

การศึกษากรอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 สำหรับการจัดการระบบสำรองข้อมูลของโรงพยาบาล

ไพศัลป์ชัย ไชยพรเดชเจริญ* และ สมชัย บุรีรักษ์

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล เขตบางกอกน้อย กรุงเทพมหานคร 10700

*อีเมลของผู้ประพันธ์บทความ: paisinchai.cha@mahidol.ac.th

บทคัดย่อ

ข้อมูลสารสนเทศทางการแพทย์เป็นสินทรัพย์ที่สำคัญอย่างยิ่งของโรงพยาบาล แต่ในปัจจุบันภัยคุกคามทางไซเบอร์โดยเฉพาะแรนซัมแวร์ได้ทวีความรุนแรงมากขึ้น การจัดให้มีระบบสำรองข้อมูลที่มีประสิทธิภาพและเป็นไปตามมาตรฐานสากล จึงมีความจำเป็นอย่างยิ่งที่ต้องดำเนินการโดยเร็ว บทความนี้มีวัตถุประสงค์เพื่อศึกษากรอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 สำหรับการจัดการระบบสำรองข้อมูลของโรงพยาบาล โดยมุ่งเน้นการวิเคราะห์ข้อกำหนดที่เกี่ยวข้องในภาคผนวก A และสังเคราะห์เป็นกรอบแนวทางเชิงปฏิบัติผ่านวงจรคุณภาพ PDCA เพื่อใช้เป็นต้นแบบในการจัดการข้อมูลสำรองให้มีความมั่นคงปลอดภัยและสอดคล้องกับข้อกำหนดคุ้มครองข้อมูลส่วนบุคคล ผลที่คาดว่าจะได้รับคือ โรงพยาบาลจะมีกระบวนการจัดการข้อมูลสำรองอย่างเป็นระบบที่รัดกุม ปลอดภัย สามารถลดความเสี่ยงจากภัยคุกคาม และสอดคล้องกับข้อกำหนดคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะช่วยยกระดับความมั่นคงปลอดภัยขององค์กรได้อย่างยั่งยืน

คำสำคัญ: ISO/IEC 27001; ความมั่นคงปลอดภัยสารสนเทศ; การสำรองข้อมูล; การบริหารจัดการข้อมูล; การบริการสุขภาพ

A Study of the ISO/IEC 27001:2022-Based Framework for Hospital Data Backup System Management

Paisinchai Chaiyaprondetcharoen* and Somchai Burirak

Faculty of Medicine Siriraj Hospital, Mahidol University, Bangkok Noi, Bangkok 10700, Thailand

*Corresponding author's e-mail: paisinchai.cha@mahidol.ac.th

Abstract

Medical information is a critical asset for hospitals. However, as cyber threats, especially ransomware, intensify, an effective data backup system aligned with international standards has become an urgent necessity. This article aims to study the ISO/IEC 27001:2022 framework for hospital data backup management. It focuses on analyzing the relevant requirements in Appendix A and synthesizing them into a practical framework using the PDCA quality cycle. This framework serves as a model for data backup management to ensure security and compliance with personal data protection laws. The expected outcome is that hospitals will establish a robust and secure backup management process, mitigating risks from threats and ensuring compliance with personal data protection laws, thereby sustainably enhancing the organization's security posture.

Keywords: ISO/IEC 27001; Information Security; Data Backup; Data Management; Healthcare

บทนำ

ข้อมูลทางการแพทย์ถือเป็นทรัพยากรที่มีความสำคัญอย่างยิ่งต่อการดำเนินงานของโรงพยาบาล ทั้งในมิติของการให้บริการรักษาพยาบาล การวิจัยและพัฒนาทางการแพทย์ ตลอดจนการบริหารจัดการองค์กรอย่างมีประสิทธิภาพ ความถูกต้องครบถ้วน รวมถึงความพร้อมในการเข้าถึงและใช้งานข้อมูลผู้ป่วย จึงถือเป็นปัจจัยส่งผลโดยตรงต่อคุณภาพการให้บริการด้านสุขภาพ (ฝ่ายสารสนเทศ, 2560) อย่างไรก็ตามข้อมูลดังกล่าวมีความเสี่ยงสูงต่อการสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต หรือการโจมตีทางไซเบอร์ ซึ่งอาจก่อให้เกิดผลกระทบต่อทั้งผู้ป่วยและองค์กร (สำนักงานคณะกรรมการการรักษามั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567)

ระบบสำรองข้อมูล (Data Backup System) จึงมีบทบาทสำคัญในการรักษาความต่อเนื่องทางธุรกิจ (Business Continuity) และความมั่นคงปลอดภัยของสารสนเทศ โดยเฉพาะในสถาบันทางการแพทย์ที่มีข้อมูลจำนวนมากและมีความอ่อนไหวสูง การจัดการระบบสำรองข้อมูลที่มีประสิทธิภาพไม่เพียงช่วยลดความเสี่ยงจากการสูญหายของข้อมูล แต่ยังช่วยสนับสนุนการกู้คืนระบบ (Disaster Recovery) ได้อย่างทันท่วงที (Soraya et al., 2025)

ในบริบทนี้ มาตรฐาน ISO/IEC 27001:2022 ได้รับการยอมรับในระดับสากลว่าเป็นกรอบแนวทางสำหรับการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ที่มีความครอบคลุม ทั้งในด้านการประเมินความเสี่ยง การกำหนดนโยบาย และการควบคุมเชิงเทคนิค (International Organization for Standardization, 2022) มาตรฐานดังกล่าวสามารถนำมาศึกษาและสังเคราะห์ใช้เพื่อยกระดับระบบสำรองข้อมูลของโรงพยาบาลให้มีประสิทธิภาพ โปร่งใส และตรวจสอบได้ ซึ่งเป็นรากฐานสำคัญในการสร้างความเชื่อมั่นให้แก่ผู้ป่วยและผู้มีส่วนเกี่ยวข้องกับองค์กร (Wibawa et al., 2024)



ภาพที่ 1 องค์ประกอบหลักของความมั่นคงปลอดภัย (CIA Triad)

ที่มา: สร้างด้วย Gemini [Google] โดยผู้เขียน เมื่อวันที่ 6 กันยายน 2025

ความหมายและความเป็นมาของมาตรฐาน ISO/IEC 27001:2022

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ซึ่งได้รับการยอมรับอย่างกว้างขวางทั่วโลก มาตรฐานนี้ไม่ได้มุ่งเน้นที่เทคโนโลยีใดเทคโนโลยีหนึ่งโดยเฉพาะ แต่เป็นกรอบการทำงาน (Framework) เชิงกระบวนการที่ช่วยให้องค์กรสามารถระบุ จัดการ และลดความเสี่ยงที่เกี่ยวข้องกับข้อมูลสารสนเทศได้อย่างเป็นระบบ หัวใจสำคัญของมาตรฐานนี้คือการสร้างแนวทางปฏิบัติที่ครอบคลุม 3 องค์ประกอบหลักของความมั่นคงปลอดภัย ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) หรือที่รู้จักกันในชื่อ “CIA Triad” (Malatji, 2023) ดังภาพที่ 1

มาตรฐานนี้ได้รับการพัฒนาและเผยแพร่โดยความร่วมมือขององค์การระหว่างประเทศว่าด้วยมาตรฐาน (International Organization for Standardization: ISO) และคณะกรรมการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์ (International Electrotechnical Commission: IEC) โดยมีรากฐานมาจากมาตรฐาน BS7799 ของสหราชอาณาจักร (United Kingdom) ซึ่งเผยแพร่ครั้งแรกในปี 1995 ก่อนจะถูกนำมาพัฒนาเป็นมาตรฐานสากลฉบับแรก ในชื่อ ISO/IEC 27001:2005 และมีการปรับปรุงครั้งสำคัญในปี 2013

สำหรับเวอร์ชันล่าสุดคือ ISO/IEC 27001:2022 ซึ่งเผยแพร่เมื่อวันที่ 25 ตุลาคม 2022 เป็นการปรับปรุงเพื่อให้ทันต่อภูมิทัศน์ของภัยคุกคามทางไซเบอร์และเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เช่น การทำงานบนคลาวด์ (Cloud Computing) และการทำงานจากทางไกล (Remote Work) การเปลี่ยนแปลงที่สำคัญในเวอร์ชันนี้คือการปรับโครงสร้างและลดจำนวนข้อกำหนดด้านการควบคุม (Controls) ในภาคผนวก A (Annex A) จาก 114 ข้อเหลือ 93 ข้อ และจัดกลุ่มใหม่เป็น 4 หมวดหมู่ ได้แก่ ด้านองค์กร (Organizational) ด้านบุคลากร (People) ด้านกายภาพ (Physical) และด้านเทคโนโลยี (Technological) เพื่อให้มีความกระชับและสอดคล้องกับยุคปัจจุบันมากขึ้น (Brezavšček & Vidmar, 2023)

ในประเทศไทย หน่วยงานภาครัฐและเอกชน โดยเฉพาะกลุ่มอุตสาหกรรมที่ต้องมีการจัดการข้อมูลที่สำคัญและอ่อนไหว เช่น สถาบันการเงินและโรงพยาบาลต่างให้ความสำคัญกับการนำมาตรฐานนี้มาศึกษาและประยุกต์ใช้เพื่อสร้างความน่าเชื่อถือและยกระดับการป้องกันข้อมูลให้สอดคล้องกับกฎหมายภายในประเทศ เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567) การมี ISMS ที่ได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 จึงเปรียบเสมือนเครื่องยืนยันว่าองค์กรมีกระบวนการจัดการความเสี่ยงด้านสารสนเทศที่เป็นระบบและเป็นไปตามมาตรฐานสากล

มาตรฐาน ISO/IEC 27001:2022 เกี่ยวข้องกับการสำรองข้อมูลอย่างไร

แม้ว่ามาตรฐาน ISO/IEC 27001:2022 จะเป็นกรอบการทำงานสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) แต่ก็มีข้อกำหนดด้านการควบคุม (Controls) ในภาคผนวก A (Annex A) หลายข้อที่มีความเกี่ยวข้องโดยตรงและโดยอ้อมกับการสำรองข้อมูลอย่างมีนัยสำคัญ มาตรฐานไม่ได้ระบุว่าต้องใช้เทคโนโลยีใด แต่กำหนดสิ่งที่ต้องมี เพื่อให้มั่นใจว่าข้อมูลจะได้รับการปกป้องและพร้อมใช้งานอยู่เสมอ

ข้อกำหนดที่เกี่ยวข้องโดยตรงที่สุดคือ A.8.13 Information Backup ซึ่งถือเป็นข้อกำหนดสำคัญยิ่ง โดยระบุว่า “ควรมีการสร้างและทดสอบการสำรองข้อมูล ซอฟต์แวร์ และระบบ ให้อยู่ในขอบเขตของนโยบายการสำรองข้อมูล” (International Organization for Standardization, 2022) การปฏิบัติตามข้อกำหนดนี้หมายความว่าโรงพยาบาลควรมีการดำเนินการดังนี้

1. นโยบายการสำรองข้อมูล (Backup Policy) ต้องมีเอกสารนโยบายอย่างชัดเจน กำหนดขอบเขต ความสำเร็จ วิธีการจัดเก็บ และระยะเวลาการเก็บรักษาข้อมูลสำรอง (Retention Period) อย่างครบถ้วนและเป็นระบบ
 2. กำหนด RPO และ RTO ต้องมีการกำหนดวัตถุประสงค์ของจุดที่ต้องการกู้คืน (Recovery Point Objective) และระยะเวลาที่ต้องการกู้คืน (Recovery Time Objective)
 3. ทดสอบการกู้คืน ต้องมีการทดสอบกระบวนการกู้คืนข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถนำกลับมาใช้งานได้จริงในกรณีเกิดเหตุการณ์ฉุกเฉินหรือไม่คาดคิด
- นอกจากนี้ ยังมีข้อกำหนดอื่น ๆ ที่สนับสนุนและสร้างความแข็งแกร่งให้กับกระบวนการสำรองข้อมูลอีกด้วย ได้แก่

ด้านการวางแผนและนโยบาย (Planning & Governance)

1. A.8.32 Change Management การบริหารจัดการการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อกระบวนการสำรองข้อมูล เช่น การอัปเดตระบบ การเปลี่ยนสถาปัตยกรรมเครือข่าย หรือการเปลี่ยนซอฟต์แวร์สำรองข้อมูล ข้อกำหนดนี้ช่วยลดความเสี่ยงจากความผิดพลาดทางเทคนิคที่อาจทำให้การสำรองหรือการกู้คืนข้อมูลล้มเหลว
2. A.5.30 ICT Readiness for Business Continuity ข้อกำหนดนี้เน้นการเตรียมความพร้อมของเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อความต่อเนื่องทางธุรกิจ ระบบสำรองข้อมูลถือเป็นองค์ประกอบหลักที่จะช่วยให้โรงพยาบาลสามารถกลับมาให้บริการได้อย่างรวดเร็วที่สุดหลังเกิดเหตุการณ์หยุดชะงัก (Tistiyan et al., 2023)

ด้านการปฏิบัติการและเทคนิค (Operational & Technical Implementation)

1. A.8.6 Capacity Management การบริหารจัดการความจุของระบบจัดเก็บข้อมูล เพื่อให้แน่ใจว่ามีพื้นที่เพียงพอสำหรับทั้งข้อมูลที่ใช้งานจริงและข้อมูลที่สำรองไว้
2. A.8.14 Information Redundancy แนะนำให้มีการทำซ้ำข้อมูล (Redundancy) ของระบบสารสนเทศที่สำคัญ เพื่อให้มีความพร้อมใช้งาน ป้องกันความล้มเหลว ณ จุดใดจุดหนึ่งของระบบ (Single Point of Failure) ซึ่งทำงานควบคู่ไปกับการสำรองข้อมูล
3. A.8.23 Information Security for Use of Cloud Services การรักษาความมั่นคงปลอดภัยของข้อมูลสำรองเมื่อมีการใช้บริการคลาวด์ (Cloud Backup) ข้อกำหนดนี้กำหนดให้ต้องมีการทำสัญญาและข้อตกลงด้านความปลอดภัยกับผู้ให้บริการคลาวด์อย่างชัดเจน รวมถึงการเข้ารหัสข้อมูล (Encryption) และการตรวจสอบสิทธิ์ของผู้เข้าถึงข้อมูล เพื่อให้มั่นใจว่าข้อมูลสำรองบนคลาวด์ได้รับการปกป้องเทียบเท่ากับข้อมูลที่เก็บภายในองค์กร

ด้านการควบคุมและการป้องกันภัยคุกคาม (Security Controls & Protection)

1. A.5.15 Access Control การควบคุมการเข้าถึงข้อมูลสำรอง โดยกำหนดสิทธิ์เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นในการเข้าถึงไฟล์หรือสื่อจัดเก็บข้อมูล พร้อมใช้กลไกการยืนยันตัวตน (Authentication) และการอนุญาตสิทธิ์ (Authorization) ตามหลัก “Least Privilege Principle” เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
2. A.5.14 Information Transfer กำหนดให้มีมาตรการป้องกันข้อมูลระหว่างการส่งผ่าน เช่น การเข้ารหัสข้อมูล (Encryption) ขณะส่งข้อมูลไปยังที่จัดเก็บข้อมูลสำรอง ไม่ว่าจะอยู่ในองค์กร (On-premise) หรือบนคลาวด์ (Cloud) เพื่อป้องกันการดักจับข้อมูล
3. A.8.8 Management of Technical Vulnerabilities การจัดการช่องโหว่ทางเทคนิคที่อาจกระทบต่อข้อมูลสำรอง เช่น การอัปเดตแพตช์ความปลอดภัย (Security Patch) การตรวจสอบช่องโหว่ในซอฟต์แวร์สำรอง

ข้อมูล หรือระบบจัดเก็บข้อมูล เพื่อป้องกันการโจมตีจากมัลแวร์ (Malware) หรือแรนซัมแวร์ (Ransomware) ที่มุ่งเป้าข้อมูลสำรอง (International Organization for Standardization, 2022)

ดังนั้น ISO/IEC 27001:2022 จึงไม่ได้มองว่าการสำรองข้อมูลเป็นเพียงกระบวนการทางเทคนิค แต่เป็นส่วนหนึ่งของกระบวนการบริหารจัดการความเสี่ยงและความต่อเนื่องทางธุรกิจที่ต้องมีการวางแผน ปฏิบัติ ตรวจสอบ และปรับปรุง (PDCA Cycle) อย่างเป็นระบบ เพื่อให้มั่นใจว่าข้อมูลสำคัญของโรงพยาบาลจะพร้อมใช้งานและปลอดภัยอยู่เสมอ

แนวทางการศึกษาตามมาตรฐานในการจัดการระบบสำรองข้อมูลของโรงพยาบาล

การศึกษารอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 ในการจัดการระบบสำรองข้อมูล จำเป็นต้องดำเนินการภายใต้กระบวนการที่มีโครงสร้างและเป็นระบบ โดยอาศัยวงจรการบริหารคุณภาพ PDCA (Plan Do Check Act) ซึ่งถือเป็นกลไกสำคัญของมาตรฐานสากลในทุกฉบับ วงจรดังกล่าวมีบทบาทในการสร้างความมั่นใจว่ากระบวนการด้านความมั่นคงปลอดภัยสารสนเทศสามารถถูกวางแผน ดำเนินการ ตรวจสอบ และปรับปรุงได้อย่างต่อเนื่อง อันจะส่งผลให้ระบบสำรองข้อมูลขององค์กรมีประสิทธิภาพ สามารถตอบสนองต่อความเสี่ยงที่เปลี่ยนแปลงได้ และสนับสนุนเป้าหมายด้านความต่อเนื่องทางธุรกิจอย่างยั่งยืน



ภาพที่ 2 วงจรคุณภาพ PDCA

ที่มา: สร้างด้วย Gemini [Google] โดยผู้เขียน เมื่อวันที่ 10 กันยายน 2025

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ตระหนักถึงความสำคัญของข้อมูลผู้ป่วยซึ่งเป็นปัจจัยหลักในการให้บริการรักษาพยาบาล จึงได้จัดทำโครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(Information Security Management System: ISMS) เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 และได้รับการรับรองมาตรฐานดังกล่าวเมื่อวันที่ 28 เมษายน 2560 (ฝ่ายสารสนเทศ, 2560) ปัจจุบัน คณะฯ อยู่ระหว่างการเตรียมความพร้อมเพื่อยกระดับสู่มาตรฐาน ISO/IEC 27001:2022 ซึ่งรวมถึงการนำวงจรคุณภาพ PDCA มาประยุกต์ใช้กับกระบวนการสำรองข้อมูล ดังภาพที่ 2

ขั้นตอนการวางแผน (Plan)

ขั้นตอนการวางแผนเป็นการวางรากฐานและกำหนดทิศทางทั้งหมด ซึ่งเป็นขั้นตอนสำคัญที่สุดในการบริหารจัดการระบบสำรองข้อมูล โดยเริ่มจากการดำเนินการดังต่อไปนี้

1. กำหนดนโยบายและวัตถุประสงค์ (Define Policy and Objectives) กำหนดนโยบายการสำรองข้อมูล (Backup Policy) เป็นลายลักษณ์อักษรที่ได้รับอนุมัติจากผู้บริหารระดับสูง โดยระบุขอบเขตของข้อมูลที่ต้องสำรอง เช่น ข้อมูลผู้ป่วย ข้อมูลการเงิน ความถี่ในการสำรอง และระยะเวลาจัดเก็บ

2. ประเมินความเสี่ยง (Risk Assessment) ระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูล เช่น แรนซัมแวร์ (Ransomware) ความล้มเหลวของฮาร์ดแวร์ (Hardware Failure) ภัยธรรมชาติ หรือความผิดพลาดของเจ้าหน้าที่ เพื่อนำมาจัดลำดับความสำคัญของระบบที่ต้องได้รับการป้องกัน

3. กำหนดค่า RPO และ RTO (Define RPO/RTO) กำหนดเป้าหมายการกู้คืนข้อมูลสำหรับระบบสารสนเทศ แต่ละประเภท

3.1 RPO (Recovery Point Objective) ขอบเขตสูงสุดของปริมาณข้อมูลที่องค์กรสามารถยอมรับได้ว่าจะสูญหายไปในการณ์ที่เกิดเหตุการณ์ฉุกเฉินหรือความล้มเหลวของระบบสารสนเทศ โดยเป็นเกณฑ์ที่กำหนดระดับการสูญเสียข้อมูลที่ยังคงอยู่ในขอบข่ายที่องค์กรสามารถดำเนินงานต่อได้ ตัวอย่างเช่น ในกรณีของระบบ Hospital Information System (HIS) ซึ่งเป็นระบบที่มีความสำคัญต่อการให้บริการทางการแพทย์ อาจกำหนดค่า RPO ไม่เกิน 15 นาที เพื่อให้มั่นใจว่าข้อมูลผู้ป่วยและข้อมูลทางคลินิกที่สำคัญจะไม่สูญหายเกินกว่าช่วงเวลาดังกล่าว

3.2 RTO (Recovery Time Objective) ระยะเวลาสูงสุดที่องค์กรสามารถยอมรับได้ในการฟื้นฟูระบบสารสนเทศหรือบริการที่หยุดชะงักให้กลับมาสู่สภาวะปกติได้ตามมาตรฐานที่กำหนด โดย RTO เป็นตัวชี้วัดที่สะท้อนถึงความสามารถในการดำเนินงานต่อเนื่องขององค์กรหลังจากเกิดเหตุการณ์ฉุกเฉิน ตัวอย่างเช่น ในกรณีของระบบ Hospital Information System (HIS) ซึ่งเป็นระบบที่มีความสำคัญอย่างยิ่งต่อการให้บริการทางการแพทย์ อาจกำหนดค่า RTO ไม่เกิน 4 ชั่วโมง เพื่อให้มั่นใจว่าสามารถกู้คืนระบบและกลับมาให้บริการได้ภายในกรอบเวลาที่กำหนด ดังภาพที่ 3



ภาพที่ 3 การกำหนดค่า RPO และ RTO

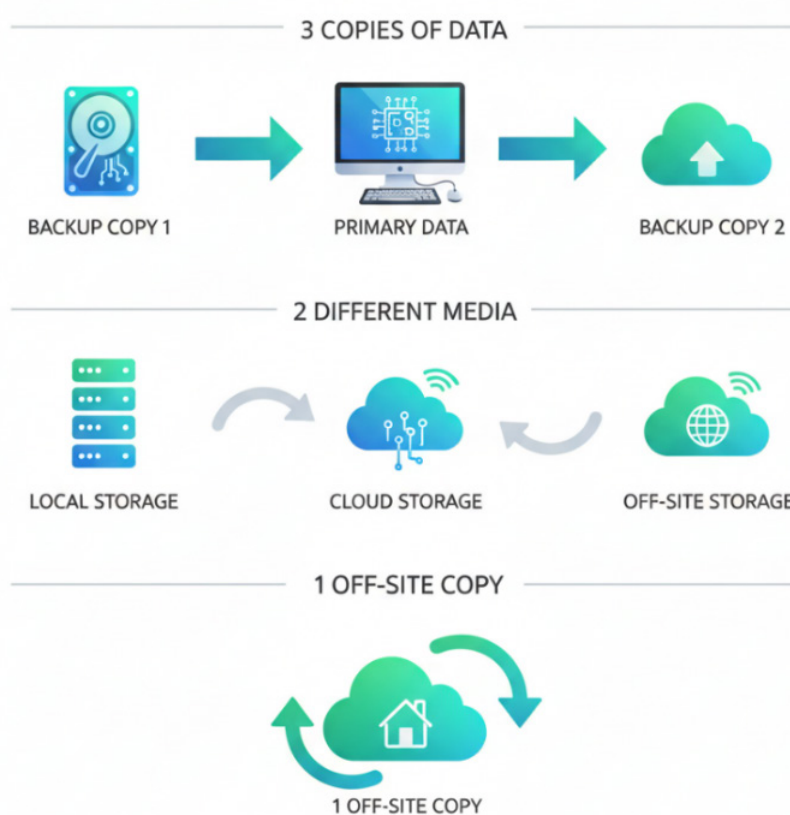
ที่มา: สร้างด้วย Gemini [Google] โดยผู้เขียน เมื่อวันที่ 10 กันยายน 2025

4. จัดตั้งทีมงานและกำหนดบทบาท (Form a Team) แต่งตั้งผู้รับผิดชอบที่ชัดเจนสำหรับกระบวนการสำรองและกู้คืนข้อมูล

ขั้นตอนการดำเนินงาน (Do)

เมื่อกำหนดแผนแล้ว โรงพยาบาลต้องนำมาปฏิบัติให้เกิดผลจริง โดยมีกระบวนการดังนี้

1. เลือกเทคโนโลยีที่เหมาะสม (Select Appropriate Technology) จัดหาระบบฮาร์ดแวร์และซอฟต์แวร์สำรองข้อมูลที่สอดคล้องกับนโยบายและค่า RPO/RTO ที่กำหนดไว้ อาจเป็นการผสมผสานระหว่างการจัดเก็บไว้ในองค์กร (On-premise) และบนคลาวด์ (Cloud) เพื่อปฏิบัติตามกฎ 3-2-1 (สำเนา 3 ชุด บนสื่อ 2 ชนิด และเก็บนอกสถานที่ 1 ชุด) (Lobur et al., 2020) ดังภาพที่ 4



ภาพที่ 4 กฎ 3-2-1 (สำเนา 3 ชุด บนสื่อ 2 ชนิด และเก็บนอกสถานที่ 1 ชุด)

ที่มา: สร้างด้วย Gemini [Google] โดยผู้เขียน เมื่อวันที่ 13 กันยายน 2025

2. ติดตั้งและกำหนดค่าระบบ (Implement and Configure) ดำเนินการติดตั้งระบบตามแผน กำหนดตารางเวลาการสำรองข้อมูลอัตโนมัติ และตั้งค่ามาตรการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูล (Encryption) ทั้งในขณะจัดเก็บและระหว่างการส่งผ่านข้อมูล

3. จัดทำเอกสารขั้นตอนการปฏิบัติงาน (Document Procedures) สร้างเอกสารคู่มือการสำรองและการกู้คืนข้อมูล (Backup and Restore Procedures) อย่างละเอียด เพื่อให้เจ้าหน้าที่สามารถปฏิบัติตามได้อย่างถูกต้องและเป็นมาตรฐานเดียวกัน

4. สร้างความตระหนักและฝึกอบรม (Awareness and Training) จัดอบรมให้เจ้าหน้าที่เข้าใจขั้นตอนการปฏิบัติงาน และสื่อสารกับผู้ใช้งานทั่วไปให้ตระหนักถึงความสำคัญของการจัดการข้อมูล

ขั้นตอนการตรวจสอบ (Check)

การตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลสำรองเป็นขั้นตอนที่สำคัญและไม่ควรมองข้าม เป็นที่ยืนยันให้มั่นใจได้ว่าระบบสำรองข้อมูลสามารถทำงานได้ตามที่คาดหวังและพร้อมใช้งานในกรณีที่เหตุการณ์ไม่คาดคิด

1. เฝ้าระวังและติดตามผล (Monitoring) ตรวจสอบผลการสำรองข้อมูลในแต่ละวัน (Daily Backup Jobs) ว่าสำเร็จหรือไม่ และแก้ไขทันทีเมื่อพบข้อผิดพลาด

2. ทดสอบการกู้คืนข้อมูล (Recovery Testing) ขั้นตอนนี้มีความสำคัญอย่างยิ่ง โดยควรมีการวางแผนและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง เพื่อพิสูจน์ว่าข้อมูลที่สำรองไว้สามารถนำกลับมาใช้งานได้จริง การทดสอบควรครอบคลุมหลายสถานการณ์ ตั้งแต่การกู้คืนไฟล์เดียวไปจนถึงการกู้คืนทั้งระบบ

3. การตรวจสอบภายใน (Internal Audit) กำหนดให้มีการตรวจสอบกระบวนการทั้งหมดโดยผู้ตรวจสอบภายในหรือคณะทำงานที่มิได้มีส่วนเกี่ยวข้องกับการปฏิบัติงานโดยตรง เพื่อทำหน้าที่ทวนสอบความถูกต้องและความสอดคล้องของการดำเนินงานกับนโยบายและข้อกำหนดของมาตรฐาน

ขั้นตอนการปรับปรุง (Act)

ขั้นตอนสุดท้ายคือการนำผลการตรวจสอบที่ได้มาวิเคราะห์ สังเคราะห์ และประยุกต์ใช้ในการพัฒนาและปรับปรุงกระบวนการสำรองข้อมูลให้มีประสิทธิภาพและความน่าเชื่อถือมากยิ่งขึ้น ทั้งนี้เพื่อให้การดำเนินงานสอดคล้องกับนโยบาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้องอย่างต่อเนื่อง

1. วิเคราะห์ผลและดำเนินการแก้ไข (Analyze and Take Corrective Action) นำข้อผิดพลาดที่ตรวจพบจากการทดสอบหรือการตรวจสอบมาวิเคราะห์หาสาเหตุเชิงระบบอย่างเป็นลำดับขั้นตอนพร้อมทั้งดำเนินการแก้ไขเชิงปฏิบัติ เพื่อป้องกันไม่ให้เกิดข้อบกพร่องหรือปัญหาซ้ำในอนาคต อันจะช่วยยกระดับประสิทธิภาพและความน่าเชื่อถือของกระบวนการโดยรวมให้ดีขึ้น

2. ทบทวนโดยฝ่ายบริหาร (Management Review) กำหนดให้มีการทบทวนผลการดำเนินงาน ผลการทดสอบ รวมถึงการวิเคราะห์ช่องว่างที่ยังต้องได้รับการปรับปรุง เพื่อนำเสนอรายงานต่อผู้บริหารระดับสูงอย่างน้อยปีละหนึ่งครั้ง กระบวนการดังกล่าวมีเป้าหมายเพื่อสร้างความมั่นใจว่า ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ได้รับการสนับสนุนอย่างเพียงพอ และมีการปรับปรุงอย่างต่อเนื่องตามนโยบายและข้อกำหนดของมาตรฐาน

การศึกษารอบแนวทางการใช้วงจร PDCA ภายใต้กรอบของมาตรฐาน ISO/IEC 27001:2022 ช่วยสนับสนุนให้โรงพยาบาลสามารถบริหารจัดการระบบสำรองข้อมูลได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยมากยิ่งขึ้น นอกจากนี้ แนวทางดังกล่าวยังมีบทบาทสำคัญในการเสริมสร้างความเชื่อมั่นให้แก่ผู้ป่วย รวมทั้งมีส่วนเกี่ยวข้องว่าข้อมูลที่มีความสำคัญจะได้รับการคุ้มครองอย่างเหมาะสม และสามารถนำกลับมาใช้งานได้อย่างทันท่วงทีเมื่อเกิดความจำเป็น (Guo et al., 2021)

กรณีศึกษาจากโรงพยาบาลต่างประเทศที่นำมาตรฐาน ISO/IEC 27001:2022 มาประยุกต์ใช้

การประยุกต์ใช้มาตรฐาน ISO/IEC 27001:2022 ในโรงพยาบาลมีตัวอย่างที่ชัดเจนในระดับสากล งานวิจัยที่ศึกษาโรงพยาบาลสองแห่งในประเทศอินโดนีเซียได้สะท้อนให้เห็นถึงมิติของความสำเร็จในการนำมาตรฐานไปปรับใช้ รวมถึงมิติของความท้าทายที่องค์กรต้องเผชิญระหว่างกระบวนการดำเนินงาน องค์ความรู้ที่ได้จากกรณีศึกษานี้จึงมีคุณค่าในการเป็นแนวทางสำหรับหน่วยบริการสุขภาพอื่น ๆ ที่มีความประสงค์จะพัฒนาและยกระดับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศตามกรอบมาตรฐานสากล

โรงพยาบาล Wava Husada (อินโดนีเซีย)

โรงพยาบาล Wava Husada ได้ทำการประเมินระบบเวชระเบียนอิเล็กทรอนิกส์ (Electronic Medical Record: EMR) โดยอ้างอิงหลักการของมาตรฐาน ISO/IEC 27001:2013 แม้จะอ้างอิงเวอร์ชัน 2013 แต่หลักการสำคัญยังคงสอดคล้องกับเวอร์ชัน 2022 ผลการศึกษาพบว่าโรงพยาบาลแห่งนี้ได้นำกลไกด้านความมั่นคงปลอดภัยไปปรับใช้ได้เป็นอย่างดีมีประสิทธิภาพ โดยมีประเด็นสำคัญที่เกี่ยวข้องโดยตรงกับการสำรองข้อมูลคือ

1. การมีระบบสำรองข้อมูล โรงพยาบาลได้จัดให้มีระบบสำรองข้อมูล (Data Backup Systems) เป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัยสารสนเทศ ซึ่งดำเนินการควบคู่กับการควบคุมสิทธิ์เข้าถึง การยืนยันตัวตน และการรักษาความลับของข้อมูล

2. นโยบายสำรองข้อมูลและการลบข้อมูล การสำรองข้อมูลและลบข้อมูลดำเนินการโดยเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น เพื่อเสริมความมั่นคงปลอดภัยและความถูกต้องของข้อมูล

3. การปฏิบัติตามกฎหมาย การมีระบบสำรองข้อมูลสอดคล้องกับกฎกระทรวงสาธารณสุขแห่งสาธารณรัฐอินโดนีเซีย (Permenkes No 24 Tahun 2022) ซึ่งกำหนดให้โรงพยาบาลต้องมีระบบสำรองข้อมูลเป็นมาตรการสำคัญในการรักษาความต่อเนื่องของบริการและความปลอดภัยของข้อมูล

4. ข้อเสนอแนะ การดำเนินงานสามารถยกระดับประสิทธิภาพได้โดยการเพิ่มมาตรการ การรับประกันว่าการดำเนินการใด ๆ ในระบบไม่สามารถปฏิเสธความรับผิดชอบได้ภายหลัง (Non-Repudiation) และการตรวจสอบบันทึกเหตุการณ์การเข้าถึงและการเปลี่ยนแปลงข้อมูลในระบบ เพื่อใช้ในการตรวจสอบย้อนหลัง (Audit Logs) อย่างต่อเนื่อง ซึ่งจะช่วยยกระดับความน่าเชื่อถือและความโปร่งใสของกระบวนการการสำรองข้อมูล

กรณีศึกษาดังกล่าวสะท้อนให้เห็นถึงการนำหลักการของมาตรฐาน ISO/IEC 27001:2013 มาประยุกต์ใช้ในทางปฏิบัติได้สำเร็จ โดยการสำรองข้อมูลถือเป็นองค์ประกอบพื้นฐานที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลผู้ป่วย และเสริมสร้างความเชื่อมั่นของผู้ที่มีส่วนเกี่ยวข้องต่อความพร้อมใช้งานและความน่าเชื่อถือของข้อมูล (Soraya et al., 2025)

โรงพยาบาล Bali Mandara (อินโดนีเซีย)

โรงพยาบาล Bali Mandara ซึ่งเคยเผชิญกับภัยคุกคามจากแรนซัมแวร์มาก่อน ได้ดำเนินการประเมินความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศโดยใช้เครื่องมือ Index KAMI 5.0 ซึ่งอ้างอิงมาตรฐาน ISO/IEC 27001:2022 โดยตรง ผลการประเมินชี้ให้เห็นถึงความท้าทายที่โรงพยาบาลต้องเผชิญอย่างชัดเจน ทั้งในแง่ของความพร้อมของระบบสารสนเทศ การจัดสรรทรัพยากรบุคคล และการบูรณาการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการดำเนินงาน

1. ผลการประเมินไม่ผ่านเกณฑ์ ผลการประเมินความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล Bali Mandara พบว่า คะแนนรวมอยู่ที่ 177 คะแนน ซึ่งถูกจัดอยู่ในระดับ “ไม่ผ่านเกณฑ์” (Not Eligible) สำหรับการรับรองมาตรฐาน ISO/IEC 27001:2022

2. ข้อเสนอแนะเพื่อการพัฒนา ข้อเสนอแนะที่สำคัญคือการเสริมความแข็งแกร่งให้กับการปกป้องข้อมูลผ่านการควบคุมการเข้าถึงและการเข้ารหัส ซึ่งมาตรการเหล่านี้มีความสัมพันธ์โดยตรงกับการรักษาความปลอดภัยของข้อมูลที่สำรองไว้ และสะท้อนให้เห็นว่ากระบวนการที่เกี่ยวข้องกับการสำรองและกู้คืนข้อมูลยังเป็นส่วนที่ต้องได้รับการพัฒนาให้เป็นระบบตามกรอบของมาตรฐาน ISO/IEC 27001:2022 อย่างต่อเนื่อง

กรณีศึกษานี้เป็นตัวอย่างที่ดีของโรงพยาบาลที่ตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และได้เริ่มต้นกระบวนการประเมินตนเองตามมาตรฐานสากล ซึ่งผลลัพธ์จากการประเมินเผยให้เห็นช่องว่างและ

ข้อบกพร่องที่จำเป็นต้องได้รับการแก้ไขและปรับปรุง เพื่อให้องค์กรสามารถสร้างความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศได้อย่างแท้จริง (Wibawa et al., 2024) ดังตารางที่ 1

ตารางที่ 1 การเปรียบเทียบกรณีศึกษาการประยุกต์ใช้มาตรฐาน ISO/IEC 27001:2022 ในโรงพยาบาลต่างประเทศ

โรงพยาบาล/ กรณีศึกษา	โรงพยาบาล Wava Husada	โรงพยาบาล Bali Mandara
บริบท/สภาพแวดล้อม	ปฏิบัติตามกฎกระทรวงสาธารณสุข อินโดนีเซียเกี่ยวกับเวชระเบียน อิเล็กทรอนิกส์	เคยประสบเหตุโจมตีด้วยแรนซัมแวร์ และไม่เคยมีการประเมินระบบความ มั่นคงปลอดภัยมาก่อน
มาตรฐานที่อ้างอิง	ISO/IEC 27001:2013 แม้จะอ้างอิงเวอร์ชัน 2013 แต่หลักการสำคัญยังคงสอดคล้องกับ เวอร์ชัน 2022	ISO/IEC 27001:2022 (ผ่าน Index KAMI 5.0)
จุดประสงค์การประเมิน	ประเมินความปลอดภัยของระบบเวช ระเบียนอิเล็กทรอนิกส์ (EMR)	ประเมินความพร้อมด้านความมั่นคง ปลอดภัยโดยรวมของโรงพยาบาล
ผลลัพธ์ที่สำคัญ	มีการสำรองข้อมูล (Data Backup) จริง ควบคุมสิทธิ์ และปกป้องข้อมูลได้ดี	ได้คะแนนเพียง 177 ระดับ Not Eligible ต้องปรับปรุงอย่างมาก
ข้อเสนอแนะ	ควรเสริม Audit Logs และ Non- repudiation เพื่อเพิ่มความน่าเชื่อถือ	จัดทำ Governance Policy, จัดการ ความเสี่ยง, เพิ่มการเข้ารหัสข้อมูล และ วางระบบสำรองข้อมูลที่ชัดเจน
นัยสำคัญต่อบทความ	เป็นตัวอย่างของการนำไปปฏิบัติสำเร็จ	เป็นตัวอย่างของความท้าทายและ ช่องว่างที่ต้องแก้ไข

จากกรณีศึกษาของโรงพยาบาลทั้งสองแห่งพบว่า แม้ทั้งสององค์กรจะมีเป้าหมายเดียวกันในการยกระดับความมั่นคงปลอดภัยสารสนเทศ แต่ผลลัพธ์ที่เกิดขึ้นกลับแตกต่างกันอย่างชัดเจน โดยโรงพยาบาล Wava Husada สามารถนำมาตรการพื้นฐานอย่างการสำรองข้อมูลไปปฏิบัติได้อย่างเป็นรูปธรรม ในขณะที่โรงพยาบาล Bali Mandara ยังคงมีช่องว่างในกระบวนการและไม่ผ่านเกณฑ์การประเมินความพร้อม ซึ่งสะท้อนให้เห็นว่าการนำมาตรฐาน ISO/IEC 27001:2022 ไปใช้ให้เกิดผลสำเร็จในทางปฏิบัตินั้น ไม่ได้ขึ้นอยู่กับตัวมาตรฐานเพียงอย่างเดียว แต่ขึ้นอยู่กับปัจจัยพื้นฐานขององค์กรเป็นสำคัญ ได้แก่ ความพร้อมขององค์กร ความมุ่งมั่นของผู้บริหารระดับสูง ในการสนับสนุนทรัพยากรและผลักดันนโยบาย และวุฒิภาวะด้านความมั่นคงปลอดภัยขององค์กรในการประเมินความเสี่ยงและวางกรอบการทำงานให้เกิดขึ้นจริง ดังนั้นการมีเพียงมาตรฐานจึงไม่เพียงพอหากองค์กรยังขาดความพร้อมในมิติเหล่านี้

ความท้าทายและปัจจัยแห่งความสำเร็จ

การศึกษารอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 กับระบบสำรองข้อมูลในโรงพยาบาล แม้ว่าจะให้ประโยชน์อย่างมีนัยสำคัญต่อความมั่นคงปลอดภัยของข้อมูลผู้ป่วยและความต่อเนื่องของการให้บริการ แต่ก็ถือเป็นกระบวนการที่มีความซับซ้อนและต้องเผชิญกับความท้าทายหลายประการ การทำความเข้าใจอุปสรรคเหล่านี้เป็นสิ่งสำคัญ เพราะช่วยให้องค์กรสามารถวางแผนและเตรียมการรับมือได้อย่างเป็นระบบและมีประสิทธิภาพ

ความท้าทายในการศึกษากรอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 กับระบบสำรองข้อมูลในโรงพยาบาล

1. ข้อจำกัดด้านงบประมาณ การลงทุนในเทคโนโลยีการสำรองข้อมูลที่ทันสมัย ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และบริการคลาวด์ที่สามารถทำ Immutable Backup ได้นั้น ต้องใช้งบประมาณที่สูง ซึ่งถือเป็นอุปสรรคสำคัญ โดยเฉพาะโรงพยาบาลภาครัฐที่มีข้อจำกัดด้านงบประมาณ

2. การขาดความตระหนักของบุคลากร บุคลากรทางการแพทย์และผู้ใช้งานทั่วไปอาจไม่ตระหนักถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ ส่งผลให้เกิดการกระทำที่เสี่ยงต่อข้อมูลหรือขาดความร่วมมือในการดำเนินการตามมาตรการด้านความมั่นคงปลอดภัย

3. ความซับซ้อนของระบบเดิม โรงพยาบาลจำนวนมากมีระบบสารสนเทศที่มีความหลากหลายและใช้งานต่อเนื่องมาเป็นเวลานาน การนำระบบสำรองข้อมูลที่เป็นมาตรฐานเดียวกันมาใช้กับทุกระบบจึงเป็นกระบวนการที่ซับซ้อนและท้าทายทางด้านเทคนิค เนื่องจากต้องคำนึงถึงความแตกต่าง ความเข้ากันได้ของเทคโนโลยี ตลอดจนข้อกำหนดด้านความมั่นคงปลอดภัยและการให้บริการอย่างต่อเนื่อง

4. การสร้างสมดุลระหว่างความปลอดภัยและการปฏิบัติงาน การตั้งค่าความปลอดภัยที่เข้มงวดเกินไปอาจกระทบต่อความเร็วในการเข้าถึงข้อมูล ซึ่งจำเป็นต่อการดูแลผู้ป่วย การหาจุดสมดุลที่เหมาะสมระหว่างความปลอดภัยและการใช้งานจึงเป็นสิ่งสำคัญ

5. การขาดแคลนบุคลากรผู้เชี่ยวชาญ การบริหารจัดการ ISMS ตามมาตรฐาน ISO/IEC 27001:2022 และเทคโนโลยีการสำรองข้อมูลสมัยใหม่ จำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถเฉพาะทาง ซึ่งเป็นตำแหน่งที่ขาดแคลนในตลาดแรงงาน ส่งผลต่อความต่อเนื่องและประสิทธิภาพของกระบวนการ

ปัจจัยแห่งความสำเร็จในการศึกษากรอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 กับระบบสำรองข้อมูลในโรงพยาบาล

จากความท้าทายที่เกิดขึ้น การดำเนินงานให้ประสบความสำเร็จจำเป็นต้องอาศัยปัจจัยสนับสนุนที่สำคัญดังนี้

1. การสนับสนุนจากผู้บริหารระดับสูง ปัจจัยที่สำคัญที่สุดคือการที่ผู้บริหารเล็งเห็นถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ และให้การสนับสนุนด้านนโยบาย จัดสรรงบประมาณ และทรัพยากรที่จำเป็น การสนับสนุนนี้จะช่วยขับเคลื่อนการดำเนินงานและสร้างความร่วมมือจากทุกฝ่ายในองค์กร

2. การสื่อสารและการฝึกอบรมที่มีประสิทธิภาพ องค์กรควรมีการสื่อสารนโยบายและขั้นตอนการปฏิบัติงานให้บุคลากรทุกระดับเข้าใจอย่างถูกต้องและชัดเจน พร้อมจัดให้มีการฝึกอบรมอย่างสม่ำเสมอ เพื่อสร้างวัฒนธรรมองค์กรให้เห็นถึงความสำคัญกับความมั่นคงปลอดภัยของข้อมูล

3. การดำเนินงานแบบค่อยเป็นค่อยไป แทนที่จะปรับเปลี่ยนทุกระบบพร้อมกัน ควรวางแผนดำเนินงานเป็นระยะ เริ่มต้นจากระบบที่สำคัญที่สุดก่อน เช่น ระบบ HIS/EMR เพื่อลดความเสี่ยงและสร้างต้นแบบความสำเร็จอันเป็นพื้นฐานสำหรับการขยายผลไปยังระบบอื่นในลำดับถัดไป

4. การทดสอบและปรับปรุงอย่างต่อเนื่อง ความสำเร็จไม่ได้จำกัดอยู่เพียงการติดตั้งระบบเท่านั้น แต่รวมถึงการทำให้มั่นใจว่าระบบสามารถทำงานได้จริงเมื่อต้องการใช้งาน การจัดทำตารางทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ และนำผลลัพธ์มาปรับปรุงแก้ไขเป็นหัวใจสำคัญของการสร้างความยืดหยุ่นทางไซเบอร์

5. การเลือกใช้เทคโนโลยีที่เหมาะสม การเลือกระบบที่สามารถตอบโต้ภัยได้ทั้งในปัจจุบันและอนาคต เช่น เทคโนโลยีที่รองรับการป้องกันแรนซัมแวร์โดยเฉพาะ จะช่วยลดความเสี่ยงและเพิ่มประสิทธิภาพในการบริหารจัดการข้อมูลในระยะยาว

บทสรุป

การสำรองข้อมูลถือเป็นหัวใจสำคัญของการให้บริการทางการแพทย์ การมีระบบสำรองข้อมูลที่แข็งแกร่งและเชื่อถือได้ไม่ได้เป็นเพียงทางเลือก แต่กลายเป็นความจำเป็นเชิงกลยุทธ์ เพื่อรับประกันความต่อเนื่องในการดูแลผู้ป่วย การปฏิบัติตามข้อกำหนด และการปกป้องชื่อเสียงของโรงพยาบาล บทความนี้นำเสนอให้เห็นว่าการศึกษารังนี้ได้สังเคราะห์กรอบแนวทางตามมาตรฐาน ISO/IEC 27001:2022 เพื่อใช้เป็นแนวคิดในการจัดการระบบสำรองข้อมูลของโรงพยาบาลอย่างเป็นระบบ โดยเน้นให้เห็นความสัมพันธ์ระหว่างข้อกำหนดในภาคผนวก A กับการปฏิบัติจริงตามวงจร PDCA ซึ่งสามารถนำไปประยุกต์ใช้ต่อยอดในการพัฒนาแนวทางปฏิบัติหรือแบบจำลองการบริหารจัดการข้อมูลสำรองในอนาคตได้

การศึกษารอบแนวทางตามมาตรฐานผ่านวงจรคุณภาพ PDCA ช่วยให้โรงพยาบาลสามารถวางแผน ปฏิบัติ ตรวจสอบ และปรับปรุงกระบวนการได้อย่างต่อเนื่อง โดยมีข้อกำหนดที่สำคัญอย่าง A.8.13 (Information Backup) และ A.5.30 (ICT Readiness for Business Continuity) เป็นแกนหลัก กรณีศึกษาจากโรงพยาบาลในต่างประเทศได้สะท้อนภาพความเป็นจริงให้เห็น ทั้งตัวอย่างของการนำไปปฏิบัติได้สำเร็จ และความท้าทายที่ยังต้องเผชิญ ซึ่งตอกย้ำว่าความสำเร็จไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่ต้องอาศัยการสนับสนุนจากผู้บริหาร ความตระหนักของบุคลากร และการทดสอบอย่างสม่ำเสมอ

ท้ายที่สุด แม้บทความนี้จะมุ่งเน้นที่บริบทของโรงพยาบาล แต่กรอบการทำงานของมาตรฐาน ISO/IEC 27001:2022 และหลักการของวงจร PDCA นั้นเป็นเครื่องมือสากลที่องค์กรทุกประเภทสามารถนำไปประยุกต์ใช้เพื่อยกระดับความมั่นคงปลอดภัยสารสนเทศของตนเองได้อย่างมีประสิทธิภาพเช่นเดียวกัน

ข้อเสนอแนะ

เพื่อให้การนำมาตรฐานไปศึกษาและประยุกต์ใช้เกิดประโยชน์สูงสุด มีข้อเสนอแนะสำหรับผู้มีส่วนเกี่ยวข้องในระดับต่าง ๆ ดังนี้

ข้อเสนอแนะเชิงนโยบายสำหรับผู้บริหารโรงพยาบาล

1. ให้ความสำคัญเป็นวาระหลัก ผู้บริหารควรบรรจุเรื่องความมั่นคงปลอดภัยไซเบอร์และความต่อเนื่องทางธุรกิจเป็นส่วนหนึ่งของยุทธศาสตร์หลักของโรงพยาบาล ไม่ใช่เพียงเรื่องของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น
2. จัดสรรงบประมาณที่เพียงพอ การลงทุนในระบบสำรองข้อมูลควรถูกมองว่าเป็นการลงทุนเพื่อความยั่งยืนขององค์กร ผู้บริหารควรจัดสรรงบประมาณที่เพียงพอสำหรับเทคโนโลยีและการฝึกอบรมบุคลากรอย่างเหมาะสม

ข้อเสนอแนะเชิงปฏิบัติสำหรับนักวิชาการคอมพิวเตอร์และฝ่ายเทคโนโลยีสารสนเทศ

1. ให้ความสำคัญกับการทดสอบ ต้องผลักดันให้การทดสอบการกู้คืนข้อมูลเกิดขึ้นจริงอย่างน้อยปีละหนึ่งครั้ง และนำผลลัพธ์มาปรับปรุงกระบวนการอย่างต่อเนื่อง
2. ใช้ประโยชน์จากเทคโนโลยีสมัยใหม่ ศึกษาและพิจารณาการนำเทคโนโลยี Immutable Backup มาใช้เป็นมาตรการป้องกันหลักต่อการโจมตีแรนซัมแวร์
3. สร้างองค์ความรู้ จัดทำคู่มือและขั้นตอนการปฏิบัติงานที่ชัดเจน รวมทั้งจัดอบรมให้ความรู้แก่บุคลากรอย่างสม่ำเสมอ

ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

1. การวิเคราะห์ความคุ้มค่า ควรมีการศึกษาวิจัยเชิงปริมาณเพื่อวิเคราะห์ความคุ้มค่าในการลงทุน (Return on Investment: ROI) ของการจัดทำระบบสำรองข้อมูลตามมาตรฐาน ISO/IEC 27001:2022 ในบริบทของโรงพยาบาลไทย
2. ผลกระทบของ AI ศึกษาความเป็นไปได้ในการนำปัญญาประดิษฐ์ (Artificial Intelligence: AI) และ Machine Learning มาช่วยในการบริหารจัดการและตรวจจับความผิดปกติของระบบสำรองข้อมูล

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จลุล่วงได้ด้วยความรู้และการสนับสนุนจากฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ซึ่งได้มอบความช่วยเหลือทั้งในด้านการเรียนรู้ การจัดสรรทรัพยากร และการสนับสนุนเทคโนโลยี เพื่อพัฒนาระบบสำรองข้อมูลให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022 ตลอดจนเปิดโอกาสให้ผู้เขียนได้มีส่วนร่วมในการดูแลและบริหารจัดการระบบสำรองข้อมูลของโรงพยาบาลศิริราช การสนับสนุนดังกล่าวมีส่วนสำคัญต่อการเพิ่มประสิทธิภาพในการปฏิบัติงานและการให้บริการผู้ป่วย ผู้เขียนขอแสดงความขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

การใช้ปัญญาประดิษฐ์ (Generative AI) ในต้นฉบับบทความ

ผู้เขียนบทความได้ใช้เครื่องมือปัญญาประดิษฐ์ (Generative AI) ได้แก่ Gemini ของ Google เพื่อช่วยในการปรับปรุงข้อความ การตรวจแก้ภาษา การแปลภาษา และการสร้างภาพ ตลอดจนการช่วยจัดระเบียบข้อมูล ทั้งนี้ ผู้เขียนได้ตรวจสอบความถูกต้อง ความครบถ้วน ความเหมาะสมของเนื้อหาด้วยตนเอง และเป็นผู้รับผิดชอบสูงสุดต่อเนื้อหาทั้งหมดของบทความที่ได้รับการตีพิมพ์ รวมถึงความถูกต้องของรายการอ้างอิงที่ปรากฏในเอกสารอ้างอิงท้ายบทความ

คำชี้แจงบทบาทผู้พิมพ์ (CRediT Author Statement)

ไพศัลป์ชัย ไชยพรเดชเจริญ: การคิดค้นแนวคิด; การตรวจสอบความถูกต้อง; การจัดการข้อมูล; การเขียนต้นฉบับบทความ; การทบทวนต้นฉบับบทความ; การสร้างภาพประกอบ, **สมชัย บุรีรักษ์:** การตรวจสอบความถูกต้อง; การทบทวนต้นฉบับบทความ

เอกสารอ้างอิง

- ฝ่ายสารสนเทศ. (2560). *ฝ่ายสารสนเทศ ผ่านการรับรองมาตรฐาน ISO27001 มาตรฐานเกี่ยวกับการบริหารจัดการสารสนเทศให้มั่นคงปลอดภัย*. กรุงเทพฯ: คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล.
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). *แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับโรงพยาบาลของรัฐ*. สืบค้นจาก <https://drive.ncsa.or.th/s/8tnTy6GTBenT5M6>
- Brezavšek, A., & Vidmar, D. (2023). *Spremembe, ki jih prinašajo nove različice v družini standardov za informacijsko varnost ISO/IEC 27000* [Changes brought by new versions in the ISO/IEC 27000 family of information security standards] (pp. 179-195). In 42nd International Conference on Organizational Science Development. Retrieved from <https://doi.org/10.18690/um.fov.3.2023.15>
- Guo, H., Wei, M., Huang, P., & Chekole, E. (2021). *Enhance enterprise security through implementing ISO/IEC 27001 standard* (pp. 1-6). 2021 IEEE International Conference on Service Operations and Logistics, and Informatics. New York: IEEE Press.
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. Switzerland: ISO.
- Lobur, M., Shcherbovskykh, S., & Stefanovych, T. (2020). *Availability audit of IoT system data reserved by 3-2-1 backup strategy based on fault tree and state transition diagram analysis* (pp. 343-346). 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies. New York: IEEE Press.
- Malatji, M. (2023). *Management of enterprise cyber security: A review of ISO/IEC 27001:2022* (pp. 117-122). 2023 International Conference on Cyber Management and Engineering. New York: IEEE Press.
- Soraya, Oktoriyani, E. N., & Mawan, M. S. A. (2025). Evaluasi keamanan dan privasi sistem rekam medis elektronik: Studi kasus di Rumah Sakit Wava Husada [Evaluation of security and privacy of electronic medical record systems: A case study at Wava Husada Hospital]. *Jurnal Rekam Medis dan Informasi Kesehatan*, 6(1), 16-24.
- Tistiyani, S., Briliyant, O., & Trianto, N. (2023). *Tailoring e-Government's ICT readiness for business continuity based on Cyber-Risk approach* (pp. 1-8). 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity. New York: IEEE Press.
- Wibawa, I. N. A. A., Susila, A. A. N. H., & Pasirullo, M. A. (2024). Information security evaluation at hospital using Index KAMI 5.0 and recommendations based on ISO/IEC 27001:2022. *Journal of Information Systems and Informatics*, 6(4), 949-963.