แผนรับมือ Business Continuity Plan (BCP) IT งานธนาคารเลือด โรงพยาบาลอุดรธานี

เหตุการณ์: โดน Ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 6 มีนาคม 2567
แผนก: งานธนาคารเลือด กลุ่มงานเทคนิคการแพทย์และพยาธิวิทยาคลินิก

ผู้รับผิดชอบ: หัวหน้ากลุ่มงาน, หัวหน้างานธนาคารเลือด

1. บทนำ

จากการโดน Ransomware attack ในวันที่ 9 ธันวาคม 2566 แผนกธนาคารเลือด ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ Ransomware attack ในครั้งนี้

ปัญหา

1. ปัญหาจากเหตุการณ์ Ransomware attack ส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ในหน่วยงานธนาคารเลือด ที่มีการเชื่อมข้อมูลของผู้ป่วยในระบบ HIS กับระบบ LIS งานธนาคารเลือด เริ่มจากการระบุตัวตนของผู้ป่วย (Patient Identify) จากทางหอผู้ป่วยมายังงานธนาคารเลือด เมื่อโดน Ransomware attack ทำให้ระบบ HIS ของทางโรงพยาบาลล่ม จึงไม่สามารถใช้โปรแกรมต่างๆได้ มีการแก้ปัญหาโดยใช้การเขียนด้วยลายมือ เช่น การระบุตัวตนผู้ป่วย การออกผลตรวจวิเคราะห์ต่างๆ การรับสิ่งส่งตรวจเข้างานธนาคารเลือดและจ่ายโลหิต
2. การค้นประวัติผู้ป่วยเก่า ประวัติผลหมู่เลือด ประวัติรับเลือดเป็นไปได้ยากเนื่องจากผลไม่เชื่อมต่อกับระบบ HIS ของโรงพยาบาล
3. ในการรับผลตรวจคัดกรองโลหิตบริจาคจากภาคบริการโลหิตแห่งชาติที่6 จังหวัดขอนแก่น ต้องใช้ระบบ LAN และอินเตอร์เน็ต เมื่อระบบล่มทำให้การนำเข้าข้อมูลผลตรวจไปเป็นด้วยความลำบาก ต้องทำระบบ Double เช็คในการนำเข้าข้อมูลแบบ Manual

- **วิเคราะห์สาเหตุของปัญหา**
  1. เมื่อโดน Ransomware attack ทำให้ระบบ HIS ของทางโรงพยาบาลล่ม จึงไม่สามารถใช้โปรแกรมต่างๆได้ และไม่มีโปรแกรมสำรองในกรณีที่ระบบ HIS และ LIS ล่ม ควรมีโปรแกรมที่สามารถทำงานได้ตามปกติ เช่น โปรแกรมค้นประวัติผู้บริจาคใน Note book ในการออกหน่วยรับบริจาคเคลื่อนที่ เผื่อกรณีดังกล่าวเกิดขึ้น
  2. ไม่มีระบบสัญญาณอินเตอร์เน็ตที่แยกจาก ระบบ LAN เพื่อใช้ในการรับผลตรวจคัดกรองโลหิตบริจาค จากสภากาชาดไทย

- **แนวทางการแก้ไขปัญหา**
  1. รายงานให้ผู้บังคับบัญชาทราบเพื่อดำเนินการแจ้งคณะกรรมการบริหารโรงพยาบาลอุดรธานี
  2. กำหนดขอบเขต / รายการตรวจ/ ข้อจำกัดการให้บริการ และแจ้งให้ผู้ใช้บริการทราบ
  3. บุคลากรในกลุ่มงานปฏิบัติตาม Flow ที่กำหนดไว้เบื้องต้นเพื่อลดความผิดพลาดในทุกกระบวนการของงานธนาคารเลือด
  4. เพิ่มอัตรากำลังคนทันที เพื่อรับมือกับการปฏิบัติงานแบบระบบ manual

อุปสรรค

- **อุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack**
  1. จำนวนอัตรากำลังของหน่วยงาน/และการจัดสรรบุคลากรเพิ่มเติมเมื่อมีเหตุการณ์ดังกล่าวเกิดขึ้น ณ เวลานั้นไม่เพียงพอต่อการรับต่อสถานการณ์ ทำให้ต้องจัดสรรในภายหลัง
  2. การดำเนินการรับมือกับเหตุการณ์ดังกล่าว ทุกหน่วยงานเป็นไปอย่างล่าช้าเพราะขาดประสบการณ์ หรือแผนรองรับมาก่อน
  3. ไม่มีโปรแกรมสำรองต่างๆไว้เผื่อกรณีดังกล่าวเกิดขึ้น
  4. ปัญหาการเข้าถึงข้อมูลส่วนตัว และประวัติอื่นๆของผู้ป่วย เช่น เลขบัตรประชาชน ผลการตรวจต่างๆ ประวัติการรับเลือด

- **วิเคราะห์สาเหตุของอุปสรรค**

1. เนื่องจากเหตุการณ์เกิดนอกเวลาราชการ ผู้ปฏิบัติในขณะนั้นมีอัตรากำลังไม่เพียงพอ จึงต้องเปลี่ยนวิธีปฏิบัติงาน เป็นแบบ manual จึงทำให้ผลการทำงานล่าช้า และมีข้อผิดพลาดในการระบุตัวตนของผู้ป่วย
2. ไม่มีการประกาศให้ผู้ปฏิบัติงานทราบถึงสถานการณ์ที่เกิดขึ้น
3. ไม่มีแนวทางการรับมือเหตุการณ์แบบนี้มาก่อน และไม่มีแผนรองรับให้ผู้ปฏิบัติงาน จึงเป็นการรับมือหน้างาน ณ ขณะนั้น

- **แนวทางการแก้ไขอุปสรรค**

1. มีแผนการจัดสรรบุคลากรเสริม เมื่อเกิดปัญหาสามารถเรียกเวร on call มาช่วยปฏิบัติงาน
2. งานตรวจวิเคราะห์มีแผนการปฏิบัติงาน เพื่อการปฏิบัติงาน แบบ manual และแจ้งให้ผู้ปฏิบัติงานปฏิบัติตาม Flow เมื่อเกิดเหตุอันไม่พึงประสงค์เกิดขึ้น
3. ให้ความรู้กับผู้ปฏิบัติงานให้สามารถปฏิบัติงานได้เมื่อเกิดปัญหา และต้องปฏิบัติตาม Flow หรือตามแนวทางที่กำหนดร่วมกันอย่างเคร่งครัด
4. ร่วมกันกำหนดแนวทางการรับมือ เผื่อในอนาคตเกิดเหตุการณ์ซ้ำ

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- **ผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก**

1. ระบบการจัดหาเลือดให้เพียงพอต่อผู้ป่วยมีปัญหา เนื่องจากเลือดที่รับบริจาคไม่สามารถใช้ได้ เพราะต้องรอผลตรวจคัดกรองจากสภากาชาดไทย ทางอีเมล์ แต่เมื่อระบบล่ม จึงไม่มีสัญญาณอินเตอร์เน็ตที่ใช้ในการ รับผลตรวจคัดกรองเลือดบริจาค
2. ผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้เต็มประสิทธิภาพ เช่น ไม่สามารถค้นประวัติเดิมของผู้ป่วย หรือผู้บริจาคเลือดได้ หรือการรับ-จ่ายโลหิตให้ผู้ป่วย
3. การบริการของหน่วยงานธนาคารเลือดเกิดความล่าช้า เช่น การลงรับสิ่งส่งตรวจจากทางหอผู้ป่วยจากระบบ HIS ไม่สามารถทำได้ จึงต้องลงเป็น manual ในโปรแกรมของ LIS เอง เสี่ยงทำให้เกิดความผิดพลาดของการลงเลข HN ผู้ป่วย อายุ เพศ หรือเลข AN เป็นต้น
4. การปฏิบัติงานของผู้ปฏิบัติงานมีความกดดันเพิ่มขึ้น เนื่องจากต้องแบกรับความเสี่ยงจากการลงระบบ LIS แบบ manual
5. ภาระงานของผู้ปฏิบัติงานเพิ่มขึ้น ในงานบริการการจ่ายเลือดผู้ป่วย ต้องใช้เจ้าหน้าที่ ทำการ double check 2 คน เพื่อป้องกันการจ่ายเลือดผิด

- **ผลกระทบต่อผู้ป่วย ญาติ และบุคลากร**

1. ผู้ป่วยได้รับเลือดล่าช้า เนื่องจากต้องใช้วิธีปฏิบัติงานแบบ manual
2. เนื่องจากทางโรงพยาบาลได้มีการกำหนดใช้เลขที่ HN ขึ้นมาใหม่ จึงทำให้การค้นประวัติเดิมข้อผู้ป่วยเป็นไปได้ยาก ถึงแม้จะมีฐานข้อมูลเดิมของคนไข้ แต่เลขที่ HN เปลี่ยนใหม่ จึงไม่สามารถค้นประวัติเดิมได้ เกิดความล่าช้าในการปฏิบัติงานขึ้น
3. ผู้บริจาคโลหิตในช่วงที่เกิดปัญหาระบบที่เกิดขึ้น จะไม่สามารถบันทึกครั้งที่บริจาคโลหิต และค้นประวัติในการบริจาคโลหิตที่ผ่านมาได้ จึงเสียสิทธิ์ในการนับจำนวนครั้งที่เข้าบริจาคเพื่อประกอบการเข้ารับเข็มบริจาคของสภากาชาดไทย
4. เนื่องจากมีการเพิ่มอัตรากำลังในการปฏิบัติงาน ทำให้บุคลากรเกิดความเหนื่อยล้าในการปฏิบัติงาน

2.2 กลยุทธ์

- **กลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack**

1. จัดให้มีการ back up ข้อมูล และมีการมอบหมายให้คณะกรรมการสารสนเทศทางการแพทย์ มีการตรวจสอบการ back up ข้อมูล ร่วมกับกลุ่มงานสารสนเทศทางการแพทย์ของโรงพยาบาล อย่างสม่ำเสมอ
2. ลักษณะแบ่งกลุ่มการใช้งานสารสนเทศตามนโยบายกลุ่มที่ 2 ที่จำเป็นต้องใช้ทั้ง LAN และ website ที่ได้รับอนุญาต ต้องมีการกำหนดสิทธิการเข้าใช้งานและเข้าถึงข้อมูล โดยควรมีจุดให้สามารถใช้งานได้เฉพาะเครื่องที่กำหนดไว้ให้เท่านั้น

3. มีการเชื่อมต่อข้อมูลเลขบัตรประชาชนของระบบ HIS และระบบ LIS และหากระบบสารสนเทศเกิดปัญหาซ้ำ กำหนดให้มีการใช้ข้อมูลเลขบัตรประชาชนของผู้ป่วยเพื่อยืนยันตัวตนของผู้ป่วย
4. ให้ความรู้กับผู้ปฏิบัติงานให้สามารถปฏิบัติงานได้เมื่อเกิดปัญหา และต้องปฏิบัติตาม Flow หรือตามแนวทางที่กำหนดร่วมกันอย่างเคร่งครัด
5. มีการกำหนด Flow การสื่อสาร /กำหนดช่องทางการสื่อสารเพื่อให้ผู้รับบริการรับทราบโดยทั่วถึงและเข้าใจสถานการณ์ที่กำลังเกิดปัญหา
6. ประสานงาน เจ้าหน้าที่ดูแลโปรแกรม LIS และเจ้าหน้าที่สารสนเทศของเครื่องตรวจวิเคราะห์อัตโนมัติ ให้นำข้อมูลที่ back up ไว้ สามารถส่งข้อมูลนำเข้า HIS เมื่อระบบเข้าสู่สภาวะปกติ
7. มีการ back up ข้อมูลค่าใช้จ่ายให้เป็นปัจจุบัน และจัดเก็บเป็นข้อมูลของแลบโดยเฉพาะ

- **วิธีการที่จะรักษางานบริการที่จำเป็น**

1. ผู้บริหารสนับสนุนงบประมาณในการจัดหาครุภัณฑ์คอมพิวเตอร์ให้กับหน่วยงาน
2. ควรจัดให้มีการแลกเปลี่ยนเรียนรู้งานด้านสารสนเทศและเทคโนโลยีของคณะกรรมการสารสนเทศของกลุ่มงานร่วมกับกลุ่มงานสารสนเทศทางการแพทย์ของโรงพยาบาลอุดรธานี
3. กลุ่มงานเทคนิคการแพทย์ฯควรจัดประชุมเชิงปฏิบัติการเพื่อให้ผู้ปฏิบัติงานมีความรู้และแนวทางปฏิบัติงานหากเกิดปัญหาขึ้น และตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานที่ผิด เพื่อให้ใช้เทคโนโลยีอย่างปลอดภัย
4. อัพเดตโปรแกรมต่างๆที่ใช้ในระบบของโรงพยาบาลให้ทันสมัย และปลอดภัยต่อการโดน ransomware รวมทั้งมีโปรแกรมสำรองเผื่อกรณีฉุกเฉินต่างๆ หากเกิดขึ้น

- **วิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร**

1. มีช่องทางสื่อสารที่มีประสิทธิภาพเพื่อให้ผู้ปฏิบัติงานทุกหน่วยงาน ทั้งแพทย์ พยาบาลหอผู้ป่วย ทราบถึงสถานการณ์ และปัญหาที่กำลังเกิดขึ้น ทำให้เข้าใจปัญหาร่วมกัน เพื่อลดแรงปะทะในการติดตามผล
2. สำหรับผู้ป่วยควรมีการแจ้งผลตรวจเคราะห์ใน application ได้ เช่น line official หรือ application อื่นที่เขียนโปรแกรมเพื่อให้ผู้ป่วยสามารถเรียกดูข้อมูลตนเองได้
3. ผู้ปฏิบัติทุกหน่วยงานควรอธิบายผู้ป่วย และญาติผู้ป่วยให้เข้าใจถึงสถานการณ์ ransomware attack ที่เกิดขึ้น

2.3 แผนปฏิบัติการ

- **ขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack**

1. มีการจัดทำแผนรองรับเมื่อเกิดปัญหาสารสนเทศซ้ำ โดยกำหนด Flow ในการปฏิบัติงานเมื่อระบบ IT ล่ม ใน 3 กรณี ดังนี้
   1.1 ระบบ HIS ล่ม
   1.2 ระบบ LIS ล่ม
   1.3 ระบบ HISและ LIS ล่ม
2. มีแผนการจัดสรรบุคลากรเสริม เมื่อเกิดปัญหาในการปฏิบัติงาน
3. งานตรวจวิเคราะห์มีแผนการปฏิบัติงาน เพื่อการปฏิบัติงาน แบบ manual และแจ้งให้ผู้ปฏิบัติงานปฏิบัติตาม Flow เมื่อเกิดเหตุอันไม่พึงประสงค์เกิดขึ้น
4. จัดทำแผนการ Back up ข้อมูลในระบบ LIS และการจัดเก็บข้อมูลในช่วงที่ระบบล่ม

- **ผู้รับผิดชอบสำหรับแต่ละขั้นตอน**

ลำดับ ผู้เกี่ยวข้อง	หน้าที่
ผู้ที่ได้รับผลกระทบจากเหตุการณ์ - ผู้ปฏิบัติงาน ณ ขณะนั้น	1. แจ้งเหตุ หรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบ หรือสงสัยว่ามีภัยคุกคามเกิดขึ้น
หัวหน้ากลุ่มงาน, หัวหน้างาน	1. รับแจ้งเหตุ หรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
ผู้รับแจ้งเหตุ	1. รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

- หัวหน้ากลุ่มงาน - หัวหน้างาน - คณะกรรมการสารสนเทศ	2. ให้คำแนะนำปรึกษาบุคลากรเกี่ยวกับการป้องกัน จุดอ่อน ข้อควรระมัดระวัง และเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน3. 3. มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
คณะกรรมการสารสนเทศ - หน่วยงาน IT ของโรงพยาบาล - หน่วยงานภายนอกที่เกี่ยวข้องกับระบบ LIS	1. เฝ้าระวัง และวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ 2. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน 3. มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
ผู้บริหารของโรงพยาบาล	1. รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยไซเบอร์

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

- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน

1. ขั้นตอนที่ 1,2,3 ใช้เวลา 1-2 วัน
2. ขั้นตอนที่ 4 ดำเนินการทุกเดือน ใช้เวลา 1-2 วัน/เดือน

2.4 ทรัพยากร

- **ทรัพยากรที่จำเป็นในการดำเนินการแผน BCP**

1. จัดเตรียมสถานที่จัดเก็บ ที่มีความมั่นคงปลอดภัย เพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูล และพยานวัตถุอื่นๆที่สำคัญ
2. จัดหาอุปกรณ์และซอฟแวร์ สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์
3. จัดหาอุปกรณ์สำรองเพิ่มเติม เช่น เครื่อง printer ใช้ในกรณีออกผลแบบ manual
4. จัดหาระบบตรวจจับ และป้องกันภัยคุกคามไซเบอร์ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Endpoint Detection & Response)
5. จัดตั้งทีมรับมือภัยคุกคามทางไซเบอร์ ส่งบุคลการเข้ารับการฝึกอบรมด้าน Cyber Security
6. จัดอัตรากำลังคน เสริมการปฏิบัติงานเมื่อเกิดเหตุการณ์

- **แหล่งที่มาของทรัพยากร**

1. งบประมาณจาก โรงพยาบาลอุดรธานี จัดหาสนับสนุนอุปกรณ์การทำงาน

2.5 การทดสอบและฝึกอบรม

- **วิธีการทดสอบแผน BCP**

1. กำหนดแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือการให้หัวหน้าหน่วยงานเป็นผู้ประเมินผู้ปฏิบัติงานในแต่ละหน่วยต่อสถานการณ์ ransomware ที่เกิดขึ้น เมื่อประเมินความรับรู้เสร็จแล้ว จัดทำรายการสรุปผลการประเมิน จากนั้นให้คิดเป็นร้อยละการรับรู้ และจัดทำเสนอแนะแนวทางแก้ไข ซึ่งแบบประเมินตนเอง ให้ผู้ปฏิบัติงานใช้ระบบตอบคำถามว่า ระเบียบข้อใดบ้างที่ปฏิบัติตาม ระเบียบข้อใดที่ไม่ปฏิบัติ สาเหตุที่ทำให้ไม่ปฏิบัติตามระเบียบคืออะไร
2. การจำลองสถานการณ์ ransomware เพื่อทดสอบว่า ผู้ปฏิบัติงานสามารถปฏิบัติตามระเบียบที่ปฏิบัติตรงตามที่กำหนดไว้

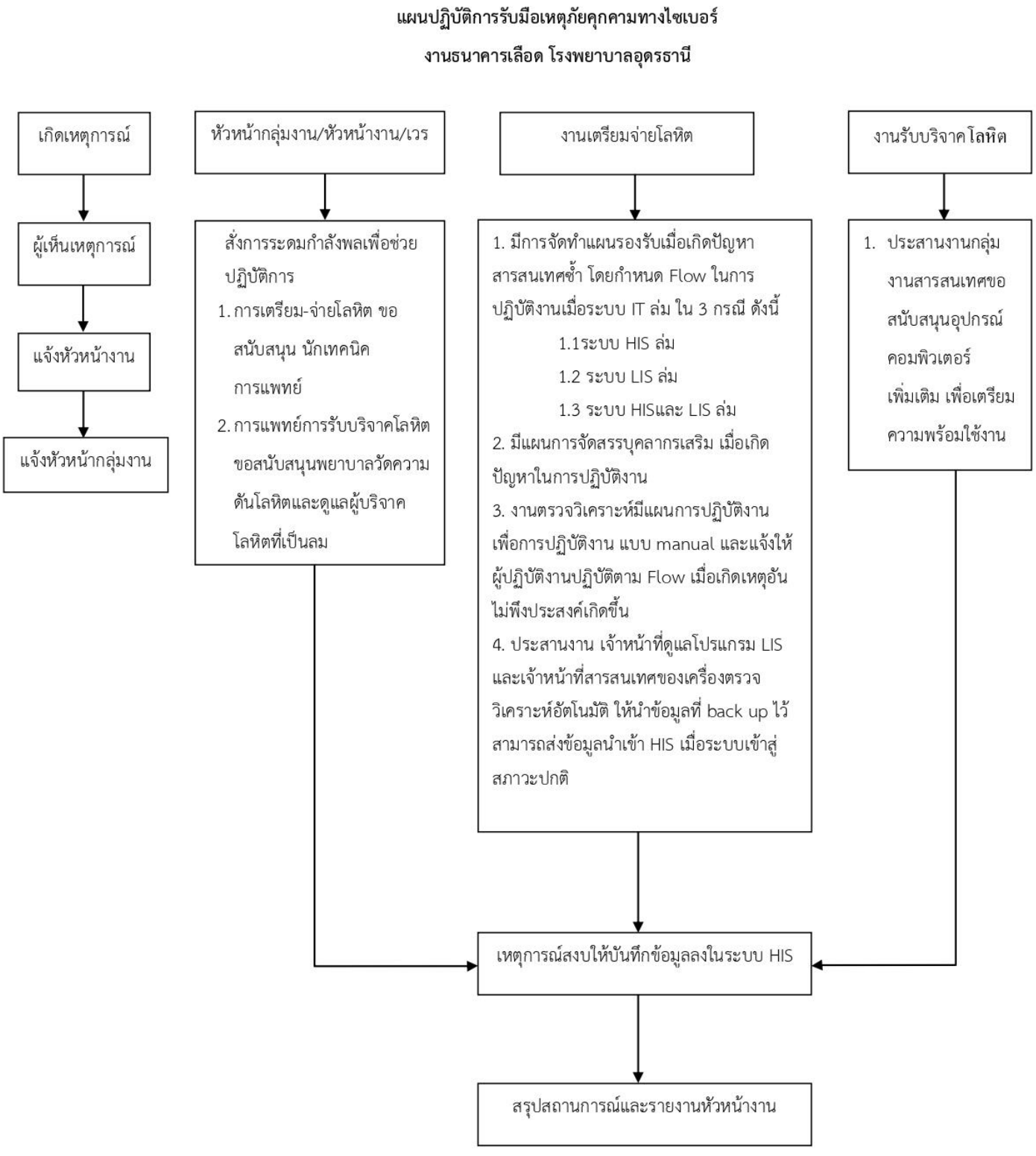
- **วิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้**

1. การให้ความรู้ซ้ำหลายๆครั้ง เปลี่ยนช่องทางการให้ข้อมูล หรือเพิ่มช่องทางการให้ข้อมูล กำหนดมาตรการให้รางวัลแก่ผู้ที่สนใจและรับรู้ระเบียบได้อย่างดี
2. จัดทำการจำลองสถานการณ์ ransomware อยู่สม่ำเสมอเพื่อให้ผู้ปฏิบัติงานได้ทบทวนแนวทางปฏิบัติอยู่ตลอดเวลา
3. รวบรวมข้อเสนอแนะและข้อคิดเห็นจากผู้ปฏิบัติงานที่เข้าร่วมการให้ความรู้ หรือจากการผ่านจำลองสถานการณ์ เพื่อใช้ในการปรับปรุงแก้ไขแผน ให้สามารถใช้งานได้จริง

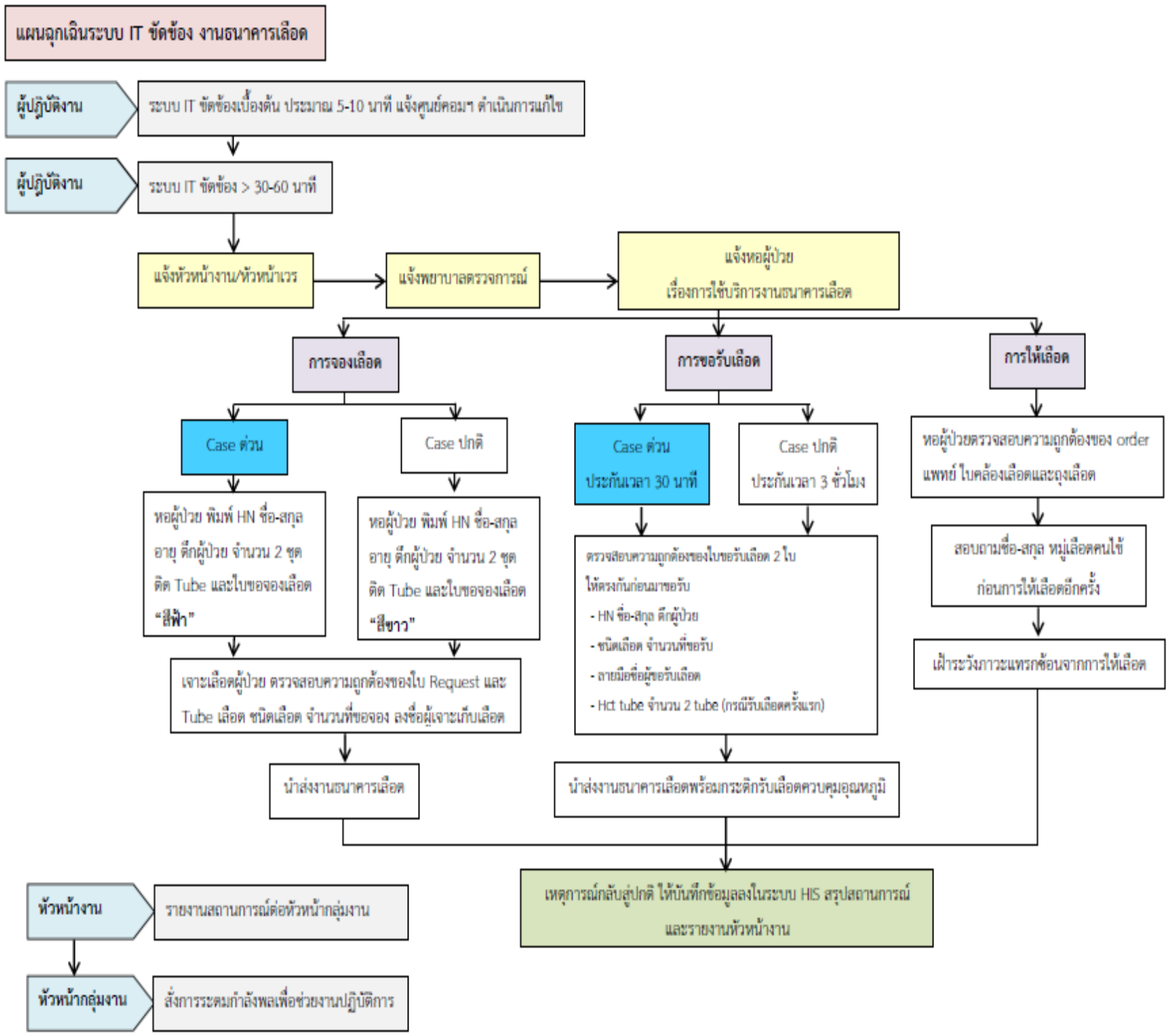
3. เอกสารแนบ

- **แผนงาน**

1.Flow แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์ งานธนาคารเลือด โรงพยาบาลอุดรธานี



2. Flow แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์ การให้บริการงานธนาคารเลือด



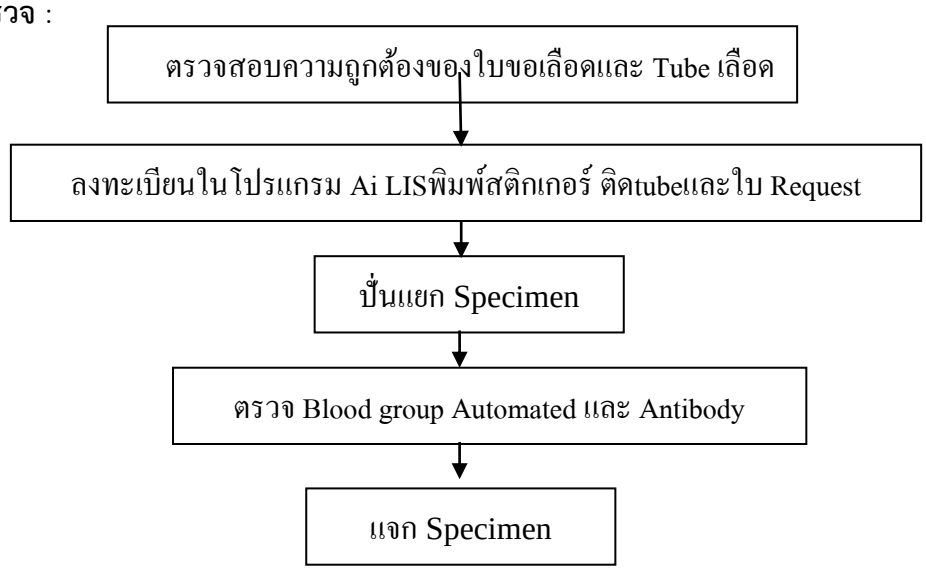
3. Flow แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์ การเตรียม – จ่ายโลหิต งานธนาคารเลือด

3.1 กรณี ระบบ HIS ล่ม

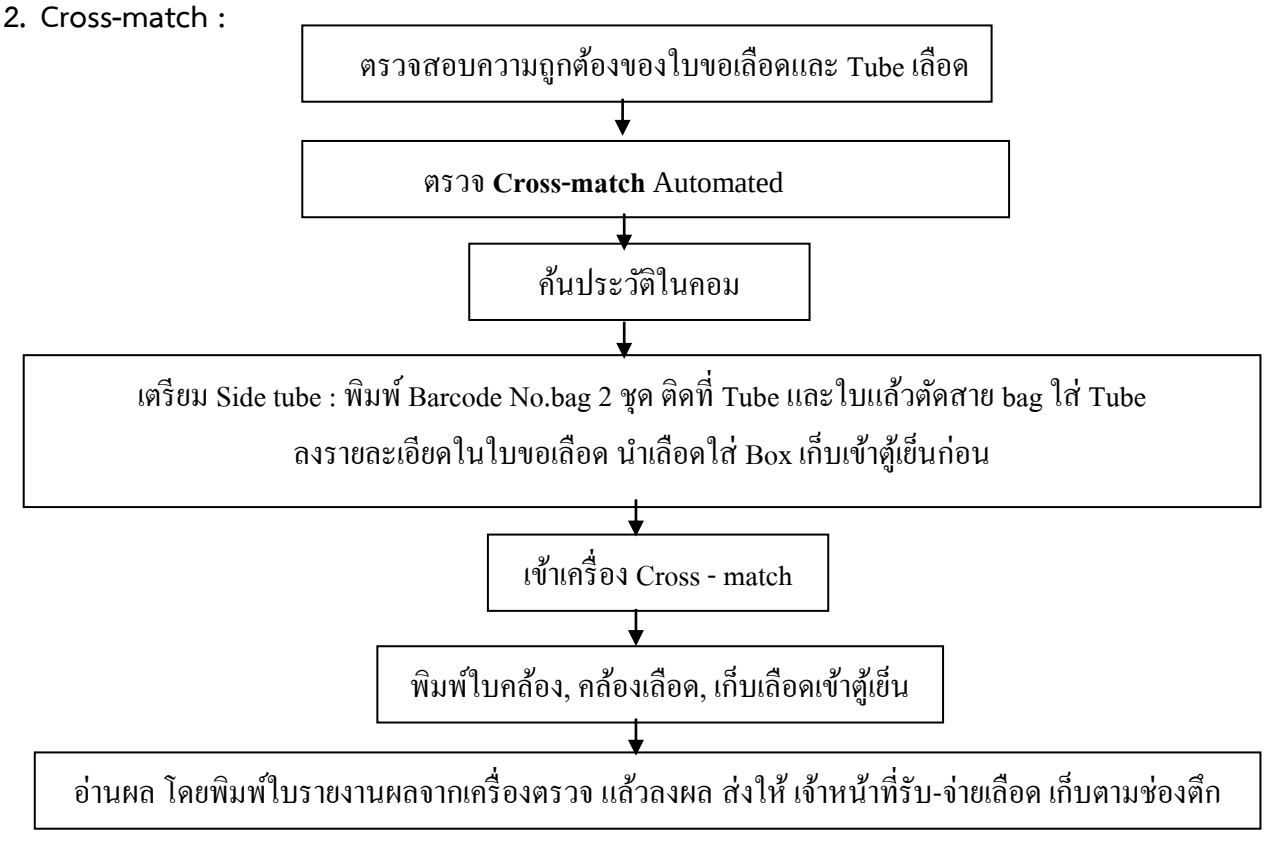
Flow งาน ห้อง Cross – matching กรณีระบบ IT ล่ม

กรณี ระบบ HIS ล่ม

1. รับสิ่งส่งตรวจ :



2. Cross-match :



(*คนไข้รายใหม่ต้องตรวจ Blood Group ซ้ำก่อนด้วยวิธี Cell grouping)

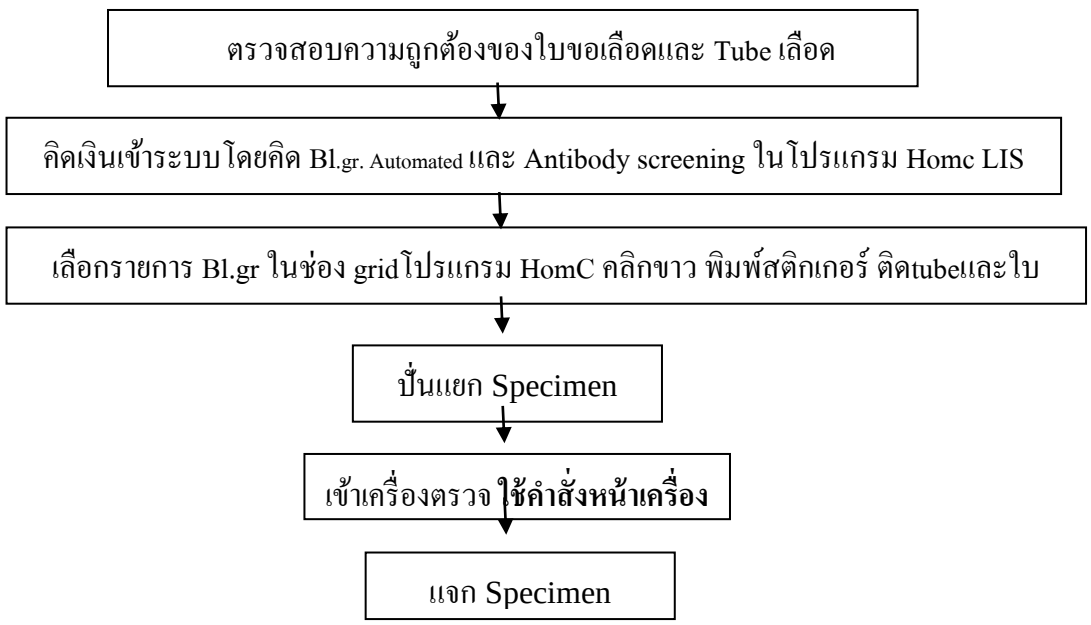
หมายเหตุ: เก็บใบขอเลือดไว้รอบันทึกข้อมูลย้อนหลังเมื่อระบบ HIS กลับสู่ภาวะปกติ

3.2 **กรณี ระบบ LIS ล่ม**

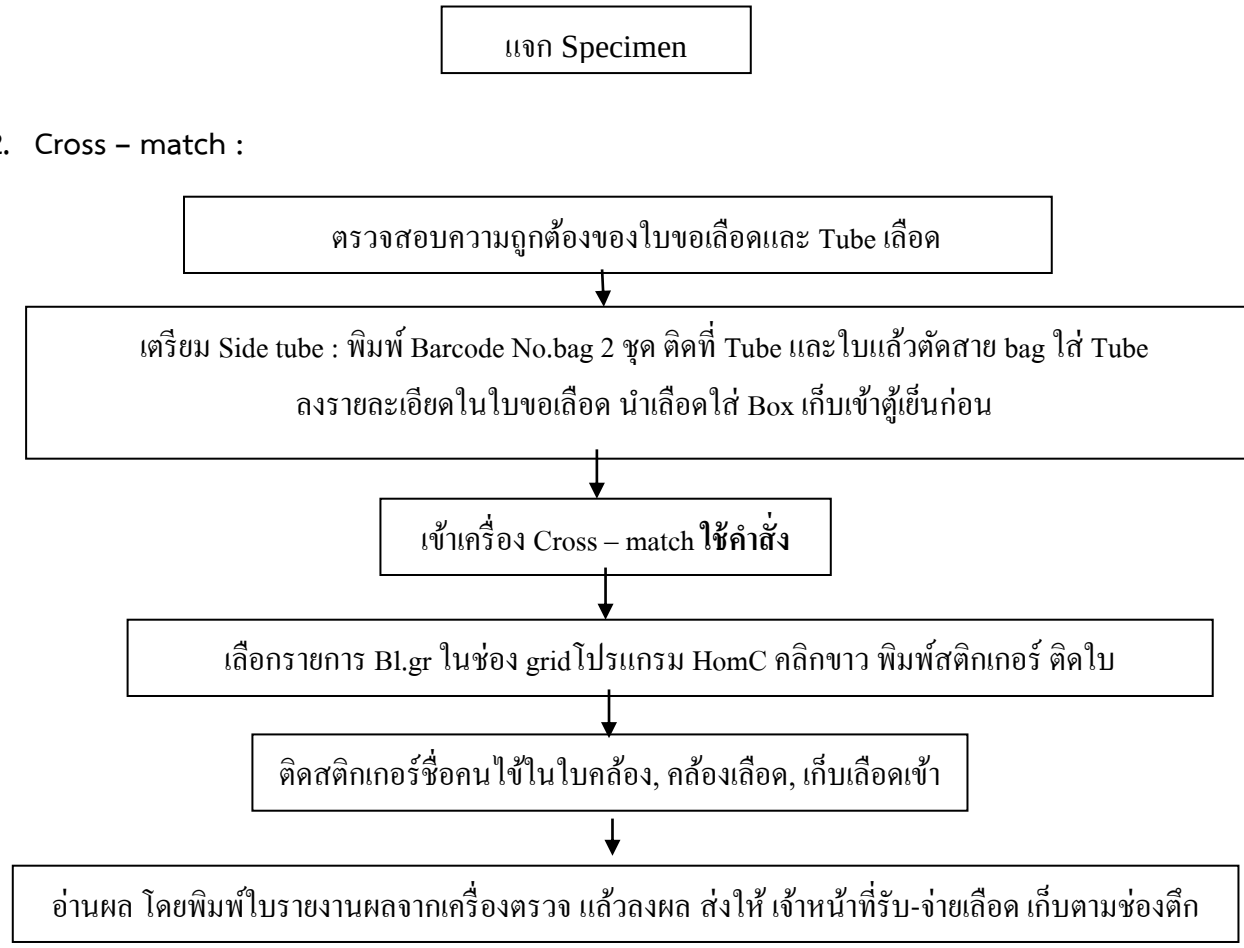
Flow งาน ห้อง Cross – matching กรณีระบบ IT ล่ม

กรณี ระบบ LIS ล่ม

1. รับสิ่งส่งตรวจ



2. Cross – match :



(*คนไข้รายใหม่ต้องตรวจ Blood Group ซ้ำก่อนด้วยวิธี Cell grouping)

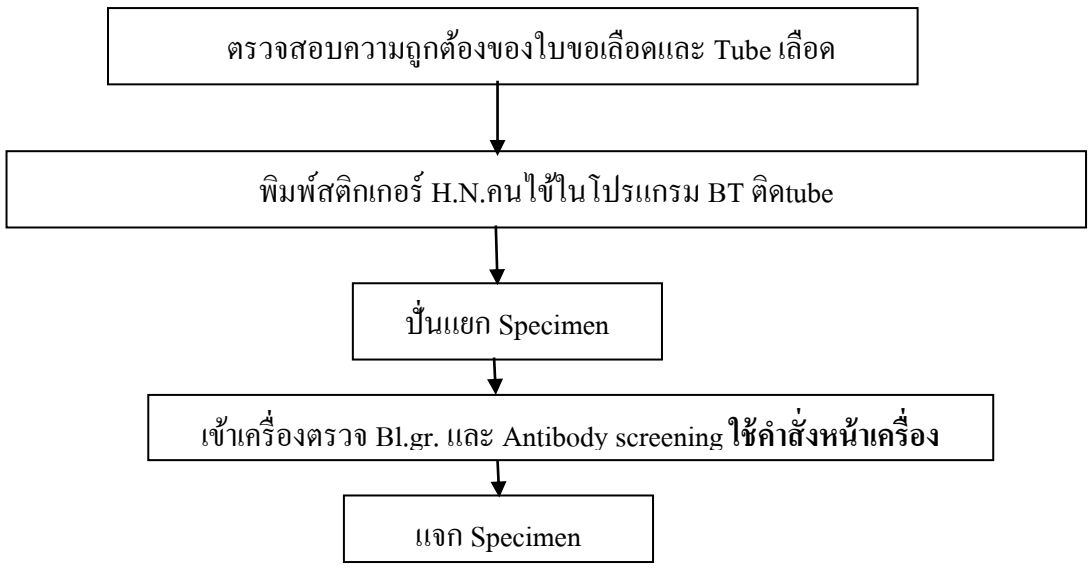
หมายเหตุ: เก็บใบขอเลือดไว้รอบันทึกข้อมูลย้อนหลังเมื่อระบบ LIS กลับสู่ภาวะปกติ

3.3 กรณี HIS และ LIS ล่ม

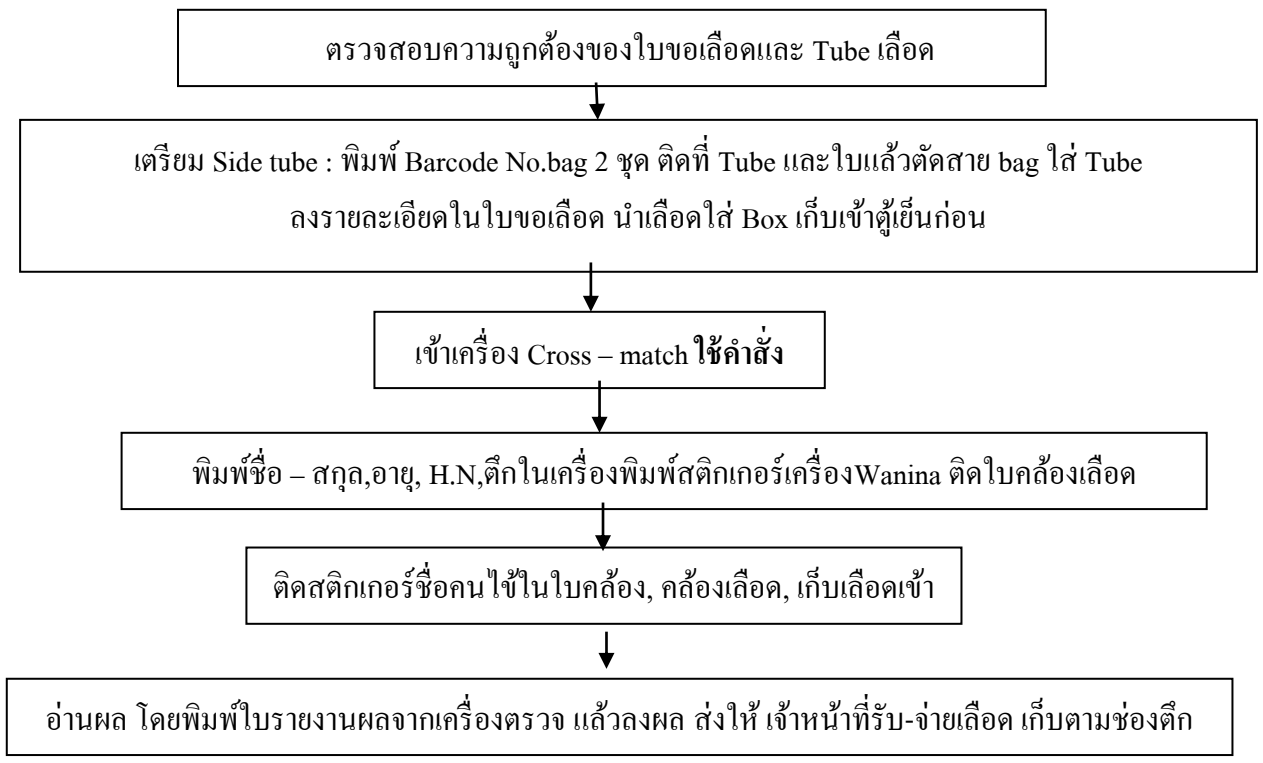
<u>Flow งาน ห้อง Cross – matching กรณีระบบ IT ล่ม</u>

<u>กรณี ระบบ HISและ LIS ล่ม</u>

1. รับสิ่งส่งตรวจ



2. Cross – match :



(*คนไข้รายใหม่ต้องตรวจ Blood Group ซ้ำก่อนด้วยวิธี Cell grouping)

<u>หมายเหตุ: เก็บใบขอเลือดไว้รอบันทึกข้อมูลย้อนหลังเมื่อระบบ LIS กลับสู่ภาวะปกติ</u>

4. วิธีปฏิบัติการจ่ายเลือด กรณีระบบ IT ล่ม

1. **เจ้าหน้าที่หอผู้ป่วยขอรับเลือด** โดยมีใบขอรับเลือด 2 ชุด ลงรายละเอียดถูกต้องชัดเจนพร้อมกับกระติกน้ำแข็ง โดยหอผู้ป่วยลงประวัติหมู่เลือดจากการเช็คประวัติในการจ่ายเลือดครั้งที่แล้วในใบขอรับเลือดหรือใบคล้องเลือด*หากเป็นผู้ป่วยรับเลือดครั้งแรกต้องมี Hct tube มาด้วยทุกครั้ง
2. **เจ้าหน้าที่จ่ายเลือด คนที่ 1**
   - ตรวจสอบใบขอรับเลือด
   - ค้นหาใบขอเลือดตามช่องตึกผู้ป่วย แล้วนำใบขอรับเลือดและใบขอเลือดใส่ลงใน Box หรือตะกร้า
   - หาเลือดในตู้เย็น
   - ตรวจสอบความถูกต้อง ตรงกัน ในใบขอเลือด, ใบขอรับเลือด, ใบคล้อง และถุงเลือด
   - ลงชื่อผู้จ่ายเลือดในใบขอเลือดและใบขอรับเลือด แล้วแจ้งให้เจ้าหน้าที่จ่ายเลือดคนที่ 2 Double check
3. **เจ้าหน้าที่จ่ายเลือด คนที่ 2**
   - ตรวจสอบความถูกต้อง ตรงกัน ในใบขอเลือด, ใบขอรับเลือด, ใบคล้อง และถุงเลือด
   - ลงชื่อผู้จ่ายเลือดในใบขอเลือดและใบขอรับเลือด
   - เรียกชื่อหอผู้ป่วยที่มารับเลือดและทวนชื่อผู้ป่วยที่มาขอรับเลือดซ้ำอีกครั้ง ก่อนจ่ายเลือดออกไป

หมายเหตุ: กรณี HIS ใช้งานได้ตามปกติ ให้คิดค่าบริการใน HomC แล้วเก็บใบเข้าช่องward

รายชื่อผู้ติดต่อ

1. นายแพทย์ สุรพงศ์ แสนโภชน์ รองผู้อำนวยการด้านเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลอุดรธานี
2. นายธนพล ธนอำพนสกุล หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์ โรงพยาบาลอุดรธานี
3. นางสาวศุภวัลย์ คำชาย นักวิทยาศาสตร์การแพทย์ชำนาญการ กลุ่มงานเทคนิคการแพทย์และพยาธิวิทยาคลินิก โรงพยาบาลอุดรธานี
4. นายอดิศักดิ์ วงค์เวียน นักเทคนิคการแพทย์ชำนาญการ กลุ่มงานเทคนิคการแพทย์และพยาธิวิทยาคลินิก โรงพยาบาลอุดรธานี
5. นางจุฑารัตน์ ช่วยจันทร์ดี ตำแหน่ง Business Development Manager บริษัท เอ.ไอ.คอนเวอร์เจนส์ (ประเทศไทย) จำกัด

- **แบบฟอร์มที่จำเป็น**

  ไม่มี

4. การอนุมัติ

หัวหน้างานธนาคารเลือด **นางสาวศุภวัลย์ คำชาย นักวิทยาศาสตร์การแพทย์ชำนาญการ**

วันที่ 6 มีนาคม 2567

5. บทสรุป

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1. มอบหมายให้คณะกรรมการสารสนเทศ ตรวจสอบการ Back up ข้อมูลของโรงพยาบาลอย่างสม่ำเสมอ		/	/
2. การใช้งานสารสนเทศที่จำเป็นต้องใช้ LANและเว็บไซต์ต้องกำหนดหรือจำกัดสิทธิการเข้าใช้งานและเข้าถึงข้อมูล		/	/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1. เชื่อมต่อข้อมูลเลขบัตรประชาชนของระบบ HIS และ LIS เพื่อใช้ยืนยันตัวตนผู้ป่วยหากเกิดกรณีดังกล่าวซ้ำ			/
2. ให้ความรู้กับผู้ปฏิบัติงานได้เมื่อเกิดปัญหา สามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างเคร่งครัด	/	/	/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1. กำหนดช่องทางการสื่อสารเพื่อให้ผู้รับบริการรับทราบโดยทั่วกัน และเข้าใจถึงสถานการณ์	/	/	/
การปฏิบัติหลังระบบกลับสู่ปรกติ			
1. ประสานงานเจ้าหน้าที่ที่ดูแลระบบ LIS ต่างๆ ให้นำข้อมูลที่ Back up ไว้ส่งข้อมูลกลับระบบ HIS		/	/
2. มีการ Back up ข้อมูลค่าใช้จ่ายให้เป็นปัจจุบัน และจัดเก็บเป็นข้อมูลของแลบโดยเฉพาะ		/	/

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT