PDPA and Cyber Security

นพ.จารุพล ตวงศิริทรัพย์

หน่วยงาน : โรงพยาบาลกาฬสินธุ์ โรงพยาบาลทั่วไปขนาด 540 เตียง ระดับ S

การดำเนินงานด้านฐานข้อมูลผู้ป่วย

วิเคราะห์ระบบภาพรวม

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

การดำเนินงานเรื่อง PDPA

Sensitive Personal Data

"ข้อมูลชีวภาพ" ตาม PDPA คือ Biometric Data (ที่ถูก คือ ข้อมูลชีวมาตร/ชีวมิติ) ใน พ.ร.บ. ใช้คำผิด แต่คำอธิบายใน พ.ร.บ. หมายถึง Biometric Data

Reference: PDPA ม.26

17

ความยินยอมของผู้ให้ข้อมูล และผู้ใช้ข้อมูล	concent การให้ข้อมูลและการนำข้อมูล sensitive data ไปใช้งานของผู้ป่วย
การเก็บรวบรวมข้อมูล	วางแผนการจัดเก็บข้อมูลภายในโรงพยาบาลโดยกำกับดูแลจากผู้ได้รับอำนาจจากผู้บริหาร และผู้ได้รับสิทธิ์เท่านั้นจึงสามารถนำเข้าข้อมูลได้
การเชื่อมโยงฐานข้อมูล	การนำฐานข้อมูลออกจาก server ต้องได้รับอนุญาตจากผู้อำนวยการ และได้รับความยินยอมจากผู้ป่วยหากเป็นกลุ่ม sensitive data
การควบคุมนำข้อมูลไปใช้	มีการวางระดับผู้เข้าถึงข้อมูลเป็นลำดับ โดยพิจารณาความจำเป็นการเข้าถึงข้อมูล และวางมาตรการการระบุตัวตนผู้เข้าถึงข้อมูลทุกครั้ง
ประกาศนโยบาย PDPA เพื่อให้เจ้าหน้าที่เข้าใจในตัวกฎหมายและบริบทการทำงานในฐานะเจ้าหน้าที่รัฐและผู้ให้บริการให้ถูกต้อง	เพิ่มความรอบรู้เรื่องพรบ.คอมพิวเตอร์ กฎหมายสิทธิ์ และการละเมิดสิทธ์ส่วนบุคคล โดยเฉพาะเรื่อง Medical record, การถ่ายรูป, การใช้สื่อ Social

แนวทางการป้องกันการโจมตี ข้อมูลของหน่วยงานท่านเป็นอย่างไร

เนื่องด้วยสถานการณ์ปัจจุบันโรงพยาบาลได้ใช้ระบบ Intranet และระบบ Internet ในวงการบริการเดียวกัน โดยมีแนวทางการป้องกันโดย

1. ติดตั้งและupdate Firewall ในการป้องกันการเชื่อมโยงสู่ระบบ internet
2. ให้ความรู้ และขอความร่วมมือจากเจ้าหน้าที่ในการเลือกใช้สื่อทางอินเตอร์เน็ต หรือการดาวโหลด file ต่างๆทาง computer ของรพ.

แนวทางการตอบสนองเมื่อมีการโจมตีทาง Cyber

1. เครื่องพรอ้มใช้งานสามารถแทนเครื่องแม่ข่ายหลักได้1 เครื่อง
2. มีเครื่องสา:รองขอ้มลู 2 เครื่อง
3. มีการสา:รองแบบ realtime ไปเก็บไว้2 เครื่อออง
4. มีการสำรองแบบ data initial ทกุ ๆ15วัน
5. มีการสำรองแบบ Backup File ทกุ ๆ 7วัน
6. มีการสำรองออกจากระบบเครือข่าย ทกุ ๆ 7วัน
7. แผนและแนวทางการกู้คืนระบบ HosXP