ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี

กลุ่มงาน : ประกันสุขภาพ

ผู้รับผิดชอบ: หัวหน้ากลุ่มงานประกันสุขภาพ,หัวหน้างาน และเจ้าหน้าที่กลุ่มงานประกันสุขภาพ

1. บทนำ

จากเหตุการณ์ Ransomware attack ในวันที่ 9 ธันวาคม 2566 ส่งผลกระทบต่อระบบบริการตรวจสอบสิทธิ, ระบบบันทึกข้อมูลค่ารักษาพยาบาลผู้ป่วยใน และระบบจัดเก็บรายได้ค่ารักษาพยาบาล กลุ่มงานประกันสุขภาพ จึงได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือเหตุการณ์ดังกล่าว ดังนี้

ปัญหา

1. จากเหตุการณ์ Ransomware attack ส่งผลกระทบต่อการทำงานของระบบคอมพิวเตอร์ และระบบสารสนเทศทางการแพทย์ ทำให้ไม่สามารถใช้โปรแกรมต่างๆ เพื่อสืบค้นฐานข้อมูลสิทธิการรักษาพยาบาลของผู้ป่วย ในการตรวจสอบสิทธิการรักษาพยาบาล จึงต้องสอบถามสิทธิการรักษาพยาบาลจากผู้ป่วย พร้อมถ่ายเอกสารบัตรประจำตัวประชาชนผู้ป่วย และ/หรือ หลักฐานใบส่งตัวจากต้นสังกัด เพื่อการตรวจสอบสิทธิการรักษาพยาบาลเบื้องต้น ทำให้การบริการผู้ป่วยเกิดความล่าช้า
2. การตรวจสอบสิทธิการรักษาพยาบาล ที่ไม่ได้ตรวจสอบจากฐานข้อมูลสิทธิของต้นสังกัดต่างๆ ทำให้เกิดความเสี่ยงในการเรียกเก็บชดเชยค่ารักษาพยาบาล
3. ผู้ป่วยนอนโรงพยาบาลที่ได้รับการออก HN และ AN เรียบร้อยแล้วก่อนเหตุการณ์ Ransomware attack ไม่สามารถใช้เลขเดิมได้ จำเป็นต้องลงทะเบียนใหม่ เพื่อให้สามารถเชื่อมต่อกับระบบ HIS ได้ ซึ่งมีผลกระทบต่อการเรียกเก็บชดเชยค่ารักษาพยาบาล เนื่องจากใน Visit เดียวกัน ผู้ป่วยมี HN และ AN หลายเลข
4. โปรแกรมที่ใช้ประมวลผล รวมถึงโปรแกรมที่ใช้นำเข้าข้อมูล 16 แฟ้ม หายไปทั้งหมด ทำให้เจ้าหน้าที่ต้องบันทึกค่ารักษาพยาบาลใหม่ทั้งหมด ตั้งแต่ข้อมูลทั่วไปของผู้ป่วย ข้อมูลการวินิจฉัยโรคซึ่งมีผลต่อน้ำหนักสัมพัทธ์ของโรค รวมถึงข้อมูลค่ารักษาพยาบาล เนื่องจากไม่สามารถนำเข้าข้อมูลได้

วิเคราะห์สาเหตุของปัญหา

1. ไม่มีการสำรองข้อมูลในฐานสำรอง ทำให้ไม่สามารถกู้คืนข้อมูลได้
2. การป้องกันไวรัสระบบคอมพิวเตอร์ และระบบรักษาความปลอดภัยด้านข้อมูลสารสนเทศของโรงพยาบาล ไม่รัดกุม รวมถึงโปรแกรมป้องกันมัลแวร์ไม่อัพเดท
3. ไม่มีแผนรับมือเมื่อเกิดสถานการณ์ฉุกเฉิน ขาดการเฝ้าระวังเหตุการณ์ดังกล่าว

ระบุแนวทางการแก้ไขปัญหา

1. แจ้งบุคลากรในหน่วยงานให้ปฏิบัติตามแผนฉุกเฉินที่โรงพยาบาลประกาศใช้
2. สื่อสารให้ผู้รับบริการทราบถึงปัญหาและระยะเวลาการรอคอย เพื่อลดความกดดันของผู้รับบริการ
3. เพิ่มอัตรากำลังคนทันที เพื่อรับมือกับการปฏิบัติงานแบบ Manual
4. จัดหาครุภัณฑ์และอุปกรณ์เพิ่ม เช่น คอมพิวเตอร์ ปริ้นท์เตอร์ และอุปกรณ์อื่นๆที่จำเป็นต่อการใช้งาน

อุปสรรค

1. เจ้าหน้าที่ไม่ทราบแผนรับมือและการปฏิบัติงานในสถานการณ์ระบบล่มทำให้เกิดความล่าช้าในการให้บริการ
2. การกู้คืนและแก้ไขโปรแกรมที่จำเป็นเป็นไปอย่างล่าช้า เนื่องจากมีเจ้าหน้าที่ผู้รับผิดชอบไม่เพียงพอ

วิเคราะห์สาเหตุของอุปสรรค

1. ไม่มีแนวทางปฏิบัติที่ชัดเจนให้ผู้ปฏิบัติงานได้ถือปฏิบัติ

2. ไม่มีการแจ้งให้เจ้าหน้าที่ผู้ปฏิบัติงานทราบถึงความรุนแรงของสถานการณ์และระยะเวลาในการแก้ไขสถานการณ์ ทำให้หน้างานไม่สามารถให้ข้อมูลแก่ผู้มารับบริการได้

ระบุแนวทางแก้ไขอุปสรรค

1. จัดทำแผนการปฏิบัติงานในสถานการณ์ระบบล่ม กำหนดระยะเวลาที่แน่นอนว่าระบบล่มนานเท่าใดจึงประกาศใช้แผน และซักซ้อมเจ้าหน้าที่ให้ปฏิบัติงานตามขั้นตอนอย่างเคร่งครัด

2. เพิ่มอัตรากำลังของเจ้าหน้าที่ให้เพียงพอต่อการรับมือในสถานการณ์ฉุกเฉินทั้งผู้ปฏิบัติงานและเจ้าหน้าที่ IT เพื่อช่วยแก้ไขสถานการณ์กรณีที่หน่วยงานต้องการการสนับสนุนด้าน IT

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

ผลกระทบของ Ransomware attack ที่มีผลต่องานบริการของแผนก

1. การตรวจสอบสิทธิผู้รับบริการ
2. การบันทึกค่ารักษาพยาบาล
3. การเรียกเก็บค่าบริการฯ จากต้นสังกัดกองทุน หรือหน่วยบริการต่างๆ

ผลกระทบของ Ransomware attack ที่มีผลต่อต่อผู้ป่วย ญาติ และบุคลากร

1. เพิ่มระยะเวลารอคอยของผู้รับบริการ เนื่องจากการตรวจสอบสิทธิและการบันทึกข้อมูลค่ารักษาพยาบาลต้องทำเป็นเอกสาร
2. การบันทึกข้อมูลด้วยเอกสารทำให้เกิดความล่าช้าในการปฏิบัติงานของเจ้าหน้าที่
3. โรงพยาบาลไม่สามารถเรียกเก็บค่ารักษาพยาบาล จากผู้รับบริการ และกองทุนอื่นๆ ได้ครบถ้วน

2.2 กลยุทธ์

1. จัดให้มีการสำรองข้อมูลผู้ป่วย ในฐานเก็บข้อมูลสำรองของโรงพยาบาลอย่างสม่ำเสมอ
2. กำหนดแผนการปฏิบัติงานในสถานการณ์ฉุกเฉินให้ชัดเจน เช่น ระยะเวลา ความรุนแรง เพื่อให้ผู้ปฏิบัติงานได้ประเมินสถานการณ์ และจัดอัตรากำลังให้เพียงพอ
3. ให้ผู้รับบริการสามารถตรวจสอบฐานข้อมูลสิทธิการรักษาพยาบาลของตนเองเบื้องต้น รวมถึงการยืนยันตัวตนในโทรศัพท์มือถือของตนเองได้

- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น

1. การกำหนดสิทธิ์ในการใช้งานโปรแกรมต่างๆ ในคอมพิวเตอร์ระบบ LAN
2. จัดทำระบบสำรองข้อมูลค่ารักษาพยาบาลในหน่วยงาน เช่น จัดเก็บในไฟล์ excel หรือสำรองข้อมูลในระบบ cloud เป็นต้น พร้อมติดตั้งระบบป้องกันไวรัสฯ และกำหนดเวลาการสำรองข้อมูลอัตโนมัติทุกวัน

- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร

- ประชาสัมพันธ์ให้ผู้ป่วยนำประวัติการมาบริการเดิมมาด้วยทุกครั้ง เช่น ใบนัดผู้ป่วย หรือ เอกสารที่ระบุตัวตนผู้ป่วยที่มี HN, AN
- ประชาสัมพันธ์ให้ผู้มารับบริการรับทราบถึงสถานการณ์และความรุนแรงของปัญหา เพื่อให้ผู้มารับบริการเข้าใจและลดความกดดันในการรอรับการบริการ
- ชี้แจงวิธีการตรวจสอบสิทธิการรักษาพยาบาลเบื้องต้น และการยืนยันตัวตน ผ่าน Application ของสปสช.

ในโทรศัพท์มือถือของตนเอง

2.3 แผนปฏิบัติการ

- **ระบุขั้นตอนที่ชัดเจนในการรับมือกับ Ransomware attack**

1. จัดทำแผนรองรับการเกิดสถานการณ์ฯ ทั้งระดับโรงพยาบาลและระดับหน่วยงาน

2. ซักซ้อมแผนการปฏิบัติงานและขั้นตอนการปฏิบัติ ตามแผนรองรับฯ แก่เจ้าหน้าที่หน้างานให้ปฏิบัติไปในทิศทางเดียวกัน

3. กำชับให้เจ้าหน้าที่ในหน่วยงาน ปฏิบัติตามแนวทาง Cyber Security ของโรงพยาบาลอย่างเคร่งครัด

3.1 กลุ่มที่ปฏิบัติงานด้วยระบบ LAN Only : ห้ามเข้าถึงระบบ Internet เด็ดขาด ได้แก่ เจ้าหน้าที่บันทึกข้อมูลค่ารักษาพยาบาลผู้ป่วยใน

3.2 กลุ่มที่ปฏิบัติงานด้วยระบบ LAN และเข้าเฉพาะเว็บไซต์ที่เกี่ยวข้องกับการปฏิบัติงาน ได้แก่ เจ้าหน้าที่ตรวจสอบสิทธิ และเจ้าหน้าที่งานเรียกเก็บค่ารักษาพยาบาล

3.3 กลุ่มที่ปฏิบัติงานด้วยระบบ Internet Only : ห้ามเข้าถึงระบบ Lan เด็ดขาด

4. เมื่อผู้ป่วยมารับบริการ เจ้าหน้าที่ตรวจสอบสิทธิ แนะนำวิธีการตรวจสอบสิทธิการรักษาพยาบาลเบื้องต้น และการยืนยันตัวตน ผ่าน Application ของสปสช. ในโทรศัพท์มือถือของตนเอง

5. จัดเก็บเอกสารทางการเงิน ให้เป็นระเบียบเรียบร้อย เพื่อให้สะดวกต่อการค้นหาและการนำมาบันทึกข้อมูลค่ารักษาพยาบาล ทั้งในช่วงเวลาที่เกิดเหตุการณ์ฉุกเฉิน หรือภายหลังระบบกลับเข้าสู่ภาวะปกติ

- **ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน**

ลำดับ/ผู้เกี่ยวข้อง	หน้าที่
ผู้ที่ได้รับผลกระทบจากเหตุการณ์ - ผู้ปฏิบัติงาน ณ ขณะนั้น	1. แจ้งเหตุ หรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามเกิดขึ้น
หัวหน้ากลุ่มงาน, หัวหน้างาน	1. รับแจ้งเหตุ หรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
ผู้รับแจ้งเหตุ - หัวหน้ากลุ่มงาน - หัวหน้างาน - คณะกรรมการสารสนเทศ	1. รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ 2. ให้คำแนะนำปรึกษาบุคลากรเกี่ยวกับการป้องกัน จุดอ่อน ข้อควรระมัดระวัง และเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน 3.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
คณะกรรมการสารสนเทศ - หน่วยงาน IT ของโรงพยาบาล	1. เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามอุปกรณ์ตรวจจับความเสี่ยงที่อาจก่อให้เกิดภัยคุกคามด้านไซเบอร์ 2.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน

	ข้อควรระมัดระวังและแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน 3.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
ผู้บริหารของโรงพยาบาล	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์

หมายเหตุ คณะกรรมการสารสนเทศ ควรเป็นบุคลากรที่มีความรู้ ความสามารถ ประสบการณ์ ผ่านการอบรมด้าน Cyber security ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้าน เกี่ยวกับการรักษาความปลอดภัยไซเบอร์

- ***ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน***
    1. ขั้นตอนการจัดทำแผนฯ : 1-2 วัน
    2. ขั้นตอนการซักซ้อมแผนฯ : 1-2 วัน
    3. ขั้นตอนการปฏิบัติงานตามแผนฯ : ดำเนินการทุกวัน

2.4 ทรัพยากร

- ***ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP***
    1. จัดหาเครื่องคอมพิวเตอร์แบบ stand alone สำรองข้อมูลทั่วไป เพื่อค้นหาชื่อผู้ป่วย
    2. จัดเตรียมสถานที่จัดเก็บที่มีความมั่นคงปลอดภัย เพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูล และพยานวัตถุอื่นๆที่สำคัญ
    3. จัดหาอุปกรณ์และซอฟแวร์ สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์
    4. จัดหาครุภัณฑ์สำรองเพิ่มเติม เช่น เครื่อง printer ใช้ในกรณีออกผลแบบ manual
    5. จัดหาระบบตรวจจับ และป้องกันภัยคุกคามไซเบอร์ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Endpoint Detection & Response)
    6. จัดตั้งทีมรับมือภัยคุกคามทางไซเบอร์ ส่งบุคลากรเข้ารับการฝึกอบรมด้าน Cyber Security
    7. จัดอัตรากำลังคนเสริมการปฏิบัติงานเมื่อเกิดเหตุการณ์

- ***ระบุแหล่งที่มาของทรัพยากร***

    งบประมาณจาก โรงพยาบาลอุดรธานี จัดหาสนับสนุนอุปกรณ์การทำงาน

2.5 การทดสอบและฝึกอบรม

- ***ระบุวิธีการทดสอบแผน BCP***

    1. กำหนดแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือการให้หัวหน้าหน่วยงานเป็นผู้ประเมินผู้ปฏิบัติงานในแต่ละหน่วยต่อสถานการณ์ ransomware ที่เกิดขึ้น เมื่อประเมินความรับรู้เสร็จแล้ว จัดทำรายการสรุปผลการประเมิน จากนั้นให้คิดเป็นร้อยละการรับรู้และจัดทำเสนอแนะแนวทางแก้ไข ซึ่งแบบประเมินตนเอง ให้ผู้ปฏิบัติงานใช้ระบบตอบคำถามว่าระเบียบข้อใดบ้างที่ปฏิบัติตาม ระเบียบข้อใดที่ไม่ปฏิบัติสาเหตุที่ทำให้ไม่ปฏิบัติตามระเบียบคืออะไร

2. การจำลองสถานการณ์ ransomware เพื่อทดสอบว่าผู้ปฏิบัติงานสามารถปฏิบัติตามระเบียบที่ปฏิบัติตรงตามที่กำหนดไว้

- **ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้**

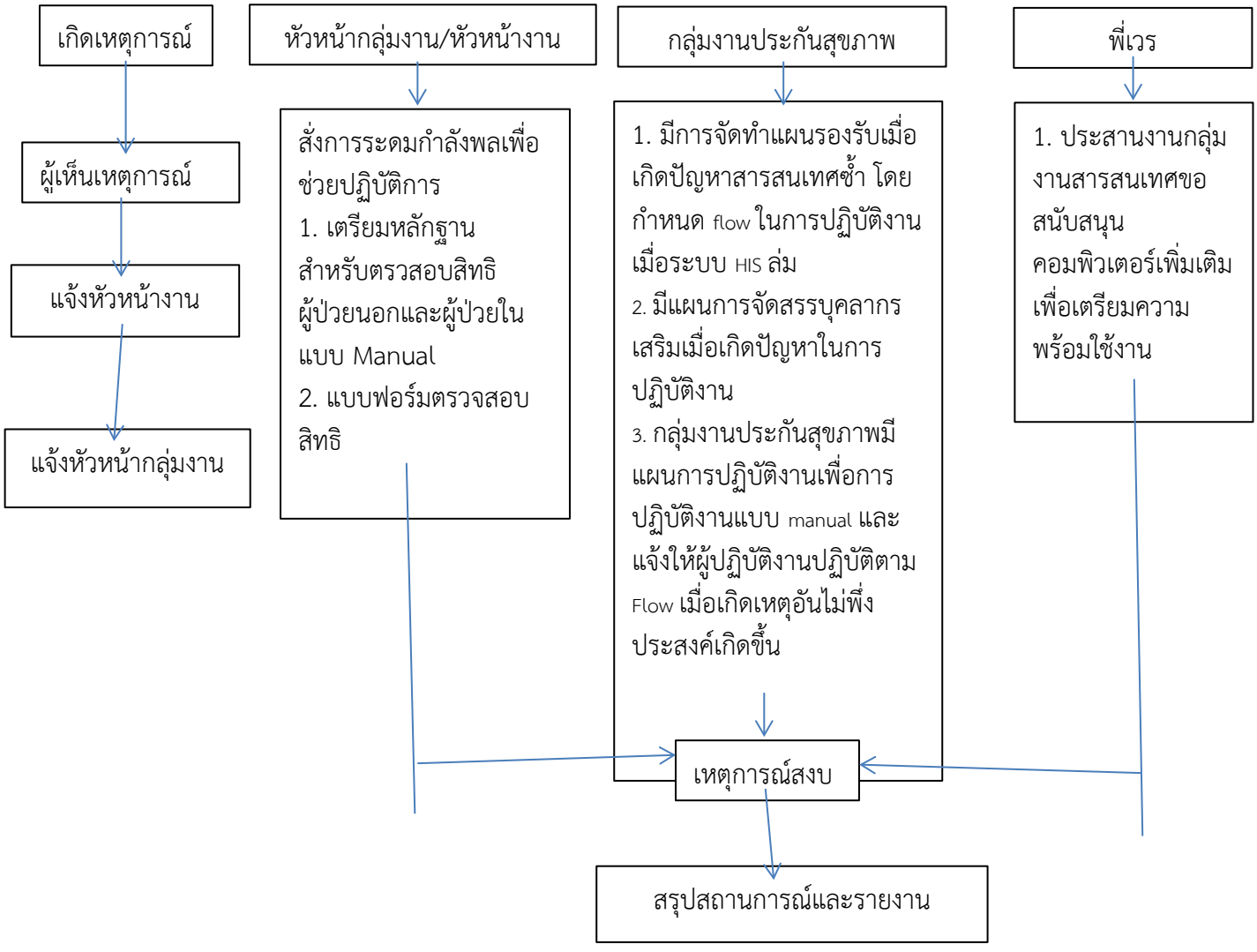
1. การให้ความรู้ซ้ำหลายๆครั้ง เปลี่ยนช่องทางการให้ข้อมูล หรือเพิ่มช่องทางการให้ข้อมูล กำหนดมาตรการให้รางวัลแก่ผู้ที่สนใจและรับรู้ระเบียบได้อย่างดี
2. จัดทำการจำลองสถานการณ์ Ransomware อย่างสม่ำเสมอเพื่อให้ผู้ปฏิบัติงานได้ทบทวนแนวทางปฏิบัติอย่างต่อเนื่อง
3. รวบรวมข้อเสนอแนะและข้อคิดเห็นจากผู้ปฏิบัติงานที่เข้าร่วมการให้ความรู้ หรือจากการผ่านจำลองสถานการณ์ เพื่อใช้ในการปรับปรุงแก้ไขแผนให้สามารถใช้งานได้จริง

3. เอกสารแนบ

- **แผนงาน**

1. แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์ กลุ่มงานประกันสุขภาพ โรงพยาบาลอุดรธานี

แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์
กลุ่มงานประกันสุขภาพ โรงพยาบาลอุดรธานี



2. แบบฟอร์ม“ถอดบทเรียน กรณีการถูกโจมตีทาง Cyber ประเภท Ransomware โรงพยาบาลอุดรธานี

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1. มอบหมายให้คณะกรรมการสารสนเทศตรวจสอบ Back up ข้อมูลของโรงพยาบาลอย่างสม่ำเสมอ		/	/
2. การให้งานสารสนเทศที่จำเป็นต้องใช้ LAN และเว็บไซต์ต้องกำหนดหรือจำกัดสิทธิการเข้าถึงข้อมูล	/	/	/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1. เชื่อมต่อข้อมูลเลขบัตรประชาชนของระบบ HIS เพื่อใช้ยืนยันตัวตนผู้ป่วยหากเกิดกรณีดังกล่าวซ้ำ			/
2. ให้ความรู้กับผู้ปฏิบัติงานได้เมื่อเกิดปัญหาสามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างเคร่งครัด	/	/	/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1. กำหนดช่องทางการสื่อสารเพื่อให้ผู้รับบริการรับทราบโดยทั่วกันและเข้าใจถึงสถานการณ์	/	/	/
การปฏิบัติหลังระบบกลับสู่ปกติ			
1. มีการ Back up ข้อมูล ให้เป็นปัจจุบัน		/	/

- รายชื่อผู้ติดต่อ เมื่อเกิดเหตุการณ์ฉุกเฉินทางระบบสารสนเทศ

    1. รายชื่อผู้ติดต่อ

        1. ภก.ดำรงเกียรติ ตั้งเจริญ รองผู้อำนวยการด้านการเงินการคลัง โรงพยาบาลอุดรธานี
        3. นายชูรัก เหล่าอรรคะ รักษาการหัวหน้ากลุ่มงานประกันสุขภาพ โรงพยาบาลอุดรธานี
        4. นางภคธรณ์ โภคสวัสดิ์ หัวหน้างานเรียกเก็บสิทธิบัตรประกันสุขภาพ (บัตรทอง)
        5. นายชัยวัฒน์ เรืองสมศรี หัวหน้างานเรียกเก็บวสิทธิบัตรประกันสังคม
        6. นางสาววริศรา วงศ์รัตนะ หัวหน้างานเรียกเก็บสิทธิเบิกจ่ายตรง
        7. นางฉัตรสุดา ทุมเสน หัวหน้างานเรียกเก็บสิทธิต่างด้าว, ท.99 และพรบ.รถ

- แบบฟอร์มที่จำเป็น

แบบฟอร์มรายการบริการและค่าบริการที่เกิด ณ ห้องตรวจ หรือจุดบริการอื่นๆ, แบบฟอร์มตรวจสอบสิทธิผู้ป่วยใน, แบบฟอร์มบันทึกค่ารักษาพยาบาล

4. การอนุมัติ

นายชูรัก เหล่าอรรคะ รักษาการหัวหน้ากลุ่มงานประกันสุขภาพ

5. บทสรุป

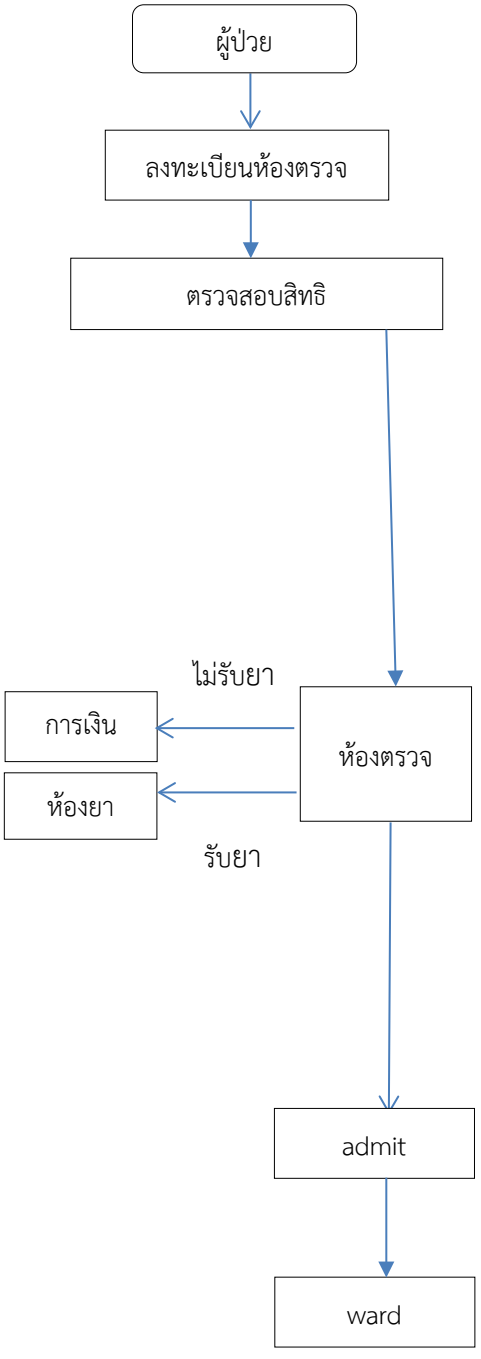
สรุปประเด็นที่ควรดำเนินการ

U= ดำเนินการได้เองระดับหน่วยงาน

S= ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I= ต้องได้รับการสนับสนุนจาก IT

Flow chart การบริการตรวจสอบสิทธิ กรณีระบบ HIS ล่ม

ผู้รับผิดชอบ	กิจกรรม	วิธีปฏิบัติ
จุดคัดกรอง/ประชาสัมพันธ์		- ชี้แจงสถานการณ์ฉุกเฉิน - แนะนำขั้นตอนรับบริการ และเอกสารที่ต้องเตรียม
เจ้าหน้าที่งานเวชระเบียน		จัดเตรียมเอกสารทางเวชระเบียน
เจ้าหน้าที่ตรวจสอบสิทธิ		1. รับเอกสารจากงานเวชระเบียน 2. .สอบถามผู้ป่วยใช้สิทธิการรักษาประเภทใด 3. แจ้งผู้ป่วยยืนยันตัวตนในการเข้ารับบริการ ด้วยการสแกน QR Code 4. ประทับตราสิทธิการรักษา และการยืนยันตัวตน ในเอกสาร 1.OPD card (เอกสารหมายเลข 1) 2.ใบสั่งยา (เอกสารหมาเลข 2) 3.ใบสำเนาบัตรปชช. ชุดที่ 2 5. แนะนำผู้ป่วยตรวจรักษา ณ ห้องตรวจต่างๆ ตามขั้นตอนรับบริการ
แพทย์ พยาบาล เจ้าหน้าที่ประจำห้องตรวจ/จุดบริการต่างๆ เภสัชกร เจ้าหน้าที่ห้องการเงิน		1. แพทย์ให้บริการตรวจรักษา หรือตรวจวินิจฉัยอื่นๆ พร้อมเขียนรหัสโรคและเขียนใบสั่งยาให้ชัดเจน 2. พยาบาล/จนท.ห้องตรวจ/จนท.ประจำจุดบริการ บันทึกรายการบริการและค่าใช้จ่าย ในแบบฟอร์มคิดค่าบริการของห้องตรวจ/จุดบริการ 3. กรณีไม่พบตราประทับการยืนยันตัวตน แนะนำผู้ป่วยยืนยันตัวตนเข้ารับบริการอีกครั้ง 4. เมื่อเสร็จสิ้นกระบวนการตรวจรักษาฯ ตรวจสอบรายการให้บริการในแบบฟอร์มคิดค่าบริการให้ครบถ้วน และเก็บรวบรวมส่งการเงินทุกเย็น กรณีผู้ป่วยไม่ได้ Admit แนะนำผู้ป่วย นำใบสั่งยายื่นที่ห้องยา
เจ้าหน้าที่ตรวจสอบสิทธิ		**กรณีผู้ป่วย Admit** 1. แนะนำผู้ป่วย ติดต่อตรวจสอบสิทธิ ที่กลุ่มงานประกันสุขภาพ ช่องบริการ 3-5 (อาคารผู้ป่วยนอกเดิม ทางไปศูนย์ราชการสะดวก รพ. อุดรธานี) 2. ถ่ายสำเนาบัตรประชาชนของผู้ป่วย ตรวจสอบสิทธิการรักษาพยาบาลจาก application NHSO หรือโทร 1330 3. อนุมัติสิทธิ์ และเขียนรายละเอียดสิทธิการรักษา ในแบบฟอร์มอนุมัติสิทธิ์ พร้อมแนบสำเนาบัตรประชาชน เพื่อนำไปยื่นแก่เจ้าหน้าที่บันทึกข้อมูลประจำหอผู้ป่วย