แผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี

กลุ่มงาน: นิติเวช

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 9 ธันวาคม 2566

ผู้รับผิดชอบ: หัวหน้ากลุ่มงานนิติเวช

1. บทนำ

จากการโดน ransomware attack ในวันที่ 9 ธันวาคม 2566 แผนกนิติเวช ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้

ปัญหา

จากเหตุการณ์ที่โดน ransomware attack ในวันที่ 9 ธันวาคม 2566 ทำให้ทางกลุ่มงานเกิดปัญหาในการดำเนินการในการจัดทำใบนำส่งผู้บาดเจ็บ/ใบคดี/เอกสารหมายสารทางคดี เกิดความล่าช้า เนื่องจากไม่สามารถค้นข้อมูลของผู้ป่วยได้ ทางกลุ่มงานจึงได้มีการประชุมภายในกลุ่มงานเพื่อหาแนวทางแก้ไข โดยการประสานทางเจ้าหน้าที่ตำรวจเจ้าของคดี ญาติคนไข้ หรือคนไข้ทางคดีเพื่อขอทราบข้อมูลของคนไข้

วิเคราะห์สาเหตุของปัญหา

เจ้าหน้าที่ที่ใช้งานในระบบคอมพิวเตอร์ไม่ปฏิบัติตามกฎระเบียบของการรักษาความปลอดภัยของโรงพยาบาล และไม่มีการสำรองข้อมูลทำให้ไม่สามารถกู้ข้อมูลในระบบคืนได้

แนวทางการแก้ไขปัญหา

1. รายงานหัวหน้ากลุ่มงานนิติเวชถึงปัญหาที่เกิดขึ้นภายในกลุ่มงาน
2. แจ้งบุคลากรในหน่วยงานให้รับทราบ
3. ปฏิบัติตามแผนฉุกเฉินที่โรงพยาบาลประกาศใช้
4. สื่อสารกับผู้มารับบริการให้ทราบถึงปัญหาและระยะเวลารอคอยเอกสาร
5. ประสานงานกับหน่วยงานที่เกี่ยวข้องในการทำงาน
6. ประสานทางเจ้าหน้าที่ตำรวจ ญาติคนไข้ หรือคนไข้ ขอทราบข้อมูลเพิ่มเติม เพื่อนำมาประกอบเอกสารให้แพทย์ลงความเห็น

อุปสรรค

จากเหตุการณ์นี้ทำให้เกิดอุปสรรคในการทำงานอย่างมากและทำให้การทำงานมีความซับซ้อนหลายขั้นตอน เนื่องจากมีการนำส่งเอกสารใบคดีเป็นจำนวนมาก หรือเจ้าหน้าที่ตำรวจมีการนำส่งเอกสารมาย้อนหลัง

2. รายละเอียดแผน BCP

ผลกระทบ

จากการโดน ransomware attack มีผลกระทบทำให้ทางกลุ่มงานทำงานได้ยากขึ้นเนื่องจากต้องเพิ่มขั้นตอนในการทำงานซึ่งมีความซับซ้อน และทำให้งานเสร็จช้าเพราะต้องประสานกับทางเจ้าหน้าที่และญาติเพิ่มเติม รวมถึงการค้นข้อมูลของคนไข้ก็ทำได้ยากขึ้น จากเหตุการณ์นี้ยังทำให้เกิดผลกระทบต่อคนไข้ คือ ทำให้คดีความเกิดความล่าช้าเพราะต้องรอเอกสารใบนำส่งผู้บาดเจ็บ/ใบคดี เพื่อนำไปใช้ประกอบการดำเนินคดีหรือขึ้นศาลเพื่อเรียกค่าเสียหาย

กลยุทธ์

ทางกลุ่มงานได้มีการวางกลยุทธ์ในการดำเนินงาน

- มีการประสานงานสอบถามข้อมูลจากเจ้าหน้าที่ตำรวจหรือญาติเพิ่มเติม
- ทำการสำรองข้อมูลเก็บไว้ในรูปแบบ paper เพื่อง่ายต่อการหาข้อมูลในภายหลัง และเพื่อลดขั้นตอนในการทำงาน
- มีการประสานงานเจ้าที่หน้าตำรวจหรือญาติมาติดต่อรับเอกสารเมื่อดำเนินการแล้วเสร็จ

แผนปฏิบัติการ

ขั้นตอนการรับมือ ransomware attack

-วางแผนรับมือ และอบรมวิธีการรับมือเมื่อเกิดเหตุการณ์

-แจ้งขั้นตอนการดำเนินงานให้บุคลากรในกลุ่มงานเพื่อปฏิบัติงานได้ถูกต้อง

ผู้รับผิดชอบแต่ละขั้นตอน

ลำดับผู้เกี่ยวข้อง	หน้าที่
- ผู้ปฏิบัติงาน ณ ขณะนั้น	1. รายงานหัวหน้ากลุ่มงานถึงปัญหาที่เกิดขึ้นภายในกลุ่มงาน

ผู้รับแจ้งเหตุ - หัวหน้ากลุ่มงาน	1.รับแจ้งเหตุ หรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์ 2.รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ 3.ให้คำแนะนำปรึกษาบุคลากรเกี่ยวกับการป้องกันจุดอ่อน ข้อควรระมัดระวัง และเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่
คณะกรรมการสารสนเทศ - หน่วยงาน IT ของโรงพยาบาล	1.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามอุปกรณ์ ตรวจจับ 2.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกันข้อควรระมัดระวังและแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน 3.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกันและตอบสนอง
ผู้บริหารของโรงพยาบาล	1.รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยทางไซเบอร์

หมายเหตุ คณะกรรมการสารสนเทศ ควรเป็นบุคลากรที่มีความรู้ ความสามารถ ประสบการณ์ ผ่านการ อบรมด้าน Cyber security ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้าน เกี่ยวกับการรักษาความปลอดภัยไซเบอร์

รายชื่อผู้ติดต่อ เมื่อเกิดเหตุการณ์ฉุกเฉินทางระบบสารสนเทศ

ชื่อ-นามสกุล	ตำแหน่ง
นพ.นิพันธ์ ทองบ่อ	หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์
นพ.จิรวัฒน์ ตีระเดชะวาทย์	หัวหน้ากลุ่มงานนิติเวช

การทดสอบและฝึกอบรม

มีการประชุม และดำเนินการอบรมวิธีการรับมือกับเหตุการณ์ ransomware attack โดยให้นำแผนที่วางไว้มาใช้ในการดำเนินงานจริง และทำการทดสอบแผนปฏิบัติการโดยเริ่มจากเอกสารย้อนหลังที่มีการส่งมาแล้วยังดำเนินการไม่ได้

เอกสารแนบ

แผนงานที่ใช้ในแผน BCP

- รับเอกสารใบนำส่งผู้บาดเจ็บ/ใบคดี
- ตรวจสอบวันที่เกิดเหตุ และวันที่คนไข้เข้า Admit ที่โรงพยาบาลอุดรธานี
- หากเป็นเหตุที่เกิดย้อนหลังที่เกิดขึ้นก่อนวันที่ 9 ธันวาคม 2566 ให้ดำเนินการประสานงานกับเจ้าหน้าที่ตำรวจเจ้าของคดี หรือญาติผู้ป่วย เพื่อสอบถามข้อมูลเพิ่มเติม
- ประสานทางกลุ่มงานเวชระเบียนในเรื่องประวัติของคนไข้
- ประสานทางแพทย์เจ้าของไข้ เพื่อเสนองาน
- เมื่อแล้วเสร็จทำการแจ้งให้เจ้าหน้าที่ตำรวจเจ้าของคดีมาเซ็นรับเอกสาร

3. การอนุมัติ

หัวหน้ากลุ่มงานนิติเวช นายแพทย์จิรวัฒน์ ตีระเดชะวาทย์ นายแพทย์ชำนาญการพิเศษ

4. บทสรุป

การจัดทำแผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่นๆ ได้อย่างมีประสิทธิภาพ

หมายเหตุ:

- แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

คำแนะนำ

- ควรทดสอบแผน BCP เป็นประจำ
- ควรฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

สรุปประเด็นที่ควรดำเนินการ

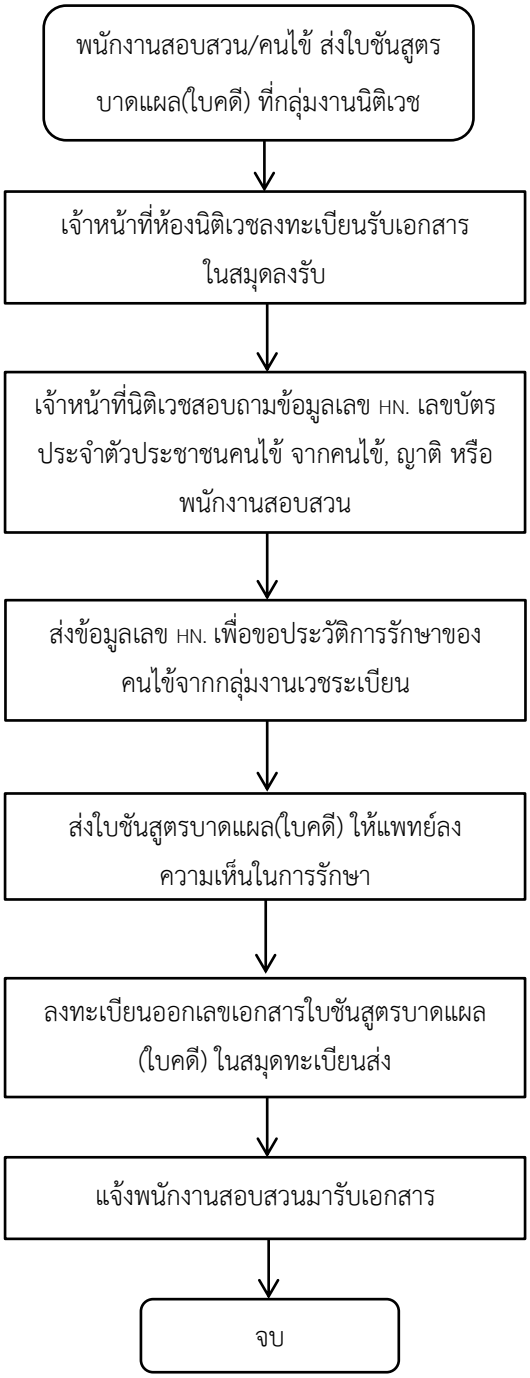
สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน ไม่เข้าเว็บไซต์อื่น ๆ ที่เสี่ยงจะทำให้เกิดอันตรายต่อระบบ	/		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ มีการวางแผนรับมือ และอบรมวิธีการรับมือเมื่อเกิดเหตุการณ์ที่โดน ransomware attack ขึ้น โดนมีการทดสอบแผนเป็นประจำ	/		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้ ทำการประสานงานกับเจ้าหน้าที่ตำรวจ ญาติ และผู้เกี่ยวข้อง เพื่อทำให้การทำงานง่ายขึ้น และปฏิบัติงานอย่างรวดเร็วเพื่อให้ทันเวลาที่กำหนด		/	
การปฏิบัติหลังระบบกลับสู่ปรกติ กลับมาใช้ระบบงานเดิมแต่ยังมีการนำขั้นตอนการทำงานที่มีในแผนมาปรับใช้ด้วยเพื่อให้งานมีประสิทธิภาพ มากยิ่งขึ้น	/		

U =ดำเนินการได้เองระดับหน่วยงาน

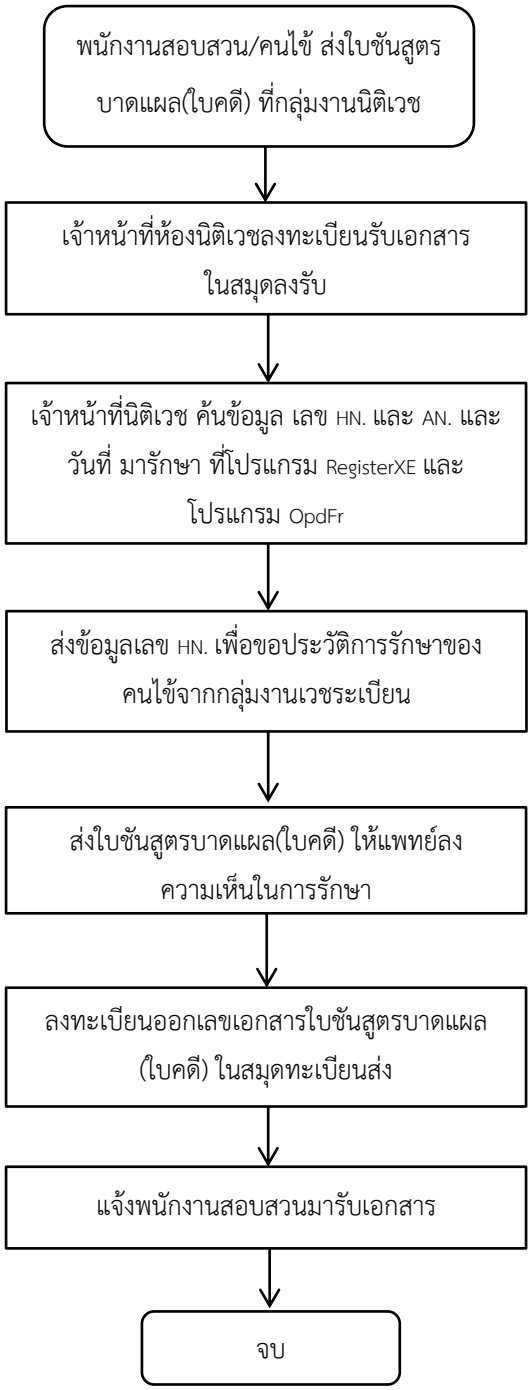
S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT

Flow chart การให้บริการใบชันสูตรบาดแผล (ใบคดี)
กรณีระบบคอมพิวเตอร์ใช้งานไม่ได้



Flow chart การให้บริการใบชันสูตรบาดแผล (ใบคดี)
กรณีระบบคอมพิวเตอร์ใช้งานได้ปกติ



ภาคผนวก

1. ตัวอย่างสมุดทะเบียนรับใบชันสูตรบาดแผล(ใบคดี)

เลขทะเบียนรับ	ลงวันที่	จาก (สถานีตำรวจ)	ถึง	ชื่อ-สกุล	การปฏิบัติงาน	หมายเหตุ

2. ตัวอย่างสมุดทะเบียนส่งใบชันสูตรบาดแผล(ใบคดี)

เลขทะเบียนส่ง	ลงวันที่	จาก	ถึง (สถานีตำรวจ)	ชื่อ-สกุล	การปฏิบัติงาน	หมายเหตุ