

บทนำความมั่นคงสารสนเทศทางการแพทย์

Week 1 — Introduction to Medical Information Security

หัวข้อการเรียนรู้

- ความหมายและความสำคัญของความมั่นคงสารสนเทศ
- บริบทด้านข้อมูลสุขภาพและระบบสาธารณสุข
- ลักษณะเฉพาะของข้อมูลสุขภาพ
- วิเคราะห์กรณีศึกษาและอภิปราย
- รวมเวลาเรียน: **120 นาที**

ความหมายของความมั่นคงสารสนเทศ

Information Security

- การคุ้มครองข้อมูลเพื่อรักษา
 - **Confidentiality** (ความลับ)
 - **Integrity** (ความถูกต้องครบถ้วน)
 - **Availability** (ความพร้อมใช้งาน)
- กรอบคิด **CIA Triad**
- สำคัญต่อระบบสุขภาพซึ่งต้อง “ใช้ข้อมูลเพื่อการรักษาอย่างต่อเนื่องและน่าเชื่อถือ”

ความสำคัญในระบบสารสนเทศ

- ข้อมูลสุขภาพ = ข้อมูลอ่อนไหวพิเศษ
- ผลกระทบเมื่อข้อมูลรั่วไหล
 - ความเสี่ยงต่อผู้ป่วย เช่น การเลือกปฏิบัติ
 - ความเสียหายต่อองค์กร เช่น การหยุดบริการ
- ตัวอย่างเหตุการณ์จริง:
 - การโจมตีด้วย ransomware
 - การเข้าถึงเวชระเบียนโดยไม่ได้รับอนุญาต

องค์ประกอบความมั่นคงสารสนเทศ

Technical

- การเข้ารหัสข้อมูล
- การควบคุมสิทธิ์ (RBAC)
- ระบบตรวจจับการบุกรุก

Administrative

- นโยบายความปลอดภัย
- การประเมินความเสี่ยง

Human

- Social Engineering

มาตรฐานและกรอบงานสำคัญ

- ISO/IEC 27001
- NIST Cybersecurity Framework
- HIPAA (สหรัฐ), PDPA (ไทย)
- มาตรฐานด้านสุขภาพ เช่น HL7, FHIR

ลักษณะเฉพาะของข้อมูลสุขภาพ

- ความอ่อนไหวสูง
- เชื่อมโยงข้ามระบบและมีความต่อเนื่องยาวนาน
- ต้องการความถูกต้องระดับสูง
- รูปแบบข้อมูลหลากหลาย
 - ข้อความ, ผลตรวจ, ภาพรังสี, สัญญาณชีพ
- ใช้ในหลายหน่วยงานของโรงพยาบาล

โฟลว์ข้อมูลสุขภาพ (Health Data Flow)

ผู้ป่วย

- ห้องตรวจ
- เวชระเบียน (EMR/EHR)
- แล็บ/ภาพรังสี
- คลินิกเฉพาะทาง
- ระบบชำระเงิน
- ระบบสุขภาพระดับเครือข่าย

กิจกรรมที่ 1: ถาม-ตอบกระตุ้นความคิด

(10 นาที)

ตัวอย่างคำถาม

- ข้อมูลใดในโรงพยาบาลสำคัญที่สุดต่อการรักษา?
- หากข้อมูลถูกเปลี่ยนแปลง จะเกิดผลกระทบอย่างไร?

กิจกรรมที่ 2: วิเคราะห์กรณีศึกษา

(กลุ่มละ 4-5 คน, 25 นาที)

ตัวอย่างเหตุการณ์

1. การโจมตีด้วย ransomware
2. เจ้าหน้าที่แชร์ข้อมูลผู้ป่วยผิดช่องทาง
3. การเข้าถึงระบบ PACS โดยไม่ได้รับสิทธิ์

โจทย์ที่ต้องวิเคราะห์

1. เกิดเหตุการณ์อะไรขึ้น
2. CIA Triad ได้ได้รับผลกระทบ
3. สาเหตุเกิดจากปัจจัยใด (เทคนิค/กระบวนการ/บุคลากร)
4. แนวทางป้องกันและแก้ไข

กิจกรรมที่ 3: นำเสนอผลกลุ่ม

(10 นาที)

- กลุ่มละ 2-3 นาที
- เน้นการอธิบายเหตุผลและการเชื่อมโยงเข้ากับหลักความมั่นคงสารสนเทศ

สรุปบทเรียน

- ข้อมูลสุขภาพมีความสำคัญและอ่อนไหวสูง
- ความมั่นคงสารสนเทศเป็นรากฐานของระบบสาธารณสุข
- ต้องคำนึงถึงองค์ประกอบด้านเทคนิค กระบวนการ และบุคลากร
- ความตระหนักรู้และการป้องกันเชิงรุกจำเป็นอย่างยิ่ง

Thank You

Week 1 Completed

สอบถาม – อภิปราย – ทบทวนเพิ่มเติมได้ในชั้นเรียน