

PDPA and Cyber Security

นพ.ฉัตรพล ตวงศิริทรัพย์

หน่วยงาน : โรงพยาบาลกาฬสินธุ์ โรงพยาบาลทั่วไปขนาด 540 เตียง ระดับ S

การดำเนินงานด้านฐานข้อมูลผู้ป่วย

วิเคราะห์ระบบภาพรวม

System	Struckture	Staff
● ระบบศูนย์ประกัน	● Server HosXP	● บุคลากรให้บริการทางการแพทย์
● ระบบHIS (HosXP ver3)	● Computer ใช้น้างาน	● เจ้าหน้าที่IT
● ระบบ Refer	● โครงสร้าง Intranet	● เจ้าหน้าที่ที่เกี่ยวข้องกับการบริการอื่นๆ (back office)
● ระบบควบคุมการใช้งานข้อมูล Digital ในรพ.	● โครงสร้าง Internet และ Firewall	
● ระบบฐานข้อมูลผู้ป่วยเฉพาะกลุ่มโรค		

การดำเนินงานเรื่อง PDPA



Sensitive
Personal Data

“ข้อมูลชีวภาพ” ตาม PDPA คือ
Biometric Data (ที่ถูก คือ ข้อมูลชีว
มาตร/ชีวมิติ) ใน พ.ร.บ. ใช้คำผิด
แต่คำอธิบายใน พ.ร.บ. หมายถึง
Biometric Data

Reference: PDPA ม.26

ความยินยอมของผู้ให้ข้อมูล และผู้ใช้ข้อมูล	concent การให้ข้อมูลและการนำข้อมูล sensitive data ไปใช้งานของผู้ป่วย
การเก็บรวบรวมข้อมูล	วางแผนการจัดเก็บข้อมูลภายในโรงพยาบาลโดยกำกับดูแลจากผู้ได้รับอำนาจจากผู้บริหาร และผู้ได้รับสิทธิ์เท่านั้นจึงสามารถนำข้อมูลได้
การเชื่อมโยงฐานข้อมูล	การนำฐานข้อมูลออกจาก server ต้องได้รับอนุญาตจากผู้อำนวยการ และได้รับความยินยอมจากผู้ป่วยหากเป็นกลุ่ม sensitive data
การควบคุมนำข้อมูลไปใช้	มีการวางระดับผู้เข้าถึงข้อมูลเป็นลำดับ โดยพิจารณาความจำเป็นการเข้าถึงข้อมูล และวางมาตรการการระบุตัวตนผู้เข้าถึงข้อมูลทุกครั้ง
ประกาศนโยบาย PDPA เพื่อให้เจ้าหน้าที่เข้าใจในตัวกฎหมายและบริบทการทำงานในฐานะเจ้าหน้าที่รัฐ และผู้ให้บริการให้ถูกต้อง	เพิ่มความรอบรู้เรื่องพรบ.คอมพิวเตอร์ กฎหมายสิทธิ และการละเมิดสิทธิส่วนบุคคล โดยเฉพาะเรื่อง Medical record, การถ่ายรูป, การใช้สื่อ Social

แนวทางการป้องกันการโจมตี ข้อมูลของหน่วยงานท่านเป็นอย่างไร

เนื่องด้วยสถานการณ์ปัจจุบัน โรงพยาบาลได้ใช้ระบบ Intranet และระบบ

Internet ในวงการบริการเดียวกัน โดยมีแนวทางการป้องกันโดย

1. ติดตั้งและupdate Firewall ในการป้องกันการเชื่อมโยงสู่ระบบ internet
2. ให้ความรู้ และขอความร่วมมือจากเจ้าหน้าที่ในการเลือกใช้สื่อทางอินเทอร์เน็ต หรือการดาวน์โหลด file ต่างๆทาง computer ของรพ.

แนวทางการตอบสนองเมื่อมีการโจมตีทาง Cyber

1. เครื่องพรอซีจันสามารถแทนเครื่องแม่ข่ายหลักได้ 1 เครื่อง
2. มีเครื่องสำรองข้อมูล 2 เครื่อง
3. มีการสำรองแบบ realtime ไปเก็บไว้ 2 เครื่อง
4. มีการสำรองแบบ data initial ทุก ๆ 15 วัน
5. มีการสำรองแบบ Backup File ทุก ๆ 7 วัน
6. มีการสำรองออกจากระบบเครือข่าย ทุก ๆ 7 วัน
7. แผนและแนวทางการกู้คืนระบบ HosXP

ทบทวน/ปรับปรุง

นโยบาย และระเบียบปฏิบัติด้านความมั่นคงปลอดภัย

ในระบบเทคโนโลยีสารสนเทศ และแนวทางการปฏิบัติการใช้งานสื่อสังคมออนไลน์
สำหรับเจ้าหน้าที่โรงพยาบาลกาฬสินธุ์

1

1. การป้องกันทรัพย์สินทางคอมพิวเตอร์ (Hardware)

- ห้ามเคลื่อนย้าย, แกะไข และปรับเปลี่ยนเครื่องคอมพิวเตอร์ เครื่องพิมพ์
- ห้ามนำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นๆมาเชื่อมต่อกับระบบเครือข่าย(ก่อนได้รับอนุญาต)



2

2. การป้องกันด้านโปรแกรม (Software)

- การติดตั้งโปรแกรมต่าง (Software) ต้องได้รับอนุญาตจากผู้ดูแลระบบ
- ห้ามจดหรือบันทึก Username Password ไว้ในสถานที่ต่างๆ เช่น เขียน User Password ติดไว้ตามเครื่องคอมพิวเตอร์ (ควรเก็บรักษาไว้เป็นความลับ)



3

3. การใช้งาน Internet

- ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการพิสูจน์ตัวตน (Login Authen) ทุกครั้งก่อนการใช้งาน
- การ Download / Update ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์



4

4. การใช้สื่อ Social Network

- ห้ามมิให้แสดงข้อความ รูปภาพที่ไม่สุภาพ การปลุกเร้าทำให้เกิดความแตกแยก การทำลายสถาบัน
- ห้ามเปิดเผยเอกสารความลับของผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ป่วยหรือผู้มีอำนาจเป็นลายลักษณ์อักษรก่อน



5

5. การใช้งานระบบ HIS (HOSXP)

- ห้ามผู้ที่ไม่เกี่ยวข้องเข้าใช้งานระบบ
- ห้ามมิให้ผู้อื่นใช้ User Password ของตนเอง
- ห้ามเปิดเผย, แกะไข / ดัดแปลง ข้อมูลผู้ป่วยจากความเป็นจริง

