Lecture Note: Introduction to Medical Information Security

Week 1 — Foundations of Medical Information Security

1. บทนำ: ความมั่นคงปลอดภัยด้านสารสนเทศทางการแพทย์

บทเรียนสัปดาห์แรกมุ่งสร้างความเข้าใจพื้นฐานเกี่ยวกับ “ความมั่นคงปลอดภัยสารสนเทศ” ในบริบทของระบบสาธารณสุขและองค์กรทางการแพทย์ ซึ่งแตกต่างจากภาคธุรกิจทั่วไปอย่างมาก เนื่องจากข้อมูลสุขภาพมีลักษณะเฉพาะทั้งด้านความอ่อนไหว ความละเอียดอ่อน และความเชื่อมโยงข้ามระบบที่ซับซ้อน ความเข้าใจพื้นฐานนี้เป็นรากฐานสำคัญสำหรับการวิเคราะห์ภัยคุกคามและการออกแบบมาตรการป้องกันในสัปดาห์ต่อ ๆ ไป

2. หัวข้อการเรียนรู้หลัก (Learning Topics)

2.1 ความหมายและความสำคัญของความมั่นคงปลอดภัยสารสนเทศ

หัวข้อนี้มุ่งให้ผู้เรียนทำความเข้าใจว่า “ความมั่นคงปลอดภัยสารสนเทศ (Information Security)” เป็นแนวคิดที่กว้างและครอบคลุมมากกว่าภารกิจของฝ่ายไอที การรักษาความปลอดภัยไม่ใช่แค่การติดตั้งซอฟต์แวร์ป้องกันไวรัสหรือกำแพงไฟ (firewall) แต่เป็นส่วนหนึ่งของ **ระบบนิเวศ (ecosystem)** ขององค์กร โดยมีองค์ประกอบที่ต้องพิจารณาหลายมิติ ได้แก่:

1) มิติด้านเทคนิค (Technical Dimension)

เป็นเครื่องมือ กลไก หรือเทคโนโลยีที่ใช้ป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคาม เช่น

- การเข้ารหัสข้อมูล
- การพิสูจน์ตัวตนหลายปัจจัย (MFA)
- การตรวจจับการบุกรุก (IDS/IPS)

แม้ว่ามิติทางเทคนิคจะมีความสำคัญ แต่เพียงอย่างเดียวไม่เพียงพอในการสร้างความปลอดภัยที่ยั่งยืน

2) มิติด้านกระบวนการ (Process Dimension)

เป็นกรอบงาน กฎระเบียบ และขั้นตอนที่องค์กรออกแบบเพื่อให้กระบวนการทำงาน “ปลอดภัยโดยโครงสร้าง (security by design)” เช่น

- นโยบายความปลอดภัยสารสนเทศ
- ขั้นตอนการสำรองข้อมูล
- การจัดการสิทธิการเข้าถึง
- แบบฟอร์มและเวิร์กโฟลว์ที่จำกัดโอกาสเกิด human error

กระบวนการที่ดีช่วยลดความเสี่ยงจากการใช้งานที่ไม่ถูกต้องหรือไม่สอดคล้องตามมาตรฐาน

3) มิติด้านบุคลากร (People Dimension)

ผู้ใช้งานระบบ เช่น แพทย์ พยาบาล เจ้าหน้าที่เวชระเบียน นักเทคนิคการแพทย์ และแอดมินระบบ ล้วนเป็นส่วนสำคัญของความปลอดภัย

- การตั้งรหัสผ่านไม่รัดกุม
- การส่งข้อมูลผ่านช่องทางส่วนตัว
- การตอบสนองต่อ social engineering
  เป็นตัวอย่างของความเสี่ยงที่เกิดจากบุคลากร

ความมั่นคงปลอดภัยที่แท้จริงต้องเกิดจากความร่วมมือระหว่างทุกฝ่ายในองค์กร ไม่ใช่ความรับผิดชอบของแผนกไอทีเพียงแผนกเดียว

2.2 บริบทข้อมูลสุขภาพและระบบบริการทางการแพทย์

ข้อมูลสุขภาพมีลักษณะเฉพาะจากกระบวนการผลิตและใช้งานที่กระจายอยู่หลายหน่วยงานในโรงพยาบาล ทำให้บริบทการจัดการข้อมูลมีความซับซ้อนกว่าระบบสารสนเทศทั่วไป

1) แหล่งกำเนิดข้อมูลหลากหลาย (Multi-source Data Production)

ข้อมูลทางการแพทย์ถูกผลิตในหลายจุด และทุกจุดมีระดับความละเอียดอ่อนต่างกัน เช่น

- ห้องตรวจผู้ป่วยนอก (OPD)
- ห้องผู้ป่วยใน (IPD)
- ห้องปฏิบัติการทางการแพทย์ (Laboratory)
- รังสีวินิจฉัย (Radiology/PACS)
- แผนกเวชระเบียน (MRD)
- ระบบการเงินและประกันสุขภาพ

แต่ละแผนกใช้ระบบที่แตกต่างกัน และต้องเชื่อมข้อมูลเพื่อให้แพทย์ตัดสินใจรักษาได้แม่นยำและทันเวลา

2) ความจำเป็นในการเชื่อมต่อระบบ (Integration Requirements)

การดูแลผู้ป่วยจำเป็นต้องดึงข้อมูลจากหลายระบบ เช่น ผลแล็บ ภาพเอกซเรย์ ประวัติยา จึงต้องมีการส่งต่อข้อมูลอย่างปลอดภัยตามมาตรฐาน เช่น HL7 หรือ FHIR เพื่อป้องกันข้อผิดพลาดและช่องโหว่ด้านความปลอดภัย

3) ความท้าทายด้านความปลอดภัย (Security Challenges)

- ความเสี่ยงจากระบบที่ล้าสมัย (legacy systems) ในโรงพยาบาล
- อุปกรณ์ทางการแพทย์ที่เชื่อมต่อเครือข่าย (IoMT)
- การเข้าถึงข้อมูลโดยบุคลากรจำนวนมาก
- ความเร่งด่วนของงานทางการแพทย์ที่อาจทำให้ละเลยมาตรการด้านความปลอดภัย

บริบทเหล่านี้ทำให้การรักษาความมั่นคงปลอดภัยข้อมูลสุขภาพมีความซับซ้อนและต้องมีกลยุทธ์เฉพาะทาง

2.3 คุณลักษณะเฉพาะของข้อมูลสุขภาพ

ข้อมูลสุขภาพมีความพิเศษที่ทำให้ต้องได้รับการดูแลอย่างรัดกุมมากกว่าข้อมูลทั่วไป ในมุมมองทางสาธารณสุข กฎหมาย และจริยธรรม

1) ความอ่อนไหวสูงมาก (Highly Sensitive)

ข้อมูลสุขภาพเปิดเผยถึงสภาวะร่างกาย จิตใจ และสภาวะทางสังคมของบุคคล เช่น

- ประวัติการติดเชื้อ HIV
- โรคทางจิตเวช
- ประวัติการผ่าตัด
  การรั่วไหลอาจก่อให้เกิดผลกระทบต่อชื่อเสียง การทำงาน และความสัมพันธ์ทางสังคม

2) ความหลากหลายของรูปแบบข้อมูล (Multi-modal Health Data)

ข้อมูลสุขภาพประกอบด้วยหลายรูปแบบ เช่น

- ตัวเลข (vital signs)
- ข้อความ (clinical notes)
- ผลแลบ
- ภาพรังสี
- สัญญาณชีพแบบต่อเนื่อง
  การปกป้องข้อมูลแต่ละประเภทต้องใช้เทคนิคที่แตกต่างกัน

3) ความเกี่ยวพันกับจริยธรรมและสิทธิผู้ป่วย (Ethical/Legal Concerns)

- การเก็บและใช้ข้อมูลต้องได้รับความยินยอม (informed consent)
- ผู้ป่วยมีสิทธิรู้และควบคุมข้อมูลของตนเองตาม PDPA
- ข้อมูลที่ผิดพลาดอาจนำไปสู่ความเสียหายทางการแพทย์ (medication error, misdiagnosis)

4) ความต้องการความถูกต้องและความต่อเนื่อง (Accuracy and Continuity)

ข้อมูลสุขภาพต้องไม่มีข้อผิดพลาดและต้องมีความต่อเนื่องในระยะยาว เช่น การติดตามผู้ป่วยเรื้อรังหลายปี ทำให้ตามหลักการแล้วต้องมีการจัดการข้อมูลอย่างเป็นระบบ

2.4 การวิเคราะห์กรณีศึกษา (Case Study Analysis)

หัวข้อนี้สอนให้ผู้เรียนฝึกนำแนวคิดทฤษฎีไปใช้กับสถานการณ์จริงในโรงพยาบาล เพื่อให้เกิดการคิดวิเคราะห์ในระดับปฏิบัติการและระดับกลยุทธ์

1) วัตถุประสงค์ของการใช้กรณีศึกษา

- เข้าใจผลกระทบของภัยคุกคามต่อผู้ป่วยและโรงพยาบาล
- ฝึกระบุองค์ประกอบของ CIA Triad ที่ถูกกระทบ
- วิเคราะห์สาเหตุราก (root cause analysis)
- เสนอแนวทางป้องกันและแก้ไขที่เป็นไปได้จริงในสถานพยาบาล

2) ประเภทสถานการณ์ที่มักนำมาศึกษา

- การโจมตี ransomware ทำให้ระบบ EMR ใช้งานไม่ได้
- เจ้าหน้าที่ส่งข้อมูลผ่านไลน์ส่วนตัว
- บุคคลภายนอกเข้าถึงภาพเอกซเรย์โดยไม่ได้รับอนุญาต
- ความผิดพลาดจากบุคลากรที่นำไปสู่การรั่วไหลของข้อมูล

3) ทักษะที่ผู้เรียนจะได้รับ

- การเชื่อมโยงเหตุการณ์กับหลักการความปลอดภัย
- การตั้งสมมติฐานและคิดวิเคราะห์เชิงระบบ
- การประเมินความเสี่ยงและวางมาตรการป้องกัน
- การมองภัยคุกคามในมุมมองของข้อมูลสุขภาพโดยเฉพาะ

3. ความหมายของความมั่นคงปลอดภัยสารสนเทศ (Information Security)

3.1 ขอบเขตและนิยามของความมั่นคงปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศเป็นศาสตร์ที่มุ่งเน้นการคุ้มครองข้อมูลในทุกมิติ ตั้งแต่ข้อมูลที่จัดเก็บในระบบสารสนเทศ การส่งผ่านข้อมูลบนเครือข่าย ไปจนถึงการบริหารจัดการบุคลากรที่เกี่ยวข้องกับข้อมูลนั้น โดยครอบคลุมการป้องกันภัยคุกคามทั้งจากภายในและภายนอกองค์กร ไม่ว่าจะเป็นอาชญากรไซเบอร์ ความผิดพลาดของบุคลากร หรือจุดอ่อนทางเทคนิคของระบบ

นิยามสำคัญคือ

> “การปกป้องข้อมูลจากการเข้าถึง การใช้ การเปิดเผย การแก้ไข และการทำลาย โดยไม่ได้รับอนุญาตหรือไม่เป็นไปตามวัตถุประสงค์ที่กำหนด”

แก่นหลักของการรักษาความมั่นคงปลอดภัยคือ **CIA Triad** ซึ่งเป็นกรอบคิดมาตรฐานสากลที่ใช้กำหนดนโยบายและออกแบบระบบรักษาความปลอดภัย

องค์ประกอบของ CIA Triad

1) ความลับ (Confidentiality)

หมายถึงการป้องกันไม่ให้ข้อมูลถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิหรือไม่จำเป็นต้องรู้ (need-to-know basis)

ความสำคัญในบริบทข้อมูลสุขภาพ

ข้อมูลสุขภาพถือเป็น “ข้อมูลอ่อนไหว (sensitive data)” ตามกฎหมายและจริยธรรมทางการแพทย์ การรั่วไหลอาจสร้างผลกระทบต่อผู้ป่วยทั้งทางร่างกาย จิตใจ สังคม และเศรษฐกิจ เช่น

- ความอับอายจากการเปิดเผยโรคเรื้อรัง
- การตีตราทางสังคม เช่น ผู้ป่วย HIV หรือโรคทางจิตเวช
- ความเสียหายต่อการทำงาน หากข้อมูลสุขภาพถูกใช้เป็นเหตุผลในการเลือกปฏิบัติ

ตัวอย่างความเสี่ยงด้านความลับในโรงพยาบาล

- การส่งข้อมูลผู้ป่วยผ่านช่องทางไม่ปลอดภัย เช่น LINE ส่วนตัว
- เจ้าหน้าที่เปิดดูประวัติผู้ป่วยที่ตนไม่มีส่วนเกี่ยวข้อง
- อุปกรณ์ที่ไม่ได้เข้ารหัส เช่น แฟลชไดรฟ์หาย
- แฮกเกอร์ขโมยข้อมูลเพื่อขายในตลาดมืด

แนวทางควบคุม

- การเข้ารหัส (encryption)
- RBAC และการกำหนดสิทธิ
- การตรวจสอบล็อกการเข้าถึงข้อมูล
- นโยบายห้ามนำข้อมูลออกนอกระบบโดยไม่จำเป็น

2) ความถูกต้องครบถ้วน (Integrity)

หมายถึงการรักษาความถูกต้อง ความเที่ยงตรง ความครบถ้วน และความสม่ำเสมอของข้อมูล ไม่ให้ถูกแก้ไข ดัดแปลง สูญหาย หรือบิดเบือน

ความสำคัญในงานทางการแพทย์

ข้อมูลสุขภาพเปรียบเสมือนรากฐานในการตัดสินใจรักษา ความผิดพลาดเพียงเล็กน้อยอาจนำไปสู่

- การวินิจฉัยผิดพลาด (misdiagnosis)
- การให้ยาเกินขนาดหรือไม่ตรงกับประวัติผู้ป่วย
- ความล่าช้าในการรักษาฉุกเฉิน
- ความเสียหายต่อกระบวนการประกันและเบิกจ่ายค่ารักษา

สถานการณ์ที่ Integrity ถูกกระทบ

- ผลแลบถูกแก้ไขโดยบุคคลที่ไม่ได้รับอนุญาต
- เครื่องมือแพทย์ส่งข้อมูลผิดพลาดจากการขัดข้อง
- ransomware ทำให้ข้อมูลถูกเข้ารหัสและไม่สามารถตรวจสอบได้
- ความผิดพลาดจากการป้อนข้อมูลของเจ้าหน้าที่ (human error)

แนวทางควบคุม

- การตรวจสอบความถูกต้องของข้อมูล (validation)
- การสำรองข้อมูลสม่ำเสมอ
- ระบบตรวจจับการแก้ไขข้อมูลผิดปกติ
- Digital signature หรือ hash function

3) ความพร้อมใช้งาน (Availability)

หมายถึงความสามารถของระบบสารสนเทศในการให้บริการได้อย่างต่อเนื่อง ไม่ล่ม ไม่ถูกขัดขวาง และตอบสนองต่อความต้องการของผู้ใช้งาน

ความสำคัญต่อความปลอดภัยทางการแพทย์

ในสถานพยาบาล “ความพร้อมใช้งาน” ไม่ใช่ความสะดวกสบาย แต่เป็นเรื่องของ “ความปลอดภัยของชีวิตผู้ป่วย” เช่น

- หากระบบ EMR ล่ม แพทย์อาจไม่สามารถเข้าถึงประวัติยาและอาการแพ้ยาได้
- PACS ใช้งานไม่ได้ ทำให้ไม่สามารถดูผล CT Scan ในกรณีฉุกเฉิน
- ระบบห้องฉุกเฉินไม่ทำงาน ทำให้เกิดความล่าช้าในการช่วยชีวิต

เหตุการณ์ที่ Availability ถูกคุกคาม

- การโจมตีแบบ DDoS
- ไฟฟ้าดับและไม่มีระบบสำรอง
- ransomware ล็อกไฟล์ทั้งหมดในระบบ
- ฮาร์ดแวร์ล้มเหลวจากการบำรุงรักษาไม่เพียงพอ

แนวทางควบคุม

- ระบบสำรองไฟฟ้า (UPS, generator)
- ระบบทำงานซ้ำซ้อน (redundancy)

- การสำรองข้อมูล (backup) และแผนกู้คืน (disaster recovery plan)
- เฝ้าระวังระบบแบบเรียลไทม์

สรุปเชิงวิเคราะห์สำหรับผู้สอน

หัวข้อ CIA Triad เป็นแกนกลางของรายวิชานี้ การสอนควรเน้นว่า

- ทั้งสามองค์ประกอบมีความสำคัญเท่าเทียมและสัมพันธ์กัน
- การละเมิดหนึ่งองค์ประกอบอาจส่งผลต่ออีกองค์ประกอบ เช่น ransomware ทำลายทั้ง Confidentiality, Integrity และ Availability พร้อมกัน
- ในระบบสาธารณสุข ความเสี่ยงมีผลโดยตรงต่อชีวิตผู้ป่วย ไม่ใช่เพียงความเสียหายด้านการเงิน

เหมาะสำหรับการใช้ **ตัวอย่างจริง (real cases)** และ **คำถามกระตุ้นคิด (guided questions)** เพื่อช่วยให้ผู้เรียนเข้าใจระดับความสำคัญของ CIA ในโลกจริงของโรงพยาบาล

4. ความสำคัญในภาคสาธารณสุข (Importance in the Healthcare Sector)

การรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพเป็นประเด็นที่สำคัญอย่างยิ่งในระบบสาธารณสุข เนื่องจากข้อมูลสุขภาพมีความละเอียดอ่อนสูง มีความเกี่ยวพันกับสิทธิความเป็นส่วนตัว ชีวิต และความปลอดภัยของผู้ป่วย รวมทั้งเป็นทรัพยากรที่มีคุณค่าสูงต่ออาชญากรไซเบอร์ ส่งผลให้ภาคสาธารณสุขเป็นหนึ่งใน “เป้าหมายหลัก” ของการโจมตีด้านไซเบอร์ทั่วโลก

การละเมิดข้อมูลครั้งหนึ่งไม่เพียงสร้างความเสียหายต่อองค์กร แต่ยังอาจส่งผลกระทบต่อผู้ป่วยเป็นวงกว้าง และรุนแรงกว่าภาคธุรกิจทั่วไป

4.1 ผลกระทบต่อผู้ป่วย (Impact on Patients)

การละเมิดความมั่นคงปลอดภัยข้อมูลสุขภาพส่งผลต่อผู้ป่วยในหลากหลายมิติ ทั้งมิติทางสังคม จิตวิทยา การเงิน และความปลอดภัยในการรักษาพยาบาล

1) ความเสี่ยงต่อการตีตราทางสังคม (Stigmatization)

ข้อมูลเกี่ยวกับโรคหรือภาวะสุขภาพบางอย่าง เช่น HIV โรคติดต่อทางเพศสัมพันธ์ ปัญหาสุขภาพจิต หรือประวัติการใช้สารเสพติด หากถูกเปิดเผยโดยไม่ได้รับอนุญาต อาจทำให้ผู้ป่วยถูกตีตรา ถูกกีดกัน หรือถูกปฏิบัติอย่างไม่เท่าเทียมในสังคม ส่งผลให้ผู้ป่วยหลีกเลี่ยงการรักษาในอนาคตเพราะกลัวข้อมูลรั่วไหล

2) ความเสี่ยงถูกนำข้อมูลไปฉ้อโกง (Fraud and Identity Theft)

อาชญากรไซเบอร์มักใช้ข้อมูลสุขภาพผสมกับข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล วันเกิด หมายเลขบัตรประชาชน เพื่อ

- สวมรอยเบิกค่ารักษา
- เปิดบัญชีธนาคาร
- ทำธุรกรรมการเงิน
- ขายข้อมูลบนตลาดมืด

ข้อมูลสุขภาพจึงมักมีมูลค่าสูงกว่าข้อมูลบัตรเครดิตหลายเท่าในตลาดใต้ดิน

3) ความเสี่ยงต่อความปลอดภัยชีวิต (Patient Safety Risk)

การสูญหายหรือความผิดพลาดของข้อมูลสุขภาพอาจส่งผลโดยตรงต่อการรักษา เช่น

- การแก้ไขข้อมูลยาโดยไม่ได้รับอนุญาต
- ระบบ EMR ใช้งานไม่ได้ในภาวะฉุกเฉิน
- ผลแลบถูกดัดแปลงทำให้แพทย์วินิจฉัยผิด
- ไม่สามารถเข้าถึงประวัติการแพ้ยา

กรณีเช่นนี้อาจส่งผลให้เกิดอันตรายถึงชีวิตของผู้ป่วยได้

4.2 ผลกระทบต่อองค์กร (Impact on Healthcare Organizations)

องค์กรด้านสาธารณสุข เช่น โรงพยาบาลและสถานพยาบาลทุกระดับ ต้องเผชิญความเสี่ยงด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง การโจมตีหรือการละเมิดข้อมูลหนึ่งครั้งอาจทำให้การให้บริการล่มทั้งระบบ

1) การหยุดชะงักของบริการ (Service Disruption)

เมื่อระบบไอทีสำคัญ เช่น EMR, PACS, LIS (Laboratory Information System) หรือระบบคลังข้อมูลถูกโจมตี

- แผนกฉุกเฉินไม่สามารถเข้าถึงข้อมูลผู้ป่วย
- หน่วยรังสีวินิจฉัยไม่สามารถอ่านผลภาพ
- ห้องปฏิบัติการไม่สามารถส่งผลตรวจ
- งานการเงินและประกันไม่สามารถดำเนินการได้

ภาวะนี้ทำให้โรงพยาบาลต้อง “หยุดบริการบางประเภท” หรือแม้กระทั่งปิดระบบทั้งหมดเพื่อควบคุมความเสียหาย

2) ค่าใช้จ่ายในการกู้คืนระบบ (Recovery and Remediation Costs)

การฟื้นฟูระบบหลังการโจมตีมีค่าใช้จ่ายสูงมาก เช่น

- การจ้างผู้เชี่ยวชาญ forensic
- การเปลี่ยนหรือกู้คืนเซิร์ฟเวอร์

- ค่าอุปกรณ์และซอฟต์แวร์เพิ่มเติม
- ค่าปรับตามกฎหมาย PDPA (หากมีความผิด)
- ค่าเสียหายจากการหยุดบริการ

ค่าใช้จ่ายรวมมักสูงกว่าความเสียหายจากภาคธุรกิจทั่วไป เนื่องจากระบบด้านสุขภาพมีความซับซ้อนมาก

3) ความสูญเสียชื่อเสียงและความเชื่อถือ (Reputational Damage)

โรงพยาบาลหรือองค์กรสุขภาพพึ่งพาความไว้วางใจจากประชาชนเป็นหลัก การละเมิดข้อมูลเพียงครั้งเดียวอาจทำให้

- ผู้ป่วยสูญเสียความเชื่อมั่น
- ภาพลักษณ์องค์กรเสียหาย
- อัตราการเข้ารับบริการลดลง
- อาจถูกตั้งคำถามถึงความรับผิดชอบและการกำกับดูแล

ในหลายประเทศ การรั่วไหลของข้อมูลสุขภาพส่งผลให้ผู้บริหารระดับสูงต้องลาออกหรือถูกสอบสวน

4.3 ตัวอย่างเหตุการณ์จริง (Real-world Incidents)

ในช่วงหลายปีที่ผ่านมา การโจมตีด้านความมั่นคงปลอดภัยในภาคสาธารณสุขเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยมีลักษณะร่วมคือ **ส่งผลกระทบทั้ง Confidentiality, Integrity และ Availability**

1) การโจมตีแบบ Ransomware ทำให้ต้องหยุดบริการฉุกเฉิน

โรงพยาบาลหลายแห่งในยุโรปและเอเชียถูกโจมตีจนระบบ EMR และระบบภาพทางการแพทย์ไม่สามารถใช้งานได้ ส่งผลให้

- ไม่สามารถรับผู้ป่วยฉุกเฉิน
- ต้องย้ายผู้ป่วยไปโรงพยาบาลอื่น
- แพทย์ไม่สามารถดูประวัติยาและผลตรวจเก่า

ถือเป็นกรณีที่ Availability ถูกกระทบอย่างรุนแรงและส่งผลต่อความปลอดภัยของผู้ป่วยโดยตรง

2) การล็อกข้อมูลในระบบ PACS

ระบบ PACS (ภาพรังสีวินิจฉัย) เป็นเครื่องมือสำคัญสำหรับแพทย์
หากถูกโจมตีหรือถูกเข้ารหัส

- แพทย์ไม่สามารถดูภาพ CT, MRI, X-ray
- การวินิจฉัยโรคเฉียบพลัน เช่น stroke และ trauma ถูกชะลอ
- อาจเกิดความสูญเสียทางคลินิก

กรณีนี้กระทบทั้ง Availability และ Integrity

3) เจ้าหน้าที่ส่งข้อมูลผู้ป่วยผ่านช่องทางไม่ปลอดภัย

ตัวอย่างที่เกิดขึ้นจริงหลายกรณี เช่น

- ส่งภาพผลตรวจ หรือรายงานผ่านไลน์ส่วนตัว
- ส่งอีเมลที่ไม่มีการเข้ารหัส
- ถ่ายรูปหน้าจอ EMR ส่งให้บุคคลอื่น

กรณีนี้ละเมิด Confidentiality โดยตรง และอาจเป็นสาเหตุให้เกิดการรั่วไหลต่อไปในวงกว้าง

ข้อชี้แนะสำหรับผู้สอน

- สามารถนำกรณีศึกษาจริงมาประกอบ เช่น เหตุการณ์ในสหราชอาณาจักร เยอรมนี หรือไทย
- เน้นให้ผู้เรียนวิเคราะห์ผลกระทบทั้งด้านบุคลากร กระบวนการ และระบบ
- กระตุ้นให้ผู้เรียนเห็นว่าข้อมูลสุขภาพไม่ใช่เพียง “ข้อมูล” แต่เป็น “ฐานสำคัญของการรักษาชีวิตผู้ป่วย”

5. องค์ประกอบของความมั่นคงปลอดภัยสารสนเทศ (Components of Information Security)

ระบบความมั่นคงปลอดภัยสารสนเทศที่ดีต้องประกอบด้วยมาตรการหลายมิติทำงานร่วมกันอย่างบูรณาการ ไม่สามารถพึ่งพาเทคโนโลยีอย่างเดียว หรือเน้นเฉพาะนโยบายองค์กรเพียงด้านเดียว ความปลอดภัยจึงเกิดจากการผสมผสานที่สมดุลระหว่าง **เทคโนโลยี (Technology)**, **กระบวนการ (Process)** และ **บุคลากร (People)**

โมเดลนี้มักถูกเรียกว่า **“Security Triad” หรือ “People-Process-Technology (PPT) Model”** ซึ่งเป็นหลักการพื้นฐานที่ใช้ในโรงพยาบาลทั่วโลก

5.1 มาตรการด้านเทคนิค (Technical Measures)

มาตรการด้านเทคนิคเป็นเครื่องมือและเทคโนโลยีที่ช่วยสร้างเกราะป้องกันระบบสารสนเทศจากภัยคุกคามที่เกิดจากการโจมตี การดักข้อมูล หรือความผิดพลาดของระบบเอง มาตรการเหล่านี้เป็น “ด่านหน้า” ของความมั่นคงปลอดภัย แต่ต้องถูกใช้อย่างถูกต้องเพื่อให้ได้ผลสูงสุด

1) Encryption (การเข้ารหัสข้อมูล)

การเข้ารหัสช่วยป้องกันไม่ให้ข้อมูลถูกอ่านหรือแก้ไขระหว่างเก็บ (data at rest) หรือระหว่างส่งต่อ (data in transit)

ประโยชน์ในโรงพยาบาล

- ป้องกันข้อมูล EMR บนเซิร์ฟเวอร์
- ป้องกันข้อมูลที่ส่งระหว่าง Lab ↔ EMR หรือ PACS ↔ Radiology Workstation
- ลดความเสียหายจากการถูกขโมยอุปกรณ์ เช่น Notebook หรือ External Drive

ตัวอย่างวิธีการเข้ารหัส

- TLS/HTTPS สำหรับการรับส่งข้อมูลบนเครือข่าย
- Disk encryption เช่น BitLocker

2) RBAC (Role-based Access Control)

RBAC เป็นการกำหนดสิทธิการเข้าถึงตาม “บทบาทหน้าที่งาน” เช่น

- แพทย์เข้าถึงข้อมูลผู้ป่วยได้ทุกแผนก
- พยาบาลเข้าถึงข้อมูลเฉพาะผู้ป่วยใน Ward ของตน
- เจ้าหน้าที่เวชระเบียนเข้าถึงเฉพาะข้อมูลประมวลผลเอกสาร

ข้อดี

- ลดความเสี่ยงจาก *insider threat*
- ป้องกันการเข้าถึงโดยไม่จำเป็น (over-privileged access)
- ช่วยในการตรวจสอบย้อนหลัง (audit) ได้ง่าย

3) Intrusion Detection / Prevention Systems (IDS/IPS)

ระบบ IDS/IPS ใช้ตรวจจับ หยุด หรือแจ้งเตือนพฤติกรรมผิดปกติ เช่น

- พยายามเจาะระบบผ่านช่องโหว่
- การสแกนพอร์ต
- การส่งข้อมูลผิดปกติจำนวนมาก
- ความพยายามเข้าถึงบัญชีผู้ใช้ซ้ำ ๆ

บทบาทในโรงพยาบาล

- ป้องกัน ransomware ที่พยายามเข้ารหัสข้อมูลในเซิร์ฟเวอร์
- เฝ้าระวังระบบ PACS ที่มักเป็นเป้าหมายโจมตี
- ตรวจจับพฤติกรรมต้องสงสัยในระบบเครือข่ายภายใน

5.2 มาตรการด้านการบริหารจัดการ (Administrative Measures)

มาตรการด้านนี้เป็นส่วนที่ “กำกับดูแล” ระบบทั้งหมด ซึ่งเป็นรากฐานของการสร้างความปลอดภัยเชิงองค์กร (organizational security) มาตรการทางการบริหารมักถูกละเลย แต่

จริง ๆ แล้วเป็นตัวกำหนดว่าวิธีการป้องกันเชิงเทคนิคควรถูกใช้และดูแลอย่างไร

1) การจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ (Security Policies)

เป็นเอกสารที่กำหนดกฎ กรอบ และแนวทางที่บุคลากรทุกคนต้องปฏิบัติตาม เช่น

- นโยบายการใช้รหัสผ่าน
- นโยบาย BYOD (Bring Your Own Device)
- นโยบายการสำรองข้อมูล
- นโยบายการเข้าถึงข้อมูลผู้ป่วย

นโยบายเหล่านี้ช่วยสร้างมาตรฐานที่สอดคล้องทั่วทั้งองค์กร

2) การประเมินความเสี่ยงเป็นประจำ (Risk Assessment & Management)

โรงพยาบาลมีหลายแผนก หลายระบบ และหลายรูปแบบข้อมูล จึงต้องมีการประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อตรวจสอบว่า

- ระบบไหนเสี่ยงที่สุด
- ช่องโหว่อะไรที่ต้องแก้ไข
- ภัยคุกคามใดมีความเป็นไปได้สูง

ผลลัพธ์ช่วยให้โรงพยาบาลวางแผนงบประมาณด้านความปลอดภัยได้อย่างมีเหตุผล

3) การกำกับดูแลโดยคณะกรรมการด้านข้อมูลสุขภาพ (Data or Health Information Governance Committee)

ในโรงพยาบาลที่มีมาตรฐานสูง มักมีคณะกรรมการข้อมูลสุขภาพทำหน้าที่

- ทบทวนนโยบาย
- อนุมัติสิทธิการเข้าถึงข้อมูล
- ตรวจสอบเหตุการณ์การละเมิดข้อมูล
- กำกับการปฏิบัติตามกฎหมาย เช่น PDPA

บทบาทของคณะกรรมการทำให้การบริหารข้อมูลเป็นระบบและโปร่งใส

5.3 ปัจจัยด้านบุคคล (Human Factors)

แม้จะมีเทคโนโลยีและนโยบายที่ดีเพียงใด แต่ “บุคลากร” คือปัจจัยที่สำคัญและเป็นต้นเหตุของเหตุการณ์ละเมิดข้อมูลส่วนใหญ่ ความผิดพลาดของมนุษย์และพฤติกรรมที่ไม่ปลอดภัยเป็นช่องโหว่สำคัญที่อาชญากรไซเบอร์ใช้โจมตี

1) Social Engineering (การโจมตีโดยใช้มนุษย์เป็นเป้าหมาย)

ผู้โจมตีใช้จิตวิทยาหลอกลวงให้เหยื่อเปิดเผยข้อมูล เช่น

- Phishing อีเมลปลอม

- โทรศัพท์แอบอ้างเป็นฝ่ายไอที
- ล่อให้คลิกลิงก์ติดตั้งมัลแวร์
- ใช้ความเร่งรีบในงานแพทย์ให้เหยื่อไม่ทันระวัง

ในโรงพยาบาล บุคลากรมักยุ่ง ทำให้โอกาสตกเป็นเหยื่อสูง

2) ความผิดพลาดจากการขาดความรู้หรือฝึกอบรม (Lack of Training)

ตัวอย่างเช่น

- ป้อนข้อมูลไม่ถูกต้อง
- ไม่รู้ว่าการส่งข้อมูลผ่าน LINE ส่วนตัวไม่ปลอดภัย
- เข้าใจผิดว่าระบบจะป้องกันทุกอย่างให้โดยอัตโนมัติ

การฝึกอบรมบุคลากรสม่ำเสมอเป็นสิ่งจำเป็นอย่างยิ่ง

3) การใช้รหัสผ่านง่าย ๆ หรือการแชร์รหัสผ่าน (Weak or Shared Credentials)

ปัญหาพบบ่อยในโรงพยาบาล เช่น

- แชร์บัญชีผู้ใช้ในทีมเวร
- ตั้งรหัสผ่าน 123456 หรือชื่อเล่น
- ไม่เปลี่ยนรหัสผ่านตามนโยบาย

ความเสี่ยงนี้ทำให้การตรวจสอบย้อนหลังทำได้ยาก และเปิดช่องให้ผู้โจมตีสวมรอยเข้าถึงข้อมูลได้ง่าย

ข้อสรุปสำคัญเพื่อการสอน

1. **มาตรการด้านเทคนิคเพียงอย่างเดียวไม่เพียงพอ** ต้องมีนโยบายและบุคลากรที่มีความรู้ประกอบ
2. **บุคลากรเป็นจุดอ่อนสำคัญที่สุด** และต้องได้รับการดูแลด้านความรู้ความเข้าใจอย่างต่อเนื่อง
3. **องค์กรที่มี maturity สูง** คือองค์กรที่มีทั้งนโยบาย กระบวนการ เทคโนโลยี และการกำกับดูแลที่ทำงานประสานกัน
4. **ทุกอย่างเชื่อมโยงกับ CIA Triad** ทั้ง Confidentiality, Integrity และ Availability

6. มาตรฐานและกรอบงานสำคัญ (Key Standards and Frameworks)

ในระบบสาธารณสุข การบริหารจัดการความมั่นคงปลอดภัยของข้อมูลไม่สามารถพึ่งพาแนวปฏิบัติภายในองค์กรเพียงอย่างเดียว แต่จำเป็นต้องยึดตามมาตรฐานระดับสากลและกรอบงานที่มีการยอมรับ เพื่อให้การจัดการข้อมูลสุขภาพมีความปลอดภัย สอดคล้องตามกฎหมาย และสามารถเชื่อมต่อระบบกับหน่วยงานอื่นได้อย่างมีประสิทธิภาพ

มาตรฐานเหล่านี้ครอบคลุมทั้งด้านเทคนิค การบริหาร ความเป็นส่วนตัว และมาตรฐานโครงสร้างข้อมูล

6.1 ISO/IEC 27001 – Information Security Management System (ISMS)

ISO/IEC 27001 เป็นมาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศที่ได้รับการยอมรับทั่วโลก โดยเน้นการบริหารจัดการความเสี่ยงอย่างเป็นระบบและต่อเนื่อง เหมาะอย่างยิ่งสำหรับโรงพยาบาลที่ต้องบริหารข้อมูลจำนวนมาก ผู้ใช้งานหลายบทบาท และระบบซอฟต์แวร์ที่หลากหลาย

ประเด็นสำคัญของ ISO/IEC 27001

- ใช้หลักการ **Risk-based Approach** ในการกำหนดมาตรการควบคุม
- มี **Annex A Controls** 93 ข้อ (เวอร์ชัน 2022) ครอบคลุมการบริหาร ความเป็นส่วนตัว และเทคโนโลยี
- เน้นการทำงานแบบ **PDCA (Plan-Do-Check-Act)** เพื่อปรับปรุงอย่างต่อเนื่อง

ความสำคัญต่อองค์กรด้านสุขภาพ

- ช่วยให้โรงพยาบาลจัดการข้อมูลสุขภาพได้เป็นระบบ
- ลดช่องโหว่จากความซับซ้อนของระบบหลายแผนก
- ช่วยเตรียมความพร้อมต่อการตรวจสอบด้านกฎหมาย เช่น PDPA
- เป็นองค์ประกอบสำคัญในการรับรองคุณภาพโรงพยาบาลระดับสากล

หัวข้อที่มักเน้นในการสอน

- ความแตกต่างระหว่างมาตรฐานกับเทคโนโลยี
- การประเมินความเสี่ยง (Risk Assessment)
- การบันทึกหลักฐานด้านความปลอดภัย (Audit Trails)

6.2 NIST Cybersecurity Framework (NIST CSF)

NIST CSF เป็นกรอบงานด้านความมั่นคงปลอดภัยที่พัฒนาโดย National Institute of Standards and Technology (สหรัฐอเมริกา) และถูกใช้ในทั้งภาครัฐและเอกชนอย่างแพร่หลาย รวมถึงโรงพยาบาลในหลายประเทศ

มีโครงสร้างหลัก 5 ฟังก์ชัน ได้แก่:

1) Identify

ระบุสินทรัพย์ ข้อมูล ความเสี่ยง และความสำคัญของระบบ
→ ใช้กำหนดลำดับความสำคัญในการป้องกัน

2) Protect

ติดตั้งมาตรการป้องกัน เช่น การเข้ารหัส การตั้งค่าสิทธิการเข้าถึง การฝึกอบรมบุคลากร
→ เพื่อลดโอกาสการเกิดเหตุการณ์

3) Detect

มุ่งเน้นระบบการเฝ้าระวัง แจ้งเตือน และตรวจจับเหตุผิดปกติ
→ เช่น IDS/IPS, SIEM

4) Respond

การรับมือเมื่อเกิดเหตุ เช่น การสื่อสาร การควบคุมเหตุการณ์
→ รวมถึง Incident Response Plan

5) Recover

การฟื้นฟูระบบให้กลับมาทำงานตามปกติ
→ เช่น แผน DRP (Disaster Recovery Plan)

ความสำคัญต่อภาคสาธารณสุข

- เหมาะสำหรับโรงพยาบาลที่ต้องการ framework ที่เข้าใจง่าย
- ช่วยจัดลำดับมาตรการด้านความมั่นคงปลอดภัย
- ใช้ร่วมกับ ISO/IEC 27001 ได้

6.3 HIPAA และ PDPA – กฎหมายที่เกี่ยวข้องกับข้อมูลสุขภาพ

HIPAA (Health Insurance Portability and Accountability Act – USA)

เป็นกฎหมายกลางของสหรัฐอเมริกาที่เน้นการคุ้มครองข้อมูลสุขภาพของผู้ป่วย (Protected Health Information – PHI)

องค์ประกอบหลักของ HIPAA

- **Privacy Rule**: ควบคุมการใช้และเปิดเผยข้อมูลสุขภาพ
- **Security Rule**: กำหนดมาตรการด้านเทคนิค การบริหาร และกายภาพ
- **Breach Notification Rule**: กำหนดให้แจ้งเหตุเมื่อเกิดการรั่วไหล

ความสำคัญต่อการเรียนการสอน

- เป็นต้นแบบของกฎหมายคุ้มครองข้อมูลสุขภาพในหลายประเทศ
- ยกตัวอย่างชัดเจนเรื่องบทลงโทษและความรับผิดชอบ
- มีมาตรฐานการเก็บข้อมูลบนระบบ EMR ที่ชัดเจน

PDPA (Personal Data Protection Act – Thailand)

เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย ครอบคลุมถึง **ข้อมูลอ่อนไหว (Sensitive Personal Data)** ซึ่งรวม “ข้อมูลสุขภาพ” โดยตรง

สิ่งที่องค์กรสุขภาพต้องคำนึงถึง

- ต้องมีฐานทางกฎหมายในการเก็บและใช้ข้อมูล เช่น
    - เพื่อการรักษาพยาบาล
    - เพื่อประโยชน์สาธารณะ
    - ตามความจำเป็นทางการแพทย์
- ต้องมีมาตรการรักษาความปลอดภัยที่เพียงพอ (Security Measures)
- ต้องแจ้งเหตุรั่วไหลภายในระยะเวลาที่กฎหมายกำหนด
- ต้องจัดทำบันทึกกิจกรรมการประมวลผล (Record of Processing Activities)

ความสำคัญในทางปฏิบัติ

- ส่งผลโดยตรงต่อทุกแผนกในโรงพยาบาล
- มีผลต่อการออกแบบเวิร์กโฟลว์ของ EMR
- ใช้เป็นกรอบกำหนดนโยบายข้อมูลผู้ป่วยในองค์กร

6.4 HL7 และ FHIR – มาตรฐานการแลกเปลี่ยนข้อมูลสุขภาพ

ระบบสุขภาพในโรงพยาบาลมักแยกเป็นหลายระบบ เช่น EMR, LIS, RIS, PACS การแลกเปลี่ยนข้อมูลระหว่างระบบจึงจำเป็นต้องมีมาตรฐานกลางเพื่อประกัน **ความถูกต้อง ความสอดคล้อง และความปลอดภัย**

HL7 (Health Level Seven)

เป็นชุดมาตรฐานสำหรับการแลกเปลี่ยนข้อมูลทางการแพทย์ เช่น

- ข้อมูลผลแลบ
- ข้อมูลประชากรผู้ป่วย
- ข้อความระหว่างระบบ

HL7 เวอร์ชัน 2.x ยังเป็นเวอร์ชันที่ใช้มากที่สุดในโรงพยาบาลทั่วโลก

FHIR (Fast Healthcare Interoperability Resources)

เป็นมาตรฐานยุคใหม่ที่ยืดหยุ่นกว่า HL7 V2/V3 ใช้แนวคิด **API** และ **RESTful Services** ทำให้สามารถ

- เชื่อมต่อระบบผ่านอินเทอร์เน็ต
- ทำงานร่วมกับ Mobile Health Apps
- ลดความซับซ้อนของระบบแลกเปลี่ยนข้อมูล

FHIR มักถูกใช้ในการพัฒนา Telemedicine, Health Applications และระบบข้อมูลสุขภาพยุคใหม่

สรุปสำหรับผู้สอน

- **ISO 27001**: เน้นด้านการบริหารความเสี่ยงและระบบการจัดการ
- **NIST CSF**: เน้นขั้นตอนปฏิบัติและการตอบสนองต่อภัย
- **HIPAA/PDPA**: เป็นกฎหมายที่เน้นความเป็นส่วนตัวและภาระหน้าที่ต่อองค์กร
- **HL7/FHIR**: เป็นมาตรฐานที่ทำให้ข้อมูลสุขภาพแลกเปลี่ยนได้อย่างถูกต้องและปลอดภัย

ผู้สอนสามารถนำ framework เหล่านี้ไปใช้เปรียบเทียบเพื่อให้ผู้เรียนเข้าใจว่าแต่ละมาตรฐานตอบโจทย์คนละมิติของความมั่นคงปลอดภัยในระบบสาธารณสุข

7. คุณลักษณะเฉพาะของข้อมูลสุขภาพ (Unique Characteristics of Health Data)

ข้อมูลสุขภาพ (Health Data) มีลักษณะเฉพาะที่แตกต่างจากข้อมูลประเภทอื่น เช่น ข้อมูลธุรกิจ การเงิน หรือข้อมูลส่วนบุคคลทั่วไป ความพิเศษของข้อมูลสุขภาพทำให้ต้องใช้มาตรการด้านความมั่นคงปลอดภัยที่รัดกุมกว่า เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับผู้ป่วยและองค์กรสาธารณสุข

1) ข้อมูลมีความอ่อนไหวสูง (Highly Sensitive Data)

ข้อมูลสุขภาพสะท้อนถึงสภาพร่างกาย จิตใจ พฤติกรรม และประวัติทางการแพทย์ของบุคคล เช่น

- โรคเรื้อรัง เช่น เบาหวาน ความดัน
- โรคที่มีการตีตราทางสังคม เช่น HIV โรคจิตเวช
- ประวัติการรักษาที่อาจถูกนำไปใช้เพื่อประโยชน์ทางธุรกิจหรือการเลือกปฏิบัติ

เหตุผลที่ต้องได้รับการปกป้องเข้มงวด:

- มีความเสี่ยงสูงต่อการถูกนำไปใช้ในทางมิชอบ
- อาจก่อให้เกิดความอับอาย ความเครียด หรือผลกระทบต่ออาชีพและความสัมพันธ์
- กฎหมาย PDPA จัดให้เป็น “ข้อมูลอ่อนไหว (Sensitive Personal Data)” ที่ต้องดูแลเป็นพิเศษ

2) การใช้งานยาวนานต่อเนื่อง (Long-term Continuity)

ข้อมูลสุขภาพต้องถูกจัดเก็บและใช้งานต่อเนื่องในระยะยาว เช่น:

- ประวัติการรักษาผู้ป่วยเรื้อรังที่ติดตามต่อเนื่องหลายปี
- ข้อมูลวัคซีน การผ่าตัด หรืออาการแพ้ยา ซึ่งต้องเข้าถึงได้ตลอดชีวิต
- ใช้ในการวางแผนรักษาหรือเฝ้าระวังด้านสาธารณสุข

ผลกระทบด้านความปลอดภัยที่เกี่ยวข้อง:

- ระบบจัดเก็บต้องมีเสถียรภาพ มีการสำรองข้อมูล และสามารถกู้คืนได้
- ข้อมูลเก่าก็ยังเป็นเป้าหมายของผู้โจมตี เพราะนำไปเชื่อมโยงอัตลักษณ์ของบุคคลได้

3) มีหลายรูปแบบ (Multi-format / Multi-modal Data)

ข้อมูลสุขภาพไม่ได้มีลักษณะเป็นข้อความธรรมดาเท่านั้น แต่ประกอบด้วยหลายรูปแบบ ได้แก่:

- **ข้อความ:** clinical notes, summary, SOAP notes
- **ตัวเลข:** vital signs, lab results
- **ภาพ:** X-ray, CT, MRI, Ultrasound
- **สัญญาณชีพ:** ECG, EEG, continuous monitoring
- **ข้อมูลเชิงเวลา (time-series)** เช่น การเฝ้าระวังสัญญาณชีพของ ICU

ผลต่อความมั่นคงปลอดภัย:

- จำเป็นต้องมีมาตรการปกป้องที่แตกต่างกันในแต่ละประเภท
- ข้อมูลภาพใน PACS มีปริมาณใหญ่ ต้องมีวิธีป้องกันและเข้ารหัสที่เหมาะสม
- ระบบที่รองรับข้อมูลหลายรูปแบบมีความเสี่ยงเพิ่มขึ้นโดยธรรมชาติ

4) ใช้ร่วมกันหลายแผนก (Interdepartmental Use)

ข้อมูลหนึ่งชุดของผู้ป่วยถูกใช้ร่วมกันในหลายหน่วยงาน เช่น

- แพทย์ผู้ตรวจ
- พยาบาล
- ห้องปฏิบัติการ
- รังสีวินิจฉัย
- เวชระเบียน
- การเงินและประกัน
- เครือข่ายบริการสุขภาพระดับจังหวัดหรือประเทศ

ผลกระทบด้านความมั่นคงปลอดภัย:

- ต้องมีระบบกำหนดสิทธิที่ละเอียด (granular access control)
- ยิ่งมีการแลกเปลี่ยนข้อมูลมาก ความเสี่ยงในการรั่วไหลยิ่งเพิ่ม
- ต้องมีมาตรฐานการแลกเปลี่ยนข้อมูล เช่น HL7 หรือ FHIR
- โอกาสเกิด human error สูงขึ้น เช่น การส่งข้อมูลผิดแผนกหรือผิดบุคคล

8. กระบวนการไหลของข้อมูลสุขภาพ (Health Data Flow)

Lecture Note – Expanded

ข้อมูลสุขภาพมีชีวิต (data lifecycle) ตั้งแต่เริ่มเก็บข้อมูล การวิเคราะห์ การใช้วินิจฉัย และการถูกส่งต่อไปยังระบบต่าง ๆ การเข้าใจเส้นทางของข้อมูล (data flow) ช่วยให้นักศึกษาและผู้ปฏิบัติงานสามารถระบุจุดเสี่ยง (vulnerabilities) และออกแบบมาตรการป้องกันที่เหมาะสม

1) ผู้ป่วย (Patient)

กระบวนการเริ่มต้นเมื่อผู้ป่วยเข้ารับบริการในระบบสุขภาพ เป็นจุดเริ่มต้นของการรวบรวมข้อมูล เช่น ประวัติส่วนตัว อาการสำคัญ ประวัติการแพ้ยา การตรวจร่างกาย

ความเสี่ยง:

- การเก็บข้อมูลบนแบบฟอร์มกระดาษโดยไม่ได้ล็อก
- การยืนยันตัวบุคคลผิดพลาด

2) ห้องตรวจ (OPD/ER)

ข้อมูลถูกบันทึกโดยแพทย์หรือพยาบาล เช่น อาการป่วย ผลตรวจเบื้องต้น การสั่งยาและการส่งตรวจ

ความเสี่ยง:

- การเปิดหน้าจอคอมพิวเตอร์ไว้โดยไม่ล็อก
- ผู้อื่นแอบดูข้อมูลบนหน้าจอ (shoulder surfing)
- การเข้าถึง EMR ด้วยบัญชีที่แชร์

3) บันทึกลง EMR/EHR

ระบบ EMR คือที่จัดเก็บประวัติผู้ป่วยทั้งหมด ข้อมูลที่ถูกบันทึกในระบบนี้จะถูกใช้ตลอดเส้นทางการรักษา

ความเสี่ยง:

- การโจมตีระบบฐานข้อมูล
- การขโมยรหัสผ่าน
- การเข้าถึงโดยเจ้าหน้าที่ที่ไม่มีส่วนเกี่ยวข้อง

4) ส่งต่อข้อมูลไปยัง Lab หรือ Radiology

ห้องปฏิบัติการและหน่วยรังสีวินิจฉัยจะได้รับคำสั่งตรวจ (orders) จากแพทย์และส่งผลกลับผ่านระบบเชื่อมต่อ (LIS, RIS, PACS)

ความเสี่ยง:

- การส่งข้อมูลผ่านระบบเครือข่ายที่ไม่เข้ารหัส
- ช่องโหว่ในระบบเก่า (legacy systems)
- การดักข้อมูล (interception) ในเส้นทางเครือข่าย

5) ส่งผลกลับสู่แพทย์ (Result Reporting)

ผลตรวจทั้งหมดถูกส่งกลับให้แพทย์ตัดสินใจรักษา

ความเสี่ยง:

- ผลแลบผิดพลาดหรือถูกแก้ไข
- การหน่วงเวลาของระบบ ทำให้การรักษาล่าช้า
- การแสดงข้อมูลผิดผู้ป่วย

6) การวินิจฉัยและการรักษา

แพทย์ใช้ข้อมูลทั้งหมดประกอบการตัดสินใจ การสั่งยา การทำหัตถการ หรือการรับผู้ป่วยเข้ารักษาในโรงพยาบาล

ความเสี่ยง:

- หากข้อมูลไม่ครบถ้วน อาจทำให้วินิจฉัยผิด
- การเข้าถึงข้อมูลไม่ได้ (system downtime) ส่งผลต่อความปลอดภัยผู้ป่วย

7) ระบบการเงิน/ประกัน (Billing/Insurance)

ใช้ข้อมูลการรักษาเพื่อคำนวณค่ารักษา ส่งเคลมประกัน หรือบันทึกข้อมูลตามกฎหมาย

ความเสี่ยง:

- การส่งข้อมูลการรักษาไปยังภายนอก เช่น บริษัทประกัน โดยไม่มีความปลอดภัยที่เพียงพอ
- ข้อมูลผู้ป่วยถูกนำไปฉ้อโกงหรือปลอมแปลงใบเคลม

8) ระบบข้อมูลระดับเครือข่าย (Health Information Exchange)

ข้อมูลอาจถูกส่งไปยังหน่วยงานระดับเขต จังหวัด หรือประเทศ เช่น เพื่อการรายงานโรคเฝ้าระวัง (Surveillance)

ความเสี่ยง:

- ความเสี่ยงจากการเชื่อมโยงระบบหลายแห่ง
- มาตรฐานความปลอดภัยไม่เท่าเทียมกัน
- การรั่วไหลระหว่างองค์กร (inter-organizational leakage)

สรุปการประเมินความเสี่ยงใน Health Data Flow

ทุกขั้นตอนของการไหลของข้อมูลมีความเสี่ยง โดยเฉพาะ:

- ช่องโหว่ของการเชื่อมต่อระหว่างระบบ
- ความผิดพลาดของบุคลากร
- อุปกรณ์ที่ไม่เข้ารหัส
- ระบบเก่าที่ไม่ได้รับการอัปเดต
- การกำหนดสิทธิการเข้าถึงไม่เหมาะสม

ผู้สอนสามารถใช้ flow นี้ในการกระตุ้นให้ผู้เรียนระบุ “vulnerable points” ด้วยตนเองเพื่อฝึกการวิเคราะห์ความเสี่ยงในโรงพยาบาลจริงได้อย่างมีประสิทธิภาพ