

แผนการประเมินความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ

โดยการมีส่วนร่วมของทุกฝ่าย

การประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศในโรงพยาบาลสันกำแพงเป็นกระบวนการที่สำคัญในการรักษาความมั่นคงและความปลอดภัยของข้อมูลทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย การประเมินความเสี่ยงช่วยให้เราสามารถระบุและจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ การดำเนินการนี้ต้องการความร่วมมือและการมีส่วนร่วมจากทุกฝ่ายที่เกี่ยวข้องเพื่อให้กระบวนการประเมินความเสี่ยงมีความครบถ้วนและเป็นระบบ

กลยุทธ์การดำเนินงานประเมินความเสี่ยง

1. การกำหนดเป้าหมายและขอบเขตการประเมินความเสี่ยง

- กำหนดเป้าหมาย:** ระบุวัตถุประสงค์ของการประเมินความเสี่ยง เช่น การป้องกันข้อมูลส่วนบุคคลของผู้ป่วย, การรักษาความมั่นคงของระบบสารสนเทศ, การปฏิบัติตามมาตรฐานและข้อกำหนดทางกฎหมาย
- ขอบเขตการประเมิน:** ระบุขอบเขตของการประเมินความเสี่ยง เช่น ระบบสารสนเทศที่ต้องการประเมิน, ทรัพยากรที่ต้องการประเมิน (ฮาร์ดแวร์, ซอฟต์แวร์, เครือข่าย, บุคลากร)

2. การระบุความเสี่ยง (Risk Identification)

- รวบรวมข้อมูล:** รวบรวมข้อมูลเกี่ยวกับระบบสารสนเทศและทรัพยากรที่เกี่ยวข้อง เช่น โครงสร้างเครือข่าย, รายละเอียดอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์, ข้อมูลการใช้งานของผู้ใช้
- ระบุภัยคุกคาม:** ระบุภัยคุกคามที่อาจเกิดขึ้น เช่น การโจมตีทางไซเบอร์, การสูญหายของข้อมูล, การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ระบุช่องโหว่:** ระบุช่องโหว่ที่อาจเกิดขึ้นในระบบ เช่น ช่องโหว่ของซอฟต์แวร์, การตั้งค่าระบบที่ไม่ปลอดภัย

3. การประเมินความเสี่ยง (Risk Assessment)

- การวิเคราะห์ความเสี่ยง:** ประเมินความเสี่ยงโดยใช้เครื่องมือและเทคนิคต่างๆ เช่น การวิเคราะห์เชิงคุณภาพ (Qualitative Analysis) และการวิเคราะห์เชิงปริมาณ (Quantitative Analysis)
- การให้คะแนนความเสี่ยง:** ให้คะแนนความเสี่ยงตามปัจจัยต่างๆ เช่น ความเป็นไปได้ของการเกิดภัยคุกคาม, ความรุนแรงของผลกระทบ, ความสามารถในการตรวจจับและป้องกัน

4. การจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization)

- การจัดลำดับความสำคัญ:** จัดลำดับความสำคัญของความเสี่ยงตามคะแนนที่ได้รับและผลกระทบที่อาจเกิดขึ้น

- การระบุความเสี่ยงที่ต้องการการจัดการ: ระบุความเสี่ยงที่มีความสำคัญสูงและต้องการการจัดการทันที

5. การจัดทำแผนการจัดการความเสี่ยง (Risk Management Plan)

- การกำหนดมาตรการป้องกัน: กำหนดมาตรการป้องกันความเสี่ยง เช่น การอัปเดตซอฟต์แวร์, การฝึกอบรม บุคลากร, การปรับปรุงการตั้งค่าระบบ
- การจัดทำแผนปฏิบัติการ: จัดทำแผนปฏิบัติการเพื่อดำเนินการตามมาตรการป้องกันที่กำหนด
- การกำหนดผู้รับผิดชอบ: กำหนดผู้รับผิดชอบในแต่ละมาตรการและกำหนดเวลาในการดำเนินการ

6. การติดตามและประเมินผล (Monitoring and Review)

- การติดตามผลการดำเนินการ: ติดตามผลการดำเนินการตามแผนการจัดการความเสี่ยง
- การประเมินผล: ประเมินผลของการดำเนินการและปรับปรุงกระบวนการตามความจำเป็น
- การรายงานผล: รายงานผลการประเมินความเสี่ยงและการจัดการความเสี่ยงต่อผู้บริหารและผู้เกี่ยวข้อง การมีส่วนร่วมของทุกฝ่าย

7. การประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศต้องการความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง เช่น

- ผู้บริหาร: ให้การสนับสนุนและกำหนดแนวทางในการประเมินความเสี่ยง
- ฝ่าย IT: จัดเตรียมข้อมูลเกี่ยวกับระบบสารสนเทศและดำเนินการตามมาตรการป้องกันความเสี่ยง
- ฝ่ายการแพทย์: ให้ข้อมูลเกี่ยวกับการใช้งานระบบสารสนเทศและความต้องการด้านความปลอดภัย
- ฝ่ายความปลอดภัย: ให้คำแนะนำเกี่ยวกับการป้องกันความเสี่ยงและการจัดการความปลอดภัย
- บุคลากรทั้งหมด: มีส่วนร่วมในการให้ข้อมูลและการปฏิบัติตามมาตรการความปลอดภัย

การประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบโดยการมีส่วนร่วมของทุกฝ่าย จะช่วยให้ โรงพยาบาลสันกำแพงสามารถระบุและจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ ป้องกันการสูญเสียข้อมูลและเพิ่มความมั่นคงปลอดภัยให้กับระบบสารสนเทศของโรงพยาบาล

ระยะเวลาดำเนินการ

แผนภูมิแสดงจำนวนรายงานอุบัติการณ์ความเสี่ยง แยกรายเดือน ปีงบประมาณ 2568

