“PDPA & Cyber security in office”

ใบงานเดี่ยว

NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

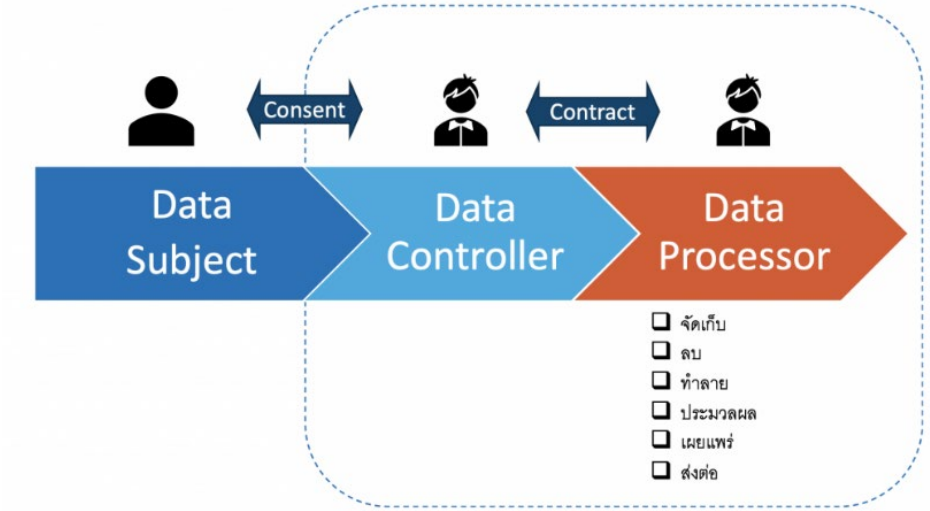
NO.2 แนวทางการป้องกันการโจมตีข้อมูลของหน่วยงานท่านเป็นอย่างไร

Yadzaree Lohlah กองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุข

NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

1. มีการจัดทำนโยบายส่วนบุคคล (Privacy Policy) เพื่อแจ้งเจ้าของข้อมูลและวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเผยแพร่ เพื่อให้เข้าใจบทบาทหน้าที่

2. มีการกำหนดบทบาทหน้าที่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล (data security) Data Controller, Data Processor, Data Subject



NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

3. มีการจัดทำบันทึกข้อตกลงการใช้งานข้อมูลขององค์กรร่วมกัน Data Processing Agreement, Data Sharing Agreement

4. การจัดทำแผนประเมินความเสี่ยง (Risk Assessment plan)

การพิจารณาระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในแต่ละด้าน (impact levels) ของข้อมูลในแพลตฟอร์มหมอพร้อม

ระดับชั้นของข้อมูล	ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง				ความเสียหาย ทางการเงิน				ความเสียหายต่อ การดำเนินงาน ขององค์กรหรือต่อ ผลประโยชน์สาธารณะ				การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต				ความปลอดภัย ของบุคคล				การละเมิดทางแพ่ง หรือทางอาญา			
	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**	โอกาส	ผลกระทบ	คะแนน	**ความเสี่ยง**
1. ข้อมูลทั่วไป	1	1	1	ปานกลาง	1	1	1	ต่ำ	1	1	1	ต่ำ	1	1	1	ต่ำ	2	1	2	ปานกลาง	1	1	1	ต่ำ
2. ข้อมูลสุขภาพสำหรับประชาชน	1	2	2	ปานกลาง	1	1	1	ต่ำ	1	1	1	ต่ำ	1	2	2	ต่ำ	1	1	1	ต่ำ	2	2	4	ปานกลาง
3. ข้อมูลสุขภาพ สำหรับเจ้าหน้าที่เกี่ยวข้องกับการรักษา เช่น แพทย์	1	2	2	ปานกลาง	1	1	1	ต่ำ	2	1	2	ปานกลาง	2	3	6	สูง	1	2	2	ปานกลาง	3	3	9	สูง

NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

หนังสือให้ความยินยอม
ในการประมวลผลข้อมูลส่วนบุคคล

ข้าพเจ้า (นาย/นาง/นางสาว) ชื่อ..... นามสกุล .....
เลขประจำตัวประชาชน: ..... ที่อยู่ที่ติดต่อได้ บ้านเลขที่.....ตรอก/ซอย.....ถนน
..... ตำบล/แขวง..... อำเภอ/เขต.....
จังหวัด..... โทรศัพท์..... ตกลง ให้กระทรวงสาธารณสุขโดย [หน่วยงานที่ขอความยินยอม] ซึ่งรวมถึงผู้ปฏิบัติงานและตัวแทนของ[หน่วยงานที่ขอความยินยอม] (“[หน่วยงานที่ขอความยินยอม]”) ทำการเก็บรวบรวม ใช้ **ข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่มีความอ่อนไหว** ของข้าพเจ้าที่ให้ไว้กับ[หน่วยงานที่ขอความยินยอม] และเปิดเผยให้แก่บุคคลหรือหน่วยงานที่ [หน่วยงานที่ขอความยินยอม] มอบหมาย เพื่อวัตถุประสงค์ดังต่อไปนี้ (สามารถเลือกได้มากกว่า 1 ข้อ)

ข้อมูลส่วนบุคคล

ยินยอม	ไม่ยินยอม	วัตถุประสงค์
☐	☐	เพื่อประโยชน์ในการพัฒนาและปรับปรุงการให้บริการของ[หน่วยงานที่ขอความยินยอม]
☐	☐	เพื่อวัตถุประสงค์ทางการตลาด การส่งเสริมการขาย การประชาสัมพันธ์ผลิตภัณฑ์และบริการของ[หน่วยงานที่ขอความยินยอม] การรับข้อมูลข่าวสาร รวมถึงสิทธิประโยชน์ต่าง ๆ
☐	☐	เพื่อการสถิติ ศึกษาวิจัย วิเคราะห์ และประเมินผลข้อมูล เพื่อประโยชน์ในการพัฒนาผลิตภัณฑ์และบริการของ[หน่วยงานที่ขอความยินยอม] รวมถึงการจัดกิจกรรมต่าง ๆ ของ[หน่วยงานที่ขอความยินยอม]
☐	☐	เพื่อการนำเสนอผลิตภัณฑ์หรือบริการของพันธมิตรหรือคู่ความร่วมมือของ[หน่วยงานที่ขอความยินยอม]

*การให้หรือไม่ให้ความยินยอมไม่ส่งผลต่อการพิจารณาการใช้บริการต่าง ๆ

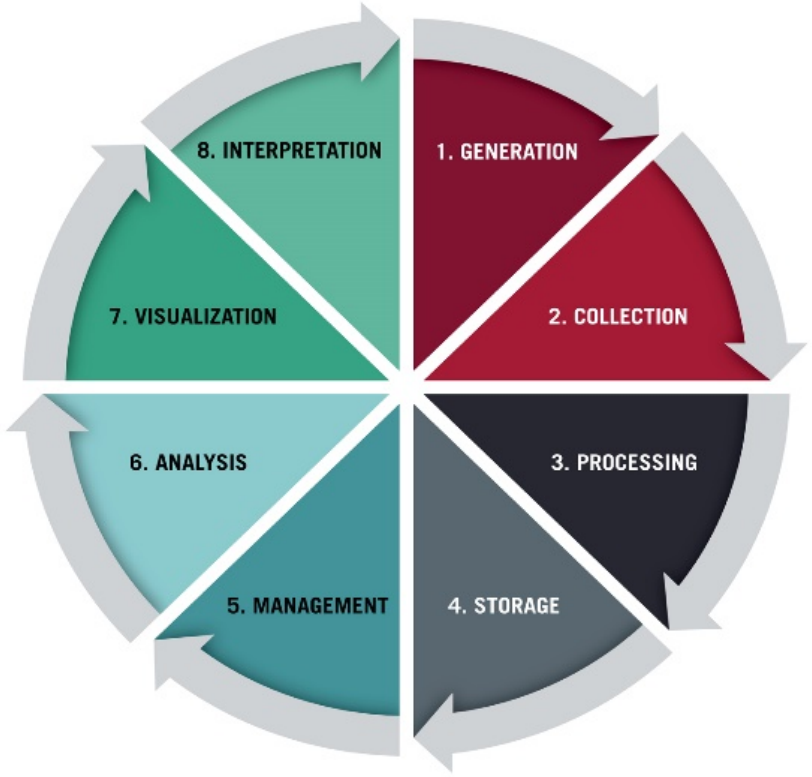
ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (ใช้เฉพาะกรณีที่มีการเก็บข้อมูลชีวภาพและข้อมูลความพิการ)

ยินยอม	ไม่ยินยอม	วัตถุประสงค์
☐	☐	ข้อมูลชีวภาพ ได้แก่ ข้อมูลภาพจำลองใบหน้า เพื่อประกอบการสร้างความสัมพันธ์ รวมถึงการพิสูจน์และยืนยันตัวตนผู้ขอใช้บริการกับ[หน่วยงานที่ขอความยินยอม]

ลงชื่อ ..... เจ้าของข้อมูลส่วนบุคคล
(.....)

NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

5. มีการจดบันทึกกิจกรรม (Record of Processing Activities หรือ RoPA) ของแผนวงจรชีวิตข้อมูลส่วนบุคคล (The Data Life Cycle) ตามมาตรฐานพรบ.ข้อมูลส่วนบุคคล



NO.1 แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

5. มีการจดบันทึกกิจกรรม (Record of Processing Activities หรือ RoPA) ของแผนวงจรชีวิตข้อมูลส่วนบุคคล (The Data Life Cycle) ตามมาตรฐานพรบ.ข้อมูลส่วนบุคคล

ประเภทของข้อมูลที่ทำการจัดเก็บ (Types of personal information collected)	Data Classification	ฐานการประมวลผล (Lawful Basis)		Have individuals been notified of the purposes for which their information is collected, used and disclosed?	Issues, Vulnerabilities, Weaknesses
ชื่อ สกุล		สัญญา			
อายุ					
ปีเกิด					
ที่อยู่					
ประวัติการศึกษา					

Collection (การเก็บรวบรวม)				Storage (การเก็บรักษา)		การใช้ในองค์กร (Usage within organisation)		การโอน การเปิดเผยไปยังองค์กรภายนอก (Transfer/Disclosure to External Parties)		Retention & Disposal		Issues, Vulnerabilities, Weaknesses
วัตถุประสงค์การจัดเก็บ (Purpose of collection)	ผู้ใช้ข้อมูล (Data Owner)	รูปแบบการนำเข้าข้อมูล (Collection Source)	สื่อที่ใช้ในการจัดเก็บ (Collection Medium)	สถานที่เก็บทางกายภาพ (Physical Storage)	สถานที่เก็บอิเล็กทรอนิกส์ (Electronic Storage)	ฝ่ายอื่นที่ใช้ข้อมูล/วัตถุประสงค์การใช้ (Users of Personal Data and Purpose of Usage)	ฝ่ายอื่นที่เข้าถึง (Access to Personal Data)	องค์กรอื่นที่มีการเปิดเผย (External Parties and Purpose of Transfer/ Disclosure)	รูปแบบการโอน (Transfer Mode) [กระดาษ/อิเล็กทรอนิกส์]	ระยะเวลาการจัดเก็บ (Retention Period)	การทำลายข้อมูล (Disposal Methods)	
การสมัครงาน	HR	จากผู้สมัครโดยตรง	ใบสมัคร	ตู้เอกสาร HR	HR Drive	Management/เพื่อการพิจารณาคัดเลือก	IT Dept	กรมการจัดหางาน/สถิติ	electroonics	1 ปี	ย่อยทำลาย	
			Web form		HR Drive					1 ปี	ใช้แถบแม่เหล็กทำลายข้อมูล	

NO.2 แนวทางการป้องกันการโจมตี ข้อมูลของหน่วยงานท่านเป็นอย่างไร (หน่วยงานกยผ.)

1. **มีการป้องกันทางด้าน physical จากภัยคุกคามที่อาจเกิดขึ้นได้จากธรรมชาติ หรือ มนุษย์**
    1. แผนการรับมือกรณีต่างๆ เช่น เกิดเหตุภัยพิบัติ ไฟไหม้ น้ำท่วม
    2. การติดกล้องวงจรปิด
    3. การติดประตูนิรภัยของห้อง Data Center
    4. การกำหนดบทบาทหน้าที่ของเจ้าหน้าที่ในการห้อง Data Center

NO.2 แนวทางการป้องกันการโจมตี ข้อมูลของหน่วยงานท่านเป็นอย่างไร (หน่วยงานกยผ.)

2. มีการป้องกันทางด้าน Logical-Network

1. การย้ายระบบสู่ Cloud Server ในที่ปลอดภัยมีระบบป้องกัน เช่น firewall
2. การจำกัดและกำหนดสิทธิผู้ดูแลเข้าใช้งาน Server DB
3. การใช้งาน VPN VM
4. การจำกัดวง Lan การเข้าถึง Internet ในองค์กรจากบุคคลภายนอก/ private IP
5. Anti-Virus / update OS