PDPA and CYber Security

VACHIRA PHUKET HOSPITAL

SUMMARY REPORT FOR PDPA PREPAREDNESS

VACHIRA PHUKET HOSPITAL

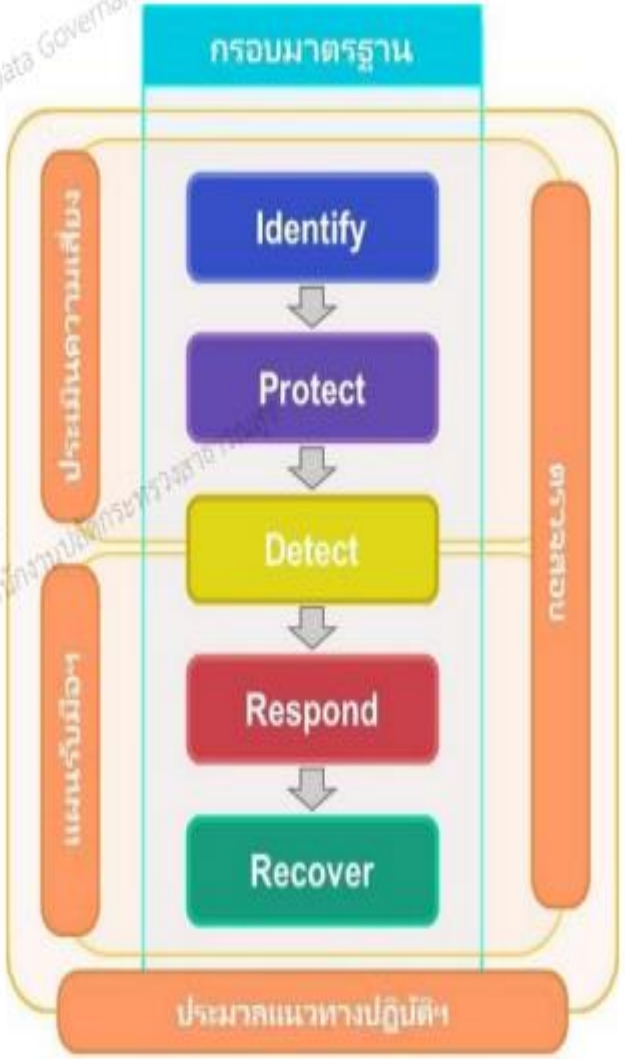
PDPA Prepareness	มาตรา	การปฏิบัติ
- จัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	41	ดำเนินการแล้ว
- จัดการ Cyber security	37	อยู่ระหว่างดำเนินการโดยงาน IT
- จัดทำ privacy notice & privacy policy	23 (3)	ดำเนินการแล้ว
- ทำสัญญา Data processing agreement	40	อยู่ระหว่างสำรวจบริษัทที่ต้องทำสัญญา
- จัดทำ ROPA (Record of Processing Activities)	39	ประชุมตัวแทนแต่ละหน่วยงาน 23/8/65
- จัดทำระเบียบการทำลายข้อมูล	33	รอ ROPA เสร็จ
- จัดให้มีระบบแจ้งเหตุละเมิดภายใน 72 ชม.	37(4)	รอ ROPA เสร็จ
- ทำระบบรองรับการใช้สิทธิ์ของ Data Subject	19,30,31, 32,36	รอ ROPA เสร็จ
- จัดอบรมเจ้าหน้าที่รพ.ทั้งหมดให้รู้จัก PDPA	42	อยู่ระหว่างวางแผนดำเนินการ

Updated 9/8/65

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๖ การจัดทำประมวลแนวทางปฏิบัติมีองค์ประกอบดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



CYBER SECURITY

VACHIRA PHUKET HOSPITAL

- จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัย สารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง)

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของ และใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆที่เกี่ยวข้องกับ ประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

CYBER SECURITY

VACHIRA PHUKET HOSPITAL

- ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

  1) การประเมินความเสี่ยง (Risk Assessment)

  (ก) การระบุความเสี่ยง (Risk Identification)

  (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)

  (ค) การประเมินค่าความเสี่ยง (Risk Evaluation)

  2) การจัดการความเสี่ยง (Risk Treatment)

  3) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

  4) การรายงานความเสี่ยง (Risk Reporting)

CYBER SECURITY

VACHIRA PHUKET HOSPITAL

- <u>การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ</u>

ข้อ 1. ระบบป้องกันผู้บุกรุก

(1) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด - ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

- ระดับความรุนแรงมากน้อยเพียงใด - หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ 2. ระบบไฟร์วอลล์

(1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(2) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์

(3) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ แจ้งหัวหน้าหน่วยงาน ดำเนินการแก้ไขปัญหา

ข้อ 3. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต (Malware) : ไวรัส หนอนอินเทอร์เน็ต รวมถึงสปายแวร์

(1) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกัน ภัยคุกคามทางอินเทอร์เน็ต

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก, มัลแวร์มาจากเครือข่ายใด และถูกส่งไปยังที่ใด

- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลวชิระภูเก็ตไปยังภายนอกหรือไม่

(2) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของโรงพยาบาลวชิระภูเก็ต

(3) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

THANK YOU

Cyber security Management

Risk Management
มาตราการป้องกัน

1. **Hardening Infrastructure** (สร้างความเข้มแข็งของ Hardware , Software , Network)
   - Vulnerability Assessment (VA)
   - Firewall , License , Patch , Anti Virus
   - Fire Protection , Access
2. **Data Integrity** (การรักษาความมั่นคง ปลอดภัยของข้อมูล)
   - Backup 3 copy ด้วยความถี่ที่เหมาะสม , DR site
3. **User Awareness** (สร้างความตระหนักของผู้ใช้งาน)
   - e-Mail , Thumb Drive , Share file
4. **System Redundant**
   - Active-Active , Active-Passive , Offline Backup
5. **จัดทำ BCP** (แผนรับเหตุฉุกเฉิน/แผนความต่อเนื่อง)
   - Business Contingency Plan
   - Business Continuity Plan

ISO 27799

ISO 27001

Recovery Response
มาตรการเผชิญเหตุ

1. **Investigation**
   - หาสาเหตุ
2. **System Recovery**
   - Cleansing OS , HIS , Network , Client
3. **Data Recovery**
   - Backup Restore
4. **Business Recovery**
   - Maunual

bsi. ISO/IEC 27001 Information Security Management

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
- หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล
- หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
- หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม
- หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ
- หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- หมวดที่ ๗ หน้าที่และความรับผิดชอบ

PDPA and Cyber Security

- จัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามมาตรา 41
- จัดการ Cyber Security ให้อยู่ในระดับดีที่สุด ตามาตรา 37 (1)
- ทำสัญญา Data Processing Agreement เป็นสัญญาแนบกับ Data Processer
- เก็บบันทึกรายละเอียดว่ารพ. มีข้อมูลส่วนบุคคล และกิจกรรมใช้งานข้อมูลส่วนบุคคลใดบ้าง เพื่อบันทึกกิจกรรมการประมวลผลข้อมูล (Record of Processing Activities หรือ ROPA) ตามมาตรา 39

Record of Processing Activities หรือ RoPA

1.ข้อมูลส่วนบุคคลที่เก็บ

2. วัตถุประสงค์ของการเก็บ ข้อมูลแต่ละประเภท

3. ข้อมูลเกี่ยวกับ Data Controller

4. ระยะเวลาการเก็บ ข้อมูลแต่ละประเภท

5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล/ เงื่อนไขบุคคลที่มีสิทธิ เข้าถึง/ เงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

6. ฐานทางกฎหมายที่ใช้ประมวล

7. การปฏิเสธ สิทธิการเข้าถึง (ม30)/ สิทธิโอนย้ายข้อมูล (ม31)/ สิทธิคัดค้าน (ม32)/ สิทธิแก้ไขให้ถูกต้อง (ม36)

8. คำอธิบายเกี่ยวมาตรการรักษาความปลอดภัย มาตรา 37 (1)

Executive Summary Report for PDPA Preparedness

- นำบันทึกกิจกรรมการประมวลผลข้อมูล (RoPA) มาวิเคราะห์เพื่อ
  - เก็บข้อมูล/ข้อมูลอ่อนไหว เท่าที่จำเป็น ตามมาตรา 26
  - การใช้ เก็บ การเปิดเผย ส่งต่อ
    พยายามหาฐาน LAWFUL BASIS เพื่อประมวลผลข้อมูล
  - จัดทำระเบียบการทำลายข้อมูล ตามมาตรา 40
  - ทำระบบชี้แจง privacy notice & privacy policy
    ตามมาตรา 23(3)

Executive Summary Report for PDPA Preparedness

- นำบันทึกกิจกรรมการประมวลผลข้อมูล (RoPA) มาวิเคราะห์เพื่อ

  - ข้อมูลฐานยินยอม ต้องจัดทำ consent
  - ทำระบบรองรับการใช้สิทธิ์ของ Data Subject ตามมาตรา 19 ถอนความยินยอม, 30 เข้าถึงข้อมูล , 31 โอนย้ายข้อมูล , 32 คัดค้านข้อมูล, 36 ลบข้อมูล
  - ระบบแจ้งเหตุละเมิดภายใน 72 ชม. ตามมาตรา 37(4)
  - พัฒนาระบบรักษาความปลอดภัย ตามมาตรา 37(1),(2)