

แผนรับมือ Business Continuity Plan (BCP)

กลุ่มงานการแพทย์แผนไทยและการแพทย์ทางเลือก โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

แผนก: กลุ่มงานการแพทย์แผนไทยและการแพทย์ทางเลือก

ผู้รับผิดชอบ: พญ.จิระภา พันธุเศรษฐ์ หัวหน้ากลุ่มงานการแพทย์แผนไทยและการแพทย์ทางเลือก

1. บทนำ

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

ปัญหา

- ระบุทริกเกอร์ปัญหาจากเหตุการณ์ ransomware attack:
 - การเข้าถึงข้อมูลต่างๆ โดยเฉพาะการเข้าในระบบอินเทอร์เน็ต, Email, line, Wifi ต้องคำนึงถึงความปลอดภัยที่อาจเป็นช่องโหว่ในการถูกแฮกข้อมูล
 - ควรทำการสำรองข้อมูล (Backup) เป็นประจำและการเก็บข้อมูลแบบ Manual ยังมีความสำคัญ
- วิเคราะห์สาเหตุของปัญหา:
 - มีการเข้าถึง Application ที่ไม่เกี่ยวข้องกับการทำงาน ผ่านเครื่องคอมพิวเตอร์ในแผนกต่างๆ ทำให้เกิดช่องโหว่ในการแฮกข้อมูลได้
 - รหัสเข้าเครื่องและโปรแกรมต่างๆ ง่ายต่อการคาดเดา
 - เครื่องที่มีข้อมูลสำคัญเช่น Database ไม่ควรมีการเชื่อมต่อกับระบบอินเทอร์เน็ตสาธารณะ
- ระบุแนวทางการแก้ไขปัญหามูลค่า
 - ใช้รหัสเข้าระบบที่รัดกุมยากต่อการคาดเดา
 - ควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ
 - บันทึกข้อมูลเป็นระบบ Manual เช่น ทะเบียนการเข้ารับการรักษาประจำวัน
 - ทำการสำรองข้อมูล (Backup) เป็นประจำ
 - ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมด ถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด ควรมีการติดตั้งโปรแกรมป้องกันมัลแวร์ลงบนเครื่องคอมพิวเตอร์ทุกเครื่อง

อุปสรรค

- ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack:
 - เจ้าหน้าที่ขาดความรู้ในเรื่องการป้องกันตนเองจากการโจมตีทางไซเบอร์
- วิเคราะห์สาเหตุของอุปสรรค:
 - หน่วยงานไม่ได้มีการจัดอบรมให้ความรู้หรือสร้างความตระหนักในเรื่องของการป้องกันการโจมตีทางไซเบอร์ และเจ้าหน้าที่ขาดความใส่ใจ เรื่องการใช้รหัสที่รัดกุมรวมถึงการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัยผ่านเครื่องคอมพิวเตอร์ของหน่วยงาน
- แนวทางการแก้ไขอุปสรรค:
 - ให้ความรู้เกี่ยวกับการใช้งานและการป้องกันตนเองที่ถูกต้องจากการโจมตีทางไซเบอร์

ฟอร์มนี้จัดทำขึ้นเพื่อให้แต่ละแผนกในโรงพยาบาลอุดรธานีสามารถจัดทำแผนรับมือ Business Continuity Plan (BCP) กรณีเกิดเหตุการณ์ ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้ แผน BCP นี้จะช่วย
ให้แต่ละแผนกสามารถดำเนินงานต่อเนื่องได้อย่างมีประสิทธิภาพ แม้จะเผชิญกับเหตุการณ์วิกฤต

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- **ผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก**
 - ไม่สามารถสืบค้นฐานข้อมูลเดิมผู้ป่วยในการรักษา และไม่สามารถบันทึกประวัติการรักษาในระบบได้
 - การเตรียมเวชระเบียน ทำให้การให้บริการล่าช้า เนื่องจากไม่มีข้อมูลเดิม ต้องใช้เวลาในการซักประวัตินานกว่าปกติ
 - ทำให้ระบบจองคิวออนไลน์ล่ม จำนวนผู้รับบริการลดลง
 - เข้าระบบคิดค่าบริการไม่ได้
- **ผลกระทบต่อผู้ป่วย ญาติ และบุคลากร**
 - ไม่สามารถสืบค้นประวัติ ฐานข้อมูลเดิมผู้ป่วยได้
 - ผลกระทบต่อผู้ป่วยและญาติ ไม่สามารถจองนัดออนไลน์ ทำให้ไม่สะดวกต่อการมารับบริการ
 - ผลกระทบต่อบุคลากร ระบบการให้บริการล่าช้า จำนวนการเข้ารับบริการลดลงโรงพยาบาล สูญเสียรายได้
ศักยภาพไม่ได้

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack
 - ทบทวน/จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน >ควบคุมการเข้าถึงเครือข่าย > สำรองข้อมูลที่สำคัญอย่างน้อย 2 ระบบไว้ในอุปกรณ์จัดเก็บข้อมูล ที่ไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์
- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น
 - เปลี่ยนระบบงานบริการไปใช้ในรูปแบบ Manual (ในรูปแบบเอกสาร)
- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
 - แจ้ง อธิบาย โดยติดประกาศและประชาสัมพันธ์ให้ผู้ป่วย ญาติ และบุคลากรทราบ และเข้าใจถึงสถานการณ์ เพื่อลดความขัดแย้ง หรือความเข้าใจผิดที่อาจจะเกิดขึ้นได้

2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack
- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน
- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน
 - **การเตรียมเวชระเบียน** : ใช้ใบสำเนาเวชระเบียน และสำรองข้อมูลผู้ป่วยที่มาใช้บริการลงใน microsoft excel, google drive จากนั้นให้เวชระเบียนลงทะเบียนผู้ป่วย ตรวจสอบสิทธิ์ผู้ป่วย แต่ละรอบการนัดบริการ
ผู้รับผิดชอบ : พนักงานธุรการและผู้ช่วยเหลือคนไข้
ระยะเวลาที่ใช้ : 15-30 นาที/รอบ
 - **การคัดกรองผู้ป่วย** : พยาบาลคัดกรองและประเมินผู้ป่วย บันทึกข้อมูลผู้ป่วยใน google drive
ผู้รับผิดชอบ : พยาบาลวิชาชีพ
ระยะเวลาที่ใช้ : 1-3 นาที/ราย

- การตรวจรักษาของแพทย์ /แพทย์แผนไทย : แพทย์ / แพทย์แผนไทยตรวจรักษาและสั่งจ่ายยา บันทึกข้อมูลผู้ป่วยใน google drive
ผู้รับผิดชอบ : แพทย์ / แพทย์แผนไทย
ระยะเวลาที่ใช้ : 5-10นาทึ/ราย
- ระบบการคิดค่าบริการ : เจ้าหน้าที่ธุรการขอข้อมูลผู้รับบริการโดยละเอียด เพื่อเดินไปชำระเงินและปิดสิทธิ์การรักษาที่การเงิน นำใบเสร็จที่ได้รับมาแนบประกอบใบรับรองแพทย์
ผู้รับผิดชอบ : พนักงานธุรการและผู้ช่วยเหลือคนไข้
ระยะเวลาที่ใช้ : 5-10 นาที/รอบ
- ระบบการจองคิวนัดนัด : จองคิวนัดนัดโดยการโทรนัดหมาย และบันทึกคิวนัดของผู้รับบริการ
ในรูปแบบเอกสารการจอง
ผู้รับผิดชอบ : พนักงานธุรการและผู้ช่วยเหลือคนไข้
ระยะเวลาที่ใช้ : 1-3 นาที/ราย
- การจองคิวนัดฝังเข็ม: มีระบบจองนัดทางไลน์กลุ่ม / Official account
ผู้รับผิดชอบ : พยาบาลและผู้ช่วยเหลือคนไข้
ระยะเวลา : 1- 3 นาที

2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP
 - คอมพิวเตอร์ เครื่องสำรองข้อมูล และเครือข่ายอินเทอร์เน็ตที่มีความทันสมัยและปลอดภัย และ ของบสนับสนุนจากโรงพยาบาล
- ระบุแหล่งที่มาของทรัพยากร : โรงพยาบาลอุดรธานี

2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP
 - Call Tree คือ การซ้อมการแจ้งเหตุฉุกเฉินให้กับสมาชิกทีมงานที่เกี่ยวข้องตามผัง รายชื่อทางโทรศัพท์หรือช่องทางอื่น ๆ ที่สามารถติดต่อ และยืนยันการรับแจ้งเหตุได้ อย่างทันการณ์
 - Tabletop Testing คือ การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้อง โดยจำลองโจทย์สถานการณ์ขึ้นมา และทดลองนำแผน BCP มาพิจารณาว่า ใช้ตอบ โจทย์แต่ละขั้นตอนได้หรือไม่
 - Simulation คือ การทดสอบโดยจำลองสถานการณ์เสมือนจริง และทดลองนำแผน BCP มาประยุกต์ใช้
 - Full BCP Exercise คือ การทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้
 - การทดสอบโดยจำลองสถานการณ์เสมือนจริง

3. เอกสารแนบ แผนงาน (เอกสารแนบท้าย)

4. การอนุมัติ

(นางจิระภา พันธุเศรษฐ์)
นายแพทย์ชำนาญการพิเศษ
หัวหน้ากลุ่มงานการแพทย์แผนไทยฯ

5. บทสรุป

ฟอร์มนี้เป็นแนวทางสำหรับแต่ละแผนกในการจัดทำแผน BCP แผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่น ๆ ได้อย่างมีประสิทธิภาพ

หมายเหตุ:

- ฟอร์มนี้สามารถปรับแต่งให้เหมาะกับแต่ละแผนกได้
- แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

แหล่งข้อมูล

คำแนะนำ

- ควรจัดทำแผน BCP ร่วมกับผู้เชี่ยวชาญด้านไอที
- ควรทดสอบแผน BCP เป็นประจำ
- ควรฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1. จัดทำแนวทาง/ทบทวนข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน			/
2. ควบคุมการเข้าถึงเครือข่ายภายนอก ของอุปกรณ์ที่มีข้อมูลสำคัญ	/		
3. สำรองข้อมูลที่สำคัญอย่างน้อย 2 ระบบไว้ในอุปกรณ์จัดเก็บข้อมูล ที่ไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์	/		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1. ทบทวนและซักซ้อมตามแผน BCP ปีละ 1 ครั้ง	/		
2. สำรองข้อมูลที่สำคัญทุก 6 เดือน			/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1. แจ้งและอธิบายให้บุคลากรที่เกี่ยวข้องทราบถึงสถานการณ์ที่เกิดขึ้น	/		
2. ดำเนินการตามแผน BCP	/		
3. แจ้งผู้มารับบริการให้ทราบและปฏิบัติตามแนวทางการแก้ไข	/		
การปฏิบัติหลังระบบกลับสู่ปรกติ			
1. ตรวจสอบความเสียหายของข้อมูล และดำเนินการแก้ไข	/		
2. ประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้อง ทบทวนแผน BCP		/	

สรุปประเด็นที่ควรดำเนินการ

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT

แผนรับมือ Business Continuity Plan (BCP) กรณีเกิดเหตุการณ์ ransomware attack

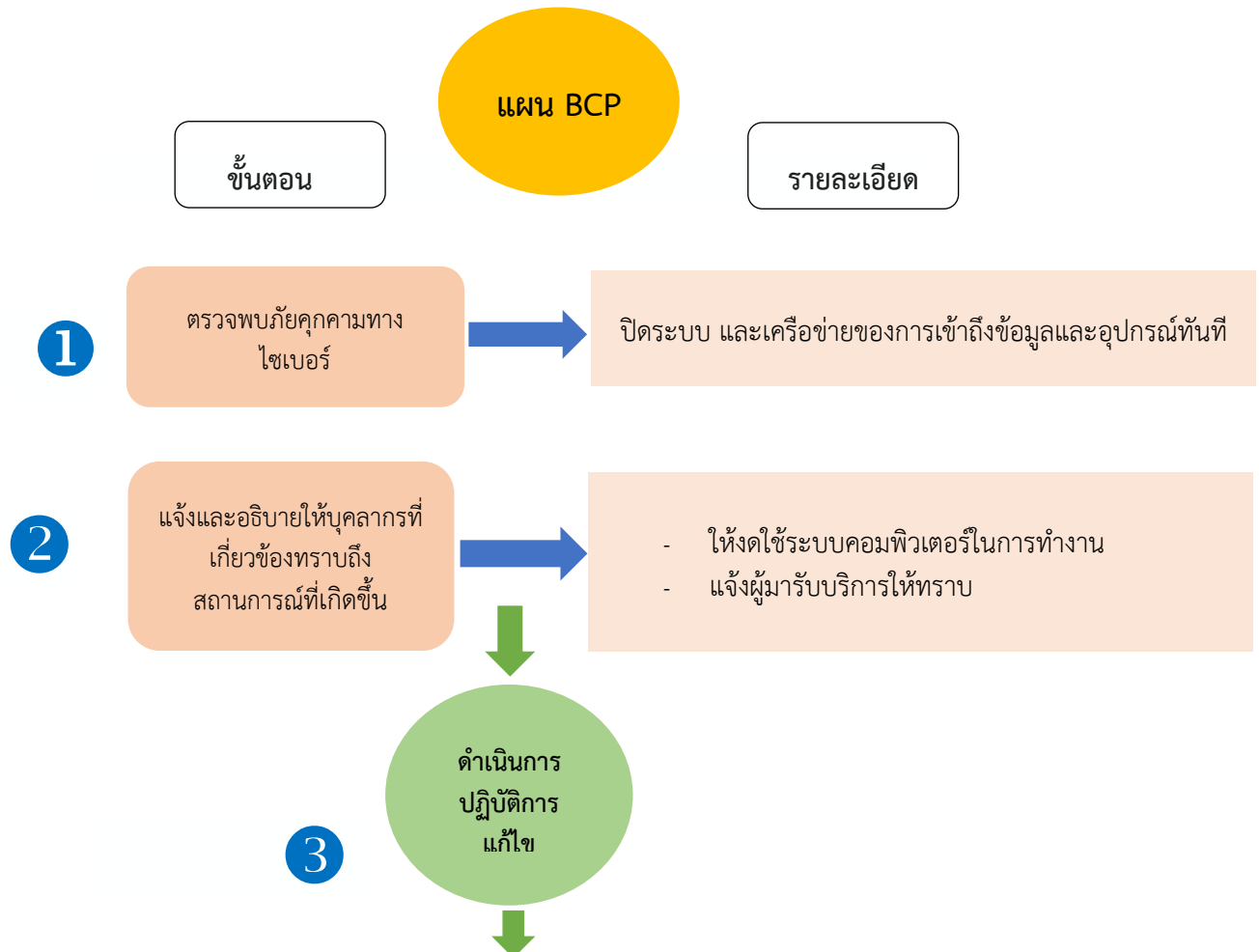
กลุ่มงานการแพทย์แผนไทยและการแพทย์ทางเลือก โรงพยาบาลอุดรธานี

ผู้รับผิดชอบ : พญ.จิระภา พันธุ์เศรษฐ์ หัวหน้ากลุ่มงานการแพทย์แผนไทยและการแพทย์ทางเลือก

เหตุการณ์ : โรงพยาบาลอุดรธานี โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

- ตรวจพบภัยคุกคามทางไซเบอร์
- แจ้งและอธิบายให้บุคลากรที่เกี่ยวข้องทราบถึงสถานการณ์ที่เกิดขึ้น
- ดำเนินการปฏิบัติการแก้ไข

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน



รายละเอียด :

- ลงทะเบียนผู้มารับบริการในสมุดบันทึกเวชระเบียนของห้องตรวจ
- จัดคิวให้ผู้รับบริการตามลำดับการมาถึงจุดบริการห้องตรวจ
- ชักประวัติ และบันทึกข้อมูลการตรวจรักษาแบบ Manual
- แนะนำผู้รับบริการนำยาเดิมมาด้วยทุกครั้งที่ได้รับบริการที่ห้องตรวจ
- ** เจ้าหน้าที่ประสานแจ้งให้หน่วยงานในเครือข่ายสาธารณสุขที่เกี่ยวข้อง แจ้งผู้ที่จะมาเข้ารับบริการในโรงพยาบาลอุดรธานี
- ให้นำประวัติการรักษาและยาเดิม (ถ้ามี) มาด้วยทุกครั้ง
- กรณีประสานงานระหว่างหน่วยงาน ใช้การสื่อสารทางโทรศัพท์
- การขอคำปรึกษาและนัดหมายคิวจากผู้รับบริการ ที่ใช้ระบบ Online ในการติดต่อ ติดต่อประกาศให้ผู้รับบริการทราบปรับเป็นการโทรจองเพื่อนัดหมายและการขอคำปรึกษา
- กรณีคนไข้มารับบริการนัดหมายครั้งต่อไป ใช้การเขียนนัดหมายในใบนัด แทนการปรี้นใบนัดในระบบนัด

