

# PDPA & Cyber security in office

โรงพยาบาลนางัวเฉลิมพระเกียรติ ๘๐ พรรษา

นายธวัชชัย ราชเจริญ



# แนวทางการดำเนินงาน PDPA ในโรงพยาบาล

01

แต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

02

จัดทำประกาศนโยบายความเป็นส่วนตัว หรือ Privacy Notice

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562

03

ประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือ Privacy Policy

04

จัดทำ Consent Management

03

เช่น นอนโรงพยาบาล หัตถการที่มีความเสี่ยง ตรวจ HIV



## แนวทางการดำเนินงาน PDPA ในโรงพยาบาล (ต่อ)

05

กำหนดการเข้าถึงข้อมูล HIS ของโรงพยาบาล

06

กำหนดระบบและบุคคลเข้าออกคลังเวชระเบียน

07

ถอดระบบ HIS ของโรงพยาบาลห้ามแก้ไข เปลี่ยนแปลงข้อมูล

08

กำหนดสิทธิในการป้อนเวชระเบียนออกจาก HIS ของโรงพยาบาล



# แนวทางการดำเนินงาน PDPA ในโรงพยาบาล (ต่อ)

09

แยกแยะระเบียบผู้รับบริการที่มีความที่เป็นความลับออกจาก HIS และคลัง  
เวชระเบียนของโรงพยาบาล

เช่น OSCC, HIV

10

จัดทำข้อตกลงการประมวลผล

กรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล, ส่งต่อข้อมูลส่วนบุคคลให้กับหน่วยงานอื่น

11

จัดทำ RoPA (Record of Processing Activities)

04

12

จัดทำความเสี่ยง ทบทวนความเสี่ยง รายงานผู้บริหาร



# แนวทางการป้องกันการโจมตี

## ภัยที่เกิดจาก Software

ติดตั้ง Firewall  
ติดตั้งซอฟต์แวร์ Anti-virus

## ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากร

ให้มีความรู้ Hardware และ Software  
เบื้องต้น  
มีกุญแจล็อคประตูห้องควบคุมระบบ  
เครือข่าย  
ติดตั้งกล้องวงจรปิด

## ภัยจากไฟไหม้ / ระบบไฟฟ้า

ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS)  
ติดตั้งอุปกรณ์ตรวจจับควัน  
ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ  
สำรองข้อมูลเก็บไว้ที่เครื่องสำรองคนละอาคาร  
เครื่อง Slave  
ติดตั้งเครื่องปรับอากาศ

## ซ่อมแผนฉุกเฉิน

ถูกโจมตี  
HIS ล่ม

**THANK  
YOU**

