PDPA ในโรงพยาบาล: ดูแลข้อมูล เหมือนดูแลชีวิต

คู่มือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรทางการแพทย์

โรงพยาบาล: ศูนย์กลางข้อมูลขนาดใหญ่ของชีวิต

การแจ้งเกิด (Birth)
ข้อมูลทารกเพื่อแจ้งเกิด

การรักษา (Treatment)
ประวัติการรักษาตลอดชีวิต

การเสียชีวิต (Death)
ข้อมูลใบมรณบัตร

Key Insight: โรงพยาบาลมีการประมวลผลข้อมูลทุกวัน จึงมีความเสี่ยงที่ข้อมูลจะรั่วไหลหรือถูกโจรกรรมได้ตลอดเวลา

ข้อมูลอ่อนไหว (Sensitive Data) คือสัญญาณชีพที่ต้องปกป้อง

ข้อมูลเหล่านี้ระบุตัวตนได้ทั้งทางตรงและทางอ้อม และต้องได้รับการดูแลความปลอดภัยขั้นสูง

เวชระเบียน /
ประวัติการรักษา

ข้อมูลกรุ๊ปเลือด /
ข้อมูลชีวภาพ

ประวัติการใช้ยา /
การแพ้ยา

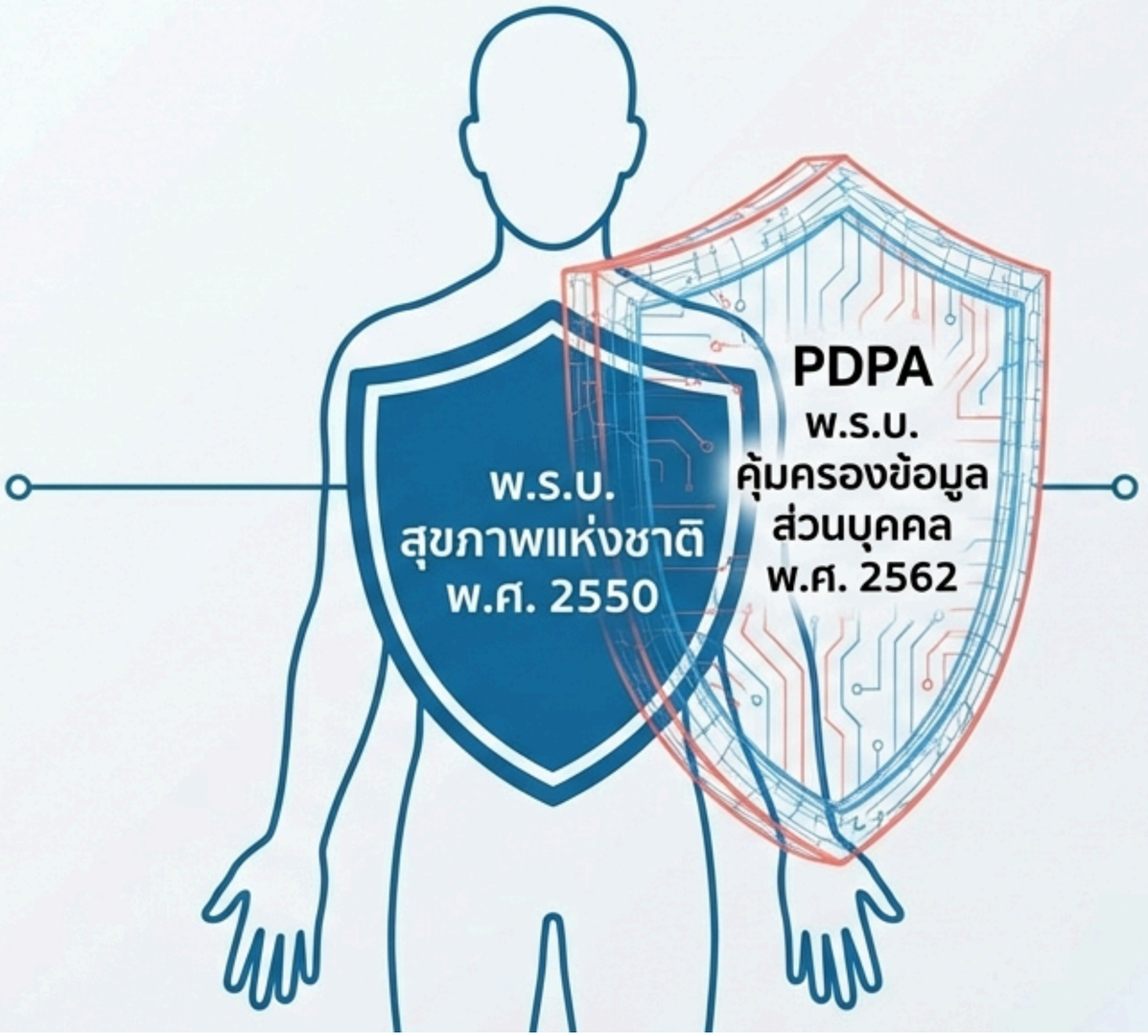
ประวัติการผ่าตัด

ข้อมูลประกันสุขภาพ /
ประกันสังคม

ผลตรวจทางห้องปฏิบัติการ /
ภาพถ่ายรังสี

เกราะป้องกัน 2 ชั้น: กฎหมายคุ้มครองความลับผู้ป่วย

เกราะชั้นแรก:
หลักการคุ้มครอง
ข้อมูลสุขภาพเดิม



เกราะชั้นที่ 2:
คุ้มครองการ
ประมวลผล ถ่ายโอน
และข้อมูลอ่อนไหว
(Sensitive Data)

บทบาทและหน้าที่ในระบบนิเวศข้อมูล

Data Subject
(เจ้าของข้อมูล)
คนไข้ / ผู้มาใช้บริการ

ให้ข้อมูล /
ให้ความยินยอม

Data Controller
(ผู้ควบคุมข้อมูล)
โรงพยาบาล
(ผู้ตัดสินใจเก็บ/ใช้ข้อมูล)

ส่งต่อข้อมูลตามคำสั่ง

Data Processor
(ผู้ประมวลผลข้อมูล)
ประกันสังคม / บริษัทประกัน /
รพ.รับส่งต่อ

หมายเหตุ: กรณีรับเคสคนไข้ส่งต่อ โรงพยาบาลผู้รับจะกลายเป็น Data Controller

เวชระเบียน: หัวใจและจุดเริ่มต้นของการคุ้มครอง

- **จุดเริ่มต้น (The Start):** ก้าวแรกของผู้ใช้บริการเริ่มที่แผนกเวชระเบียน
- **ข้อมูลที่เก็บ (Data):** ชื่อ, ที่อยู่, เลขบัตรประชาชน, วันเกิด, กรุ๊ปเลือด

ข้อมูลภายใน: ข้อมูลของแพทย์ พยาบาล และลูกจ้าง ก็ต้องได้รับการคุ้มครองเช่นกัน

ความยินยอม (Consent) vs. ข้อยกเว้นทางการแพทย์

ต้องขอความยินยอม (Consent Required)

สำหรับการเก็บข้อมูลทั่วไปและการเปิดเผยข้อมูล

ข้อยกเว้น: ไม่ต้องขอความยินยอม (Exceptions)

Vital Interest (ฐานประโยชน์สำคัญต่อชีวิต)

กรณีฉุกเฉิน / ผู้ป่วยไร้สติ
เพื่อป้องกันอันตรายต่อชีวิต

Public Health (ฐานประโยชน์สาธารณะ)

ป้องกันโรคระบาด
(เช่น COVID-19 Timeline)

ฐานทางกฎหมายอื่นๆ ในการประมวลผล

การทำงานประจำวันในโรงพยาบาล มักรองรับด้วยฐานกฎหมายเหล่านี้ (ไม่ต้องขอ Consent แยก)

Contract Basis (ฐานสัญญา)

เพื่อปฏิบัติตามสัญญาระหว่างผู้ป่วยกับโรงพยาบาล ในการให้บริการรักษา

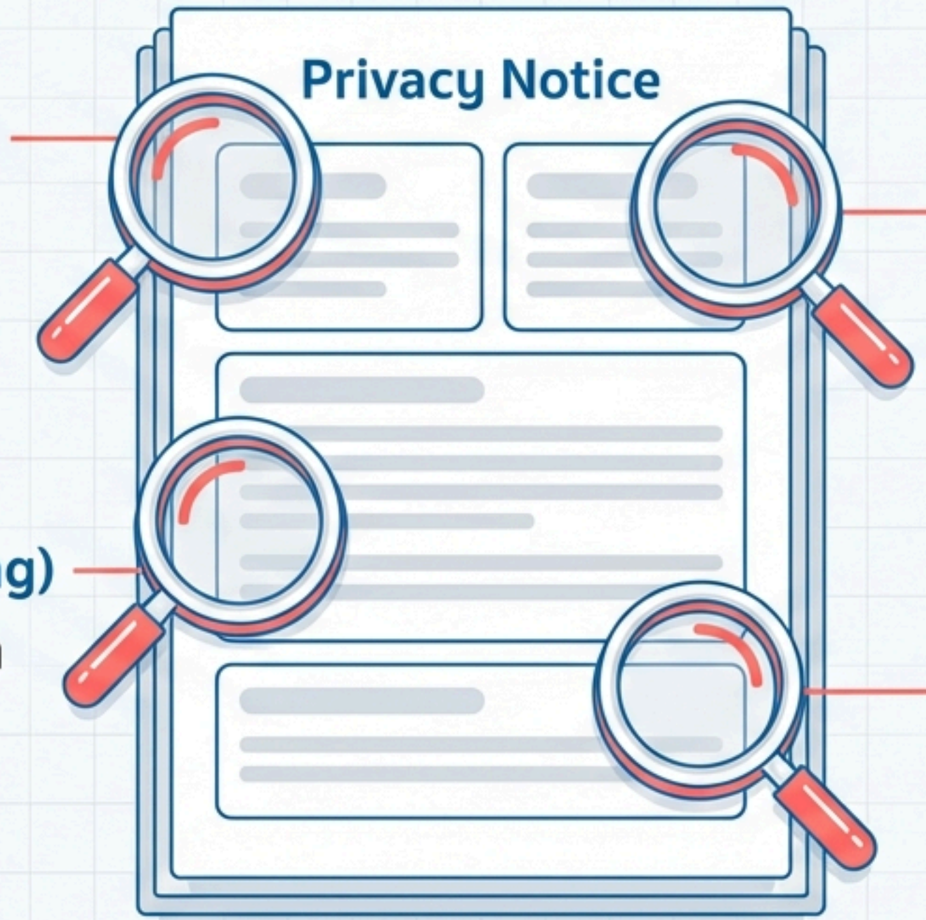
Health / Social Care (ฐานการดูแลรักษาสุขภาพ)

การวินิจฉัยโรคทางการแพทย์ และการจัดการด้านสุขภาพโดยบุคลากรวิชาชีพ (เช่น แพทย์เรียกดูประวัติ)

ข้อควรจำ: แม้ไม่ต้องขอ Consent แต่ต้องแจ้งให้ทราบผ่าน Privacy Notice เสมอ

เครื่องมือแห่งความโปร่งใส: Privacy Notice

สิ่งที่ต้องแจ้งให้ผู้ป่วยทราบ **‘ก่อน’** หรือ **‘ขณะ’** เก็บข้อมูล



เก็บอะไร? (What)

- ชื่อ
- ประวัติสุขภาพ
- ผลเลือด

เก็บนานเท่าไร? (How Long)

- ตามกฎหมายสถานพยาบาล

เก็บทำไม? (Why)

- เพื่อการรักษา
- นัดหมาย
- การเงิน

ให้ใครบ้าง? (Who)

- บริษัทประกัน
- รพ. ส่งต่อ

ทำไมต้องมี Privacy Notice?

เหตุผลสำคัญที่โรงพยาบาลต้องจัดทำและแจ้งนโยบายความเป็นส่วนตัว (Privacy Notice)

1. ปฏิบัติตามกฎหมาย

PDPA มาตรา 23 บังคับไว้ ฝ่าฝืน**ปรับสูงสุด 1 ล้านบาท**

2. ความโปร่งใส

สร้างความชัดเจน ให้ผู้ป่วยทราบขอบเขต

3. คุ้มครองข้อมูลอ่อนไหว

ป้องกันการใช้ผิดวัตถุประสงค์

4. รองรับการเชื่อมโยง

ระบุฐานกฎหมาย เมื่อต้องส่งตัวผู้ป่วย (Refer)

สิทธิของผู้ป่วยในฐานะเจ้าของข้อมูล

สิทธิในการเข้าถึง (Right to Access)

ขอรับสำเนาข้อมูลการรักษาของตนเอง

สิทธิในการแก้ไข (Right to Rectify)

ขอแก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบัน

สิทธิในการลบ (Right to Delete)

ขอให้ลบข้อมูลเมื่อหมดความจำเป็น (ตามเงื่อนไขกฎหมาย)

สิทธิในการถอนความยินยอม (Right to Withdraw)

ยกเลิกความยินยอม ที่เคยให้ไว้ได้

บทสรุป: มาตรฐานการดูแลข้อมูล คือมาตรฐานการรักษา

- ข้อมูลสุขภาพ = Sensitive Data ที่ต้องดูแลเหมือนชีวิต
- เข้าใจบทบาท: Hospital (Controller) vs Patient (Subject)
- ฉุกเฉิน (Vital Interest) ช่วยชีวิตได้ทันที ไม่ต้องรอ Consent
- Privacy Notice คือเกราะคุ้มครองทางกฎหมาย

“ การรักษาความปลอดภัยของข้อมูล
คือส่วนหนึ่งของการรักษาผู้ป่วย”

จัดทำและเรียบเรียงโดย

นายธนโชติ มีมานะทำ

นิติกรปฏิบัติการ คณะแพทยศาสตร์ มหาวิทยาลัยบูรพา