาศทดแทน - ของเดิมที่ใช้งานเกิน ๗ ปี	- ติดตั้งระบบแจ้งเตือนอุณหภูมิ - ปรับปรุงระบบปรับอากาศของ - โรงพยาบาลจัดทำเมื่อ ก.ค. ๒๕๖๓	ระบบแจ้งเตือนอุณหภูมิแจ้งเตือนทางไลน์โดยเจ้าหน้าที่ที่เกี่ยวข้องอยู่ในกลุ่มไลน์ รับทราบข้อความที่แจ้งทันทีที่ระบบปรับอากาศไม่พบปัญหาอุณหภูมิสูงกว่ากำหนด(ส.ค.- ก.ย.๒๕๖๓)ไม่มีอุบัติเหตุ

ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ระดับความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ช่วงเวลาดำเนินการ	ผลลัพธ์/ความก้าวหน้า
๖.เวชระเบียนขาดความครบถ้วนสมบูรณ์	- ทำให้ข้อมูลในเวชระเบียนไม่น่าเชื่อถือเกิดความผิดพลาดในการรักษาเกิดความเสียหายต่อทรัพย์สิน	๑๐	- จัดตั้งคณะกรรมการตรวจสอบคุณภาพเวชระเบียน โดยสหสาขาวิชาชีพและทำการตรวจสอบความสมบูรณ์ของเวชระเบียน โดยคณะกรรมการตรวจสอบเวชระเบียน - อบรมการบันทึกเวชระเบียนที่ถูกต้องแก่เจ้าหน้าที่	- คำสั่งแต่งตั้งคณะกรรมการ เมื่อ ๒๖ ต.ค. ๒๕๖๑ - จัดอบรมการบันทึกเวชระเบียน เมื่อ ๖ พ.ย. ๒๕๖๑ - เริ่ม ทำ Internal Audit เมื่อ ต.ค. ๒๕๖๑ - ปัจจุบัน	OPD - ผลการทำInternal audit ความสมบูรณ์ของการบันทึกเวชระเบียน (สปสช)-ปี๒๕๖๑ = ๖๓.๙๓% - -ปี๒๕๖๒ = ๖๙.๖๙% - ความสมบูรณ์ของการบันทึกเวชระเบียน (สนย)-ปี๒๕๖๑ = ๖๐.๔๒% - -ปี๒๕๖๒ = ๕๐.๐๒% IPD - ผลการทำ Internal audit ความสมบูรณ์ของการบันทึกเวชระเบียน (สปสช) - -ปี๒๕๖๑ = ๖๑.๐๑% - -ปี๒๕๖๒ = ๖๓.๐๖% - ความสมบูรณ์ของการบันทึกเวชระเบียน (สนย) - -ปี๒๕๖๑ = ๗๖.๗๘% - -ปี๒๕๖๒ = ๖๗.๒๐%
๗.ให้ICD ๑๐ ผิดพลาด	- ทำให้ข้อมูลในเวชระเบียนไม่น่าเชื่อถือ เกิดความผิดพลาดในการรักษา เกิดความเสียหายต่อทรัพย์สิน	๑๐	- จัดตั้งคณะกรรมการตรวจสอบคุณภาพเวชระเบียน โดยสหสาขาวิชาชีพและทำการตรวจสอบความสมบูรณ์ของเวชระเบียน โดย	- คำสั่งแต่งตั้งคณะกรรมการ เมื่อ ๒๖ ต.ค. ๒๕๖๑ - เริ่มทำ Internal audit เมื่อ ต.ค. ๒๕๖๑ - ปัจจุบัน	ผลการทำ Internal audit คุณภาพการให้รหัสโรคถูกต้อง OPD -ปี๒๕๖๑ = ๓๘.๘๘ % -ปี๒๕๖๒ = ๓๖.๘๗ % IPD -ปี๒๕๖๑ = ๗๓.๖๗ % -ปี๒๕๖๒ = ๘๖.๕๐ %

			คณะกรรมการตรวจสอบ เวชระเบียน - อบรมการบันทึกเวช ระเบียนที่ถูกต้องแก่ เจ้าหน้าที่		
๘.ให้สิทธิ์ผิดพลาด	ทำให้ผู้ป่วยได้รับสิทธิ์การรักษา ที่ไม่ตรงตามสิทธิ์ที่มีและส่งผล ให้โรงพยาบาลสูญเสียค่ารักษา ที่ควรจะได้รับตามสิทธิ์ของ ผู้ป่วยนั้น	๑๐	- จัดอบรมให้ความรู้แก่ เจ้าหน้าที่เกี่ยวกับขั้นตอนการ ตรวจสอบความถูกต้องของ การให้สิทธิ์ และการทำบัตร ให้ทุกคน - จัดทำแนวทางการตรวจสอบ สิทธิ์การทำบัตรที่ตรวจสอบ ได้	- -ประชุมชี้แจงขั้นตอนการ ปฏิบัติงาน ภายในหน่วยงาน - ทำ RCA ๒๑ ก.พ. ๒๕๖๓ - และจัดทำแนวทางปฏิบัติเรื่อง - การให้สิทธิ์ ตรวจสอบสิทธิ์ - การทำบัตร	- ยังพบความเสี่ยงเรื่องการ Identification Patientผิดพลาด จึง ได้ปรับปรุงแนวทางการปฏิบัติงาน ซึ่ง อยู่ระหว่างดำ เนินการแก้ไขปรับปรุง
๙.ทำบัตรผิดคน	ทำให้เกิดการรักษาผิดพลาด ผิดคน ส่งผลให้โรงพยาบาลสูญเสีย ทรัพย์สิน และความน่าเชื่อถือ	๑๐	- จัดอบรมให้ความรู้แก่ เจ้าหน้าที่เกี่ยวกับขั้นตอนการ ตรวจสอบความถูกต้องของ การตรวจสอบสิทธิ์ และการ ให้สิทธิ์ให้ทุกคน - จัดทำแนวทางการตรวจสอบ สิทธิ์ที่ตรวจสอบได้ และเป็น ขั้นตอนชัดเจน	- -ประชุมชี้แจงขั้นตอนการ ปฏิบัติงาน ภายในหน่วยงาน - ทำ RCA ๒๑ ก.พ. ๒๕๖๓และ จัดทำแนวทางปฏิบัติเรื่องการ ให้สิทธิ์ ตรวจสอบสิทธิ์การทำ บัตร	

ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	ระดับความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ช่วงเวลาดำเนินการ	ผลลัพธ์/ความก้าวหน้า
๑๐.การสวมสิทธิ์	- ทำให้ผู้ป่วยไม่สามารถใช้สิทธิ์ที่ตัวเอง - มีและถูกบุคคลอื่นสวมสิทธิ์แทน	๗	- จัดอบรมให้ความรู้แก่เจ้าหน้าที่เกี่ยวกับขั้นตอนการตรวจสอบความถูกต้องของการตรวจสอบสิทธิ์ และการให้สิทธิ์ให้ถูกคน - จัดทำแนวทางการตรวจสอบสิทธิ์ที่ตรวจสอบได้ และเป็นขั้นตอนชัดเจน	- ประชุมชี้แจงขั้นตอนการปฏิบัติงาน ภายในหน่วยงาน - ทำ RCA ๒๑ ก.พ. ๒๕๖๓ - จัดทำแนวทางปฏิบัติเรื่องการให้สิทธิ์ ตรวจสอบสิทธิ์การทำบัตร	ยังพบความเสี่ยงเรื่องการIdentification Patient ผิดพลาด จึงได้ปรับปรุงแนวทางการปฏิบัติงาน ซึ่งอยู่ระหว่างดำเนินการแก้ไขปรับปรุง
๑๑.ข้อร้องเรียน	- ทำให้เสียภาพลักษณ์ที่ดีของโรงพยาบาล	๘	- อบรมเจ้าหน้าที่บริการด้านหน้าให้ - มีพฤติกรรมบริการที่ดี - อบรม Lean Concept แก่เจ้าหน้าที่งานด้านหน้า	- อบรม Lean concept แก่เจ้าหน้าที่งานด้านหน้า ๑๐๐% เมื่อ ก.ค.๒๕๖๓	เจ้าหน้าที่ เข้ารับการอบรมLean ๑๐๐%