# PDPA and Cyber Security

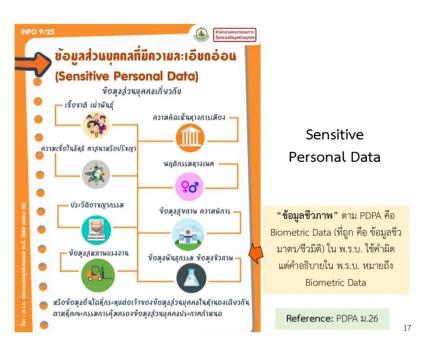
นพโจารุพล ตวงศิริทรัพย์

# หน่วยงาน : โรงพยาบาลกาฬสินธุ์ โรงพยาบาลทั่วไปขนาด 540 เตียง ระดับ S การดำเนินงานด้านฐานข้อมูลผู้ป่วย

## วิเคราะห์ระบบภาพรวม

System	Struckture	Staff
• ระบบศูนย์ประกัน	Server HosXP	<ul><li>บุคลากรให้บริการทางการ</li><li>แพทย์</li></ul>
• ระบบHIS (HosXP ver3)	• Computer ใช้หน้างาน	● เจ้าหน้าที่IT
● ระบบ Refer	● โครงสร้าง Intranet	<ul> <li>เจ้าหน้าที่เกี่ยวข้องกับการ</li> <li>บริการอื่นๆ (back office)</li> </ul>
<ul> <li>ระบบควบคุมการใช้งาน</li> <li>ข้อมูล Digital ในรพ.</li> </ul>	<ul> <li>โครงสร้าง Internet และ</li> <li>Firewall</li> </ul>	
<ul><li>ระบบฐานข้อมูลผู้ป่วย</li><li>เฉพาะกลุ่มโรค</li></ul>		

# การดำเนินงานเรื่อง PDPA



concent การให้ข้อมูลและการนำข้อมูล sensitive data ไปใช้งานของ ความยินยอมของผู้ให้ข้อมูล และผู้ใช้ ผ้ป่วย ข้อมูล วางแผนการจัดเก็บข้อมูลภายในโรงพยาบาลโดยกำกับดูแลจากผู้ การเก็บรวบรวมข้อมูล ได้รับอำนาจจากผู้บริหาร และผู้ได้รับสิทธิ์เท่านั้นจึงสามารถนำเข้า ข้อมูลได้ การนำฐานข้อมูลออกจาก server ต้องได้รับอนุญาตจากผู้อำนวยการ การเชื่อมโยงฐานข้อมูล และ ได้รับความยินยอมจากผู้ป่วยหากเป็นกลุ่ม sensitive data มีการวางระดับผู้เข้าถึงข้อมูลเป็นลำดับ โดยพิจารณาความจำเป็นการ การควบคุมนำข้อมูลไปใช้ เข้าถึงข้อมูล และวางมาตรการการระบุตัวตนผู้เข้าถึงข้อมูลทุกครั้ง เพิ่มความรอบรู้เรื่องพรบ.คอมพิวเตอร์ กฎหมายสิทธิ์ และการละเมิด ประกาศนโยบาย PDPA เพื่อให้ สิทธ์ส่วนบุคคล โดยเฉพาะเรื่อง Medical record, การถ่ายรูป, การใช้ เจ้าหน้าที่เข้าใจในตัวกฎหมายและ สื่อ Social บริบทการทำงานในฐานะเจ้าหน้าที่รัฐ และผู้ให้บริการให้ถูกต้อง

## แนวทางการป้องกันการโจมตี ข้อมูลของหน่วยงานท่านเป็นอย่างไร

เนื่องด้วยสถานการณ์ปัจจุบันโรงพยาบาลได้ใช้ระบบ Intranet และระบบ Internet ในวงการบริการเดียวกัน โดยมีแนวทางการป้องกันโดย

- ติดตั้งและupdate Firewall ในการป้องกันการเชื่อมโยงสู่ระบบ internet
- ให้ความรู้ และขอความร่วมมือจากเจ้าหน้าที่ในการเลือกใช้สื่อทาง อินเตอร์เน็ต หรือการดาวโหลด file ต่างๆทาง computer ของรพ.

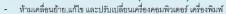
## แนวทางการตอบสนองเมื่อมีการโจมตีทาง Cyber

- เครื่องพรอัมใช้งานสามารถแทนเครื่องแม่ข่ายหลักได้1 เครื่อง
- ี้ มีเครื่องสา ํรองขอ*้*มถู 2 เครื่อง
- มีการสา ํรองแบบ realtime ไปเก็บไว้2 เครื่ออง
- มีการสำรองแบบ data initial ทกุ ๆ15วัน
- มีการสำรองแบบ Backup File ทกุ ๆ 7วัน
- มีการสำรองออกจากระบบเครือข่าย ทกุ ๆ 7วัน
- แผนและแนวทางการกู้คืนระบบ HosXP

ในระบบเทคโนโลยีสารสนเทศ และแนวทางการปฏิบัติการใช้งานสื่อสังคมออนไลน์ สำหรับเจ้าหน้าที่โรงพยาบาลกาฬสินธ์



## การป้องกันทรัพย์สินทางคอมพิวเตอร์ (Hardware)







## 2. การป้องกันด้านโปรแกรม (Solfware)

การติดตั้งโปรแกรมต่าง (Solfware ) ต้องได้รับอนุญาตจากผู้ดูแลระบบ

การ Download / Update ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์







### 3. การใช้งาน Internet

ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการพิสูจน์ตัวตน (Login Authen) ทุกครั้งก่อนการใช้งาน









### 4. การใช้สื่อ Social Network

ห้ามมิให้แสดงข้อความ รูปภาพที่ไม่สุขภาพ การปลุกเจ้าที่ทำให้เกิดความแตกแยก การทำลายสถาบัน <mark>ห้ามเปิดเผยเ</mark>อกสารความลับของผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ป่วยหรือผู้มีอำนาจเป็นลายลักษณ์อักษรเ





### 5. การใช้งานระบบ HIS (HOSxP)

ห้ามผู้ที่ไม่เกี่ยวข้องเข้าใช้งานระบบ



ห้ามมิให้ผู้อื่นใช้ User Password ของตนเอง

ห้ามเปิดเผย แก้ไข / ดัดแปลง ข้อมูลผู้ป่วยจากความเป็นจริง