การให้บริการ Remote เข้ามาใช้งาน HOSxP จากภายนอกองค์กร ศูนย์อนามัยที่ 10 อุบลราชธานี

1.กลุ่มงาน สื่อสารประชาสัมพันธ์ และเทคโนโลยีสารสนเทศ

2. ผู้รับชิดชอบหลัก

นายเอกภพ ทะวาเงิน นักวิชาการคอมพิวเตอร์ชำนาญการ

3. ผู้รับชิดชอบร่วม

นางสาวสุกานดา แก้วล้อมบึง พยาบาลวิชาชีพชำนาญการพิเศษ

4. สรุปผลงานโดยย่อ / Abstract

ศูนย์อนามัยที่ 10 อุบลราชธานี เป็นหน่วยงานสาธารณสุขระดับเขตที่ใช้ระบบสารสนเทศโรงพยาบาล HOSxP เป็นโครงสร้างพื้นฐานหลักในการบริหารจัดการข้อมูลสุขภาพ บุคลากรมีความจำเป็นต้องเข้าถึงระบบดังกล่าวจากภายนอกองค์กรมากขึ้นในยุคการทำงานแบบดิจิทัล อย่างไรก็ตาม พบว่ากระบวนการให้บริการ Remote Access ยังขาดมาตรฐาน ขั้นตอน และการควบคุมความปลอดภัยที่ชัดเจน ก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลสุขภาพและไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 การดำเนินงาน CQI ครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาและกำหนดมาตรฐานกระบวนการให้บริการ Remote Access เข้าใช้งาน HOSxP ลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มประสิทธิภาพการปฏิบัติงานของบุคลากร โดยใช้วงจรคุณภาพ PDCA เป็นกรอบการดำเนินงานตลอดปีงบประมาณ 2568

ผลการดำเนินงานพบว่าทุกตัวชี้วัดบรรลุเป้าหมายที่กำหนด ได้แก่ อัตราการดำเนินการคำขอ Remote Access ภายใน 1 วันทำการเพิ่มขึ้นจากร้อยละ 52 เป็นร้อยละ 95 ผู้ใช้งานทุกรายผ่านการยืนยันตัวตนแบบหลายปัจจัย (MFA) ร้อยละ 100 ไม่พบ Security Incident ตลอดระยะเวลาดำเนินการ บุคลากรผ่านการอบรมด้านความปลอดภัยร้อยละ 92 และความพึงพอใจของผู้ใช้งานอยู่ที่ร้อยละ 87 นอกจากนี้ยังเกิดนวัตกรรม 4 ชิ้น ได้แก่ คู่มือ SOP การให้บริการ Remote Access ระบบ VPN ผสาน MFA แบบมาตรฐาน Dashboard ติดตามสถานะแบบ Real-time และคลังความรู้ด้านความปลอดภัยสารสนเทศสำหรับบุคลากรสาธารณสุข

บทเรียนสำคัญที่ได้รับคือการสนับสนุนจากผู้บริหาร การอบรมบุคลากรอย่างต่อเนื่อง และการกำหนดตัวชี้วัดที่วัดได้จริง เป็นปัจจัยแห่งความสำเร็จที่ขาดไม่ได้ในการพัฒนาคุณภาพด้านเทคโนโลยีสารสนเทศของหน่วยงานสาธารณสุข

5. ที่มาของปัญหา

ศูนย์อนามัยที่ 10 อุบลราชธานี เป็นศูนย์วิชาการด้านการส่งเสริมสุขภาพระดับเขต สังกัดกรมอนามัย กระทรวงสาธารณสุข รับผิดชอบพื้นที่ดำเนินการ 5 จังหวัด ได้แก่ อุบลราชธานี ศรีสะเกษ มุกดาหาร ยโสธร และอำนาจเจริญ ซึ่งมีบทบาทสำคัญในการให้บริการด้านสาธารณสุขแก่ประชาชนในพื้นที่เขตสุขภาพที่ 10 อย่างครอบคลุมและต่อเนื่อง

ในกระบวนการบริหารจัดการด้านสุขภาพของหน่วยงาน ระบบ HOSxP ถูกนำมาใช้เป็นระบบสารสนเทศหลัก HOSxP เป็นระบบสารสนเทศโรงพยาบาล (Hospital Information System) ที่รู้จักกันในนาม Electronic Health Record (EHR) ซึ่งให้บริการโรงพยาบาลมากกว่า 300 แห่งทั่วประเทศไทย โดยมีวัตถุประสงค์เพื่ออำนวยความสะดวกในกระบวนการทำงานด้านสุขภาพ ตั้งแต่ศูนย์สุขภาพชุมชนขนาดเล็กไป

จนถึงโรงพยาบาลส่วนกลาง ด้วยเหตุนี้ HOSxP จึงเป็นโครงสร้างพื้นฐานด้านดิจิทัลที่มีความสำคัญอย่างยิ่งต่อการปฏิบัติงานของบุคลากรภายในองค์กร

สถานการณ์การทำงานในปัจจุบันมีความเปลี่ยนแปลงอย่างมีนัยสำคัญ บุคลากรมีความจำเป็นต้องเข้าถึงข้อมูลและใช้งานระบบ HOSxP จากภายนอกองค์กรมากขึ้น ไม่ว่าจะเป็นการปฏิบัติงานนอกสถานที่ การออกตรวจพื้นที่ การทำงานในวันหยุด หรือในสถานการณ์ฉุกเฉินต่าง ๆ ซึ่งการเข้าถึงระบบจากระยะไกล (Remote Access) อย่างไม่เป็นระบบหรือขาดมาตรฐาน ย่อมก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลได้

ความเสี่ยงดังกล่าวมีน้ำหนักทางกฎหมายอย่างชัดเจน เนื่องจาก ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ข้อมูลด้านสุขภาพจัดเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ซึ่งไม่สามารถเก็บรวบรวมใช้ หรือเปิดเผยได้หากไม่ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล โดยโรงพยาบาล คลินิก บริษัทประกัน และหน่วยงานที่เกี่ยวข้องทั้งหมดต้องนำมาตรการทางเทคนิคและองค์กรมาใช้เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ดังนั้น การออกแบบระบบ Remote Access ที่ปลอดภัยจึงไม่ใช่เพียงการพัฒนาเชิงเทคนิค แต่เป็นข้อกำหนดทางกฎหมายที่องค์กรต้องปฏิบัติตาม

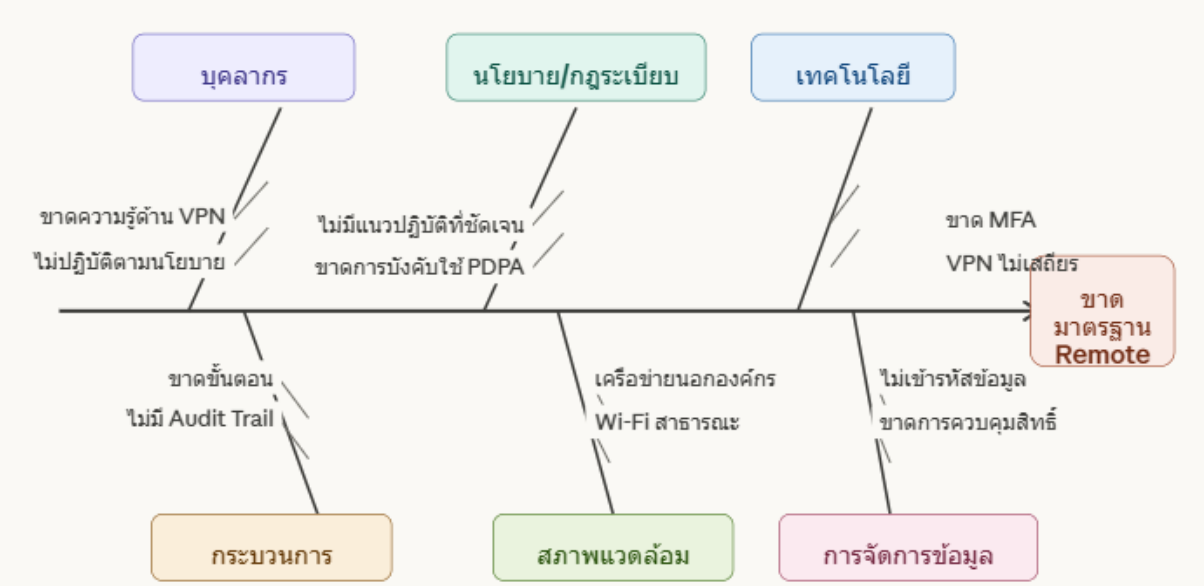
ในด้านเทคนิค การใช้งาน Virtual Private Network (VPN) ถือเป็นแนวทางมาตรฐานที่ได้รับการยอมรับ VPN เข้ารหัสการเชื่อมต่ออินเทอร์เน็ตระหว่างผู้ใช้งานระยะไกลกับเครือข่ายขององค์กร ซึ่งเป็นสิ่งสำคัญในการป้องกันไม่ให้ผู้ไม่ประสงค์ดีดักจับข้อมูลที่สำคัญระหว่างการส่งผ่านอินเทอร์เน็ต บุคลากรด้านสาธารณสุขควรเข้าถึงข้อมูลผู้ป่วยผ่านการเชื่อมต่อ VPN ที่ปลอดภัยเท่านั้น โดยเฉพาะเมื่อใช้งาน Wi-Fi สาธารณะหรือเครือข่ายที่บ้าน

อย่างไรก็ตาม ในทางปฏิบัติพบว่ากระบวนการให้บริการ Remote Access เข้าสู่ระบบ HOSxP ของศูนย์อนามัยที่ 10 อุบลราชธานีในปัจจุบัน ยังขาดการกำหนดขั้นตอน มาตรฐาน และการควบคุมที่ชัดเจน ส่งผลให้เกิดปัญหาในหลายด้าน ทั้งความล่าช้าในการขอรับบริการ ความเสี่ยงด้านความปลอดภัยของข้อมูล รวมถึงการขาดการบันทึกและตรวจสอบย้อนหลัง (Audit Trail) ที่เป็นระบบ

กฎหมาย PDPA ของไทย ซึ่งมีแนวทางสอดคล้องกับหลักการ GDPR ของสหภาพยุโรป พร้อมด้วยพระราชบัญญัติไซเบอร์ซีเคียวริตี้ ได้กำหนดให้หน่วยงานที่เกี่ยวข้องกับข้อมูลสุขภาพต้องให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคล การยินยอมในการใช้ข้อมูล และความเป็นส่วนตัว ดังนั้น การพัฒนากระบวนการให้บริการ Remote Access ที่มีมาตรฐาน ปลอดภัย และสามารถตรวจสอบได้ จึงเป็นสิ่งที่ศูนย์อนามัยที่ 10 อุบลราชธานี ต้องดำเนินการอย่างเร่งด่วนเพื่อรองรับการปฏิบัติงานของบุคลากรในยุคดิจิทัล ลดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ และปฏิบัติตามกรอบกฎหมายที่บังคับใช้อยู่ในปัจจุบันได้อย่างครบถ้วน การจัดทำรายงาน CQI ฉบับนี้จึงมีจุดมุ่งหมายเพื่อวิเคราะห์ปัญหา พัฒนากระบวนการ และกำหนดมาตรฐานการให้บริการ Remote Access เข้าใช้งาน HOSxP จากภายนอกองค์กรให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น

6. การวิเคราะห์ปัญหา

เพื่อให้การพัฒนาคุณภาพเป็นไปอย่างตรงจุด จึงได้นำเครื่องมือวิเคราะห์สาเหตุรากเหง้า (Root Cause Analysis) โดยใช้แผนผังก้างปลา (Fishbone Diagram / Cause and Effect Diagram) มาวิเคราะห์สาเหตุของปัญหาการให้บริการ Remote Access เข้าใช้งาน HOSxP จากภายนอกองค์กร ใน 5 มิติหลัก ดังนี้



แผนผังก้างปลา: สาเหตุปัญหาการให้บริการ Remote Access เข้าใช้งาน HOSxP
ศูนย์อนามัยที่ 10 อุบลราชธานี

จากการวิเคราะห์สาเหตุของปัญหาด้วยแผนผังก้างปลา สามารถจำแนกสาเหตุออกเป็น 5 มิติหลัก ดังนี้

6.1 ด้านบุคลากร (Man)

บุคลากรผู้ใช้งานขาดความรู้ความเข้าใจเกี่ยวกับการใช้งาน VPN และระบบ Remote Access อย่างถูกต้องและปลอดภัย รวมถึงขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) ส่งผลให้ไม่ปฏิบัติตามนโยบายความปลอดภัยขององค์กรอย่างเคร่งครัด เช่น การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงระบบผ่านเครือข่ายที่ไม่น่าเชื่อถือ

6.2 ด้านนโยบายและกฎระเบียบ (Policy)

องค์กรยังขาดแนวปฏิบัติ (Guideline) และนโยบายการใช้งาน Remote Access ที่ชัดเจนและเป็นลายลักษณ์อักษร รวมถึงยังไม่มีการกำหนดมาตรการรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 ในส่วนที่เกี่ยวกับการเข้าถึงข้อมูลสุขภาพจากระยะไกลอย่างครบถ้วน ทำให้เกิดช่องว่างด้านการปฏิบัติตามกฎหมาย

6.3 ด้านเทคโนโลยี (Technology)

ระบบโครงสร้างพื้นฐานที่รองรับการเชื่อมต่อจากระยะไกลยังขาดกลไกการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ที่เพียงพอ อีกทั้ง VPN Server ที่ใช้งานอยู่ในปัจจุบันอาจมีความไม่เสถียรหรือยังไม่ได้รับการอัปเดตและตรวจสอบความปลอดภัยอย่างสม่ำเสมอ ส่งผลให้เกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์

6.4 ด้านกระบวนการ (Process)

กระบวนการขอรับบริการและการอนุมัติ Remote Access ยังไม่มีขั้นตอนที่เป็นมาตรฐาน ไม่มีการบันทึกและตรวจสอบย้อนหลัง (Audit Trail) ที่ครบถ้วน และขาดการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Access Review) อย่างสม่ำเสมอ ทำให้ไม่สามารถตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติได้อย่างทันท่วงที

6.5 ด้านสภาพแวดล้อมและการจัดการข้อมูล (Environment & Data Management)

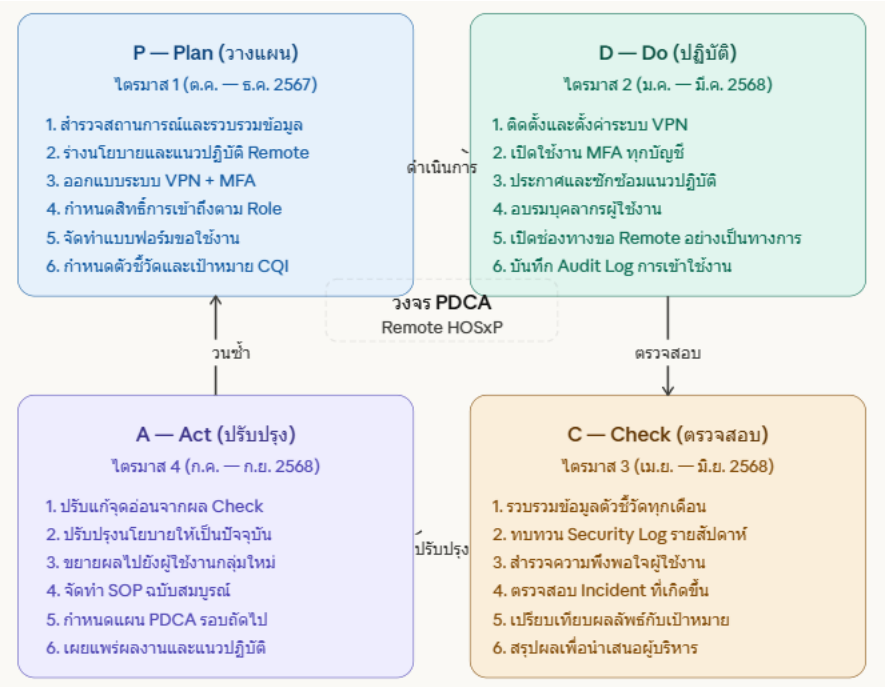
ผู้ใช้งานมักเชื่อมต่อจากเครือข่ายภายนอกองค์กรที่ไม่สามารถควบคุมความปลอดภัยได้ เช่น Wi-Fi สาธารณะหรือเครือข่ายส่วนตัวที่บ้าน ประกอบกับการรับส่งข้อมูลบางส่วนยังขาดการเข้ารหัส (Encryption) ที่เหมาะสม รวมถึงการจัดการสิทธิ์การเข้าถึงข้อมูล (Access Control) ยังไม่มีความละเอียดเพียงพอตามหลักการ Least Privilege ซึ่งเป็นความเสี่ยงสำคัญต่อความปลอดภัยของข้อมูลสุขภาพของผู้รับบริการ

7. วัตถุประสงค์

1. เพื่อพัฒนาและกำหนดมาตรฐานกระบวนการให้บริการ Remote Access เข้าใช้งานระบบ HOSxP จากภายนอกองค์กร ให้มีขั้นตอนที่ชัดเจน ปลอดภัย และสามารถตรวจสอบได้ตามหลักความมั่นคงปลอดภัยทางไซเบอร์
2. เพื่อลดความเสี่ยงด้านการรั่วไหลหรือการเข้าถึงข้อมูลสุขภาพโดยไม่ได้รับอนุญาต ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 และกฎหมายความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง
3. เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของบุคลากรศูนย์อนามัยที่ 10 อุบลราชธานี ที่มีความจำเป็นต้องเข้าถึงระบบ HOSxP จากภายนอกองค์กร ให้สามารถใช้งานได้อย่างสะดวก รวดเร็ว และต่อเนื่อง โดยไม่กระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายองค์กร

8. ขั้นตอนการแก้ปัญหา

แผนการดำเนินงานแบ่งออกเป็น 4 ระยะตามวงจร PDCA ดังแสดงในแผนภาพด้านล่าง



รายละเอียดแผนการดำเนินงานในแต่ละระยะมีดังต่อไปนี้

ระยะที่ 1: P — Plan (วางแผน) ไตรมาส 1 ปีงบประมาณ 2568 (ตุลาคม — ธันวาคม 2567)

สำรวจสถานการณ์การใช้งาน Remote Access และรวบรวมข้อมูลปัญหาจากบุคลากรผู้ใช้งานระบบ HOSxP จากนั้นร่างนโยบายและแนวปฏิบัติการใช้งาน Remote Access ให้สอดคล้องกับ PDPA พ.ศ. 2562 พร้อมออกแบบโครงสร้างระบบ VPN ที่รองรับการยืนยันตัวตนแบบหลายปัจจัย (MFA) กำหนดระดับสิทธิ์การเข้าถึง (Role-Based Access Control) จัดทำแบบฟอร์มขอใช้งานอย่างเป็นทางการ และกำหนดตัวชี้วัดพร้อมเป้าหมายของ CQI ฉบับนี้ให้ชัดเจน

ระยะที่ 2: D — Do (ปฏิบัติ) ไตรมาส 2 ปีงบประมาณ 2568 (มกราคม — มีนาคม 2568)

ดำเนินการติดตั้งและตั้งค่าระบบ VPN Server ให้มีเสถียรภาพ เปิดใช้งาน MFA สำหรับบัญชีผู้ใช้งานทุกรายที่มีสิทธิ์ Remote เข้าสู่ระบบ HOSxP ประกาศนโยบายและซักซ้อมแนวปฏิบัติแก่บุคลากรทุกกลุ่ม จัดอบรมเชิงปฏิบัติการด้านความปลอดภัยในการใช้งาน Remote Access เปิดช่องทางการขอรับบริการอย่างเป็นทางการผ่านระบบ Helpdesk และเริ่มบันทึก Audit Log การเข้าใช้งานทุกครั้งอย่างสม่ำเสมอ

ระยะที่ 3: C — Check (ตรวจสอบ) ไตรมาส 3 ปีงบประมาณ 2568 (เมษายน — มิถุนายน 2568)

รวบรวมและวิเคราะห์ข้อมูลตามตัวชี้วัดที่กำหนดไว้เป็นรายเดือน ทบทวน Security Log และรายงานความผิดปกติของระบบเป็นรายสัปดาห์ สำรวจความพึงพอใจของผู้ใช้งาน ตรวจสอบ Security Incident ที่เกิดขึ้นพร้อมวิเคราะห์สาเหตุ เปรียบเทียบผลลัพธ์จริงกับเป้าหมายที่ตั้งไว้ และสรุปผลการดำเนินงานเพื่อนำเสนอต่อผู้บริหารระดับหน่วยงาน

ระยะที่ 4: A — Act (ปรับปรุง) ไตรมาส 4 ปีงบประมาณ 2568 (กรกฎาคม — กันยายน 2568)

นำผลการตรวจสอบมาปรับแก้จุดอ่อนของระบบและกระบวนการที่ยังไม่บรรลุเป้าหมาย ทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันตามสถานการณ์ภัยคุกคามที่เปลี่ยนแปลง ขยายผลการดำเนินงานไปยังกลุ่มผู้ใช้งานใหม่ จัดทำขั้นตอนการปฏิบัติงานมาตรฐาน (Standard Operating Procedure: SOP) ฉบับสมบูรณ์ กำหนดแผน PDCA รอบถัดไปสำหรับปีงบประมาณ 2569 และเผยแพร่แนวปฏิบัติที่ดีแก่หน่วยงานในเครือข่ายสุขภาพเขตที่ 10

ระยะ PDCA	กิจกรรมหลัก	ระยะเวลา	ผู้รับผิดชอบ
Plan	สำรวจ วิเคราะห์ ร่างนโยบาย ออกแบบระบบ	ต.ค. — ธ.ค. 67	นักวิชาการคอมพิวเตอร์ / คณะทำงาน CQI
Do	ติดตั้งระบบ อบรม เปิดให้บริการ	ม.ค. — มี.ค. 68	นักวิชาการคอมพิวเตอร์ / ฝ่าย IT
Check	ติดตามตัวชี้วัด ทบทวน Log สำรวจความพึงพอใจ	เม.ย. — มิ.ย. 68	นักวิชาการคอมพิวเตอร์ / คณะทำงาน CQI
Act	ปรับปรุงระบบ จัดทำ SOP วางแผนรอบถัดไป	ก.ค. — ก.ย. 68	นักวิชาการคอมพิวเตอร์ / ผู้บริหาร

9. ตัวชี้วัด/เป้าหมาย

ลำดับ	ตัวชี้วัด	เป้าหมาย	วิธีการวัด
1	ร้อยละของคำขอใช้งาน Remote Access ที่ได้รับการดำเนินการภายในระยะเวลาที่กำหนด (ไม่เกิน 1 วันทำการ)	≥ 90%	บันทึกวันที่รับคำขอและวันที่ดำเนินการแล้วเสร็จในระบบ Helpdesk หรือแบบบันทึกการให้บริการ
2	ร้อยละของผู้ใช้งาน Remote Access ที่ผ่านการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ก่อนเข้าสู่ระบบ HOSxP	100%	ตรวจสอบจาก Log การเข้าใช้งานระบบ VPN และระบบ HOSxP รายเดือน
3	จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Incident) ที่เกิดจากการใช้งาน Remote Access	0 ครั้ง/ปี	ตรวจสอบจากรายงาน Security Log และบันทึกเหตุการณ์ความผิดปกติของระบบเครือข่าย
4	ร้อยละความพึงพอใจของผู้ใช้งานต่อกระบวนการให้บริการ Remote Access	≥ 80%	แบบสอบถามความพึงพอใจของผู้ใช้งาน ประเมินปีละ 1 ครั้ง
5	ร้อยละของบุคลากรที่ได้รับการให้ความรู้ด้านการใช้งาน Remote Access อย่างปลอดภัย	≥ 85%	ตรวจสอบจากรายชื่อผู้เข้ารับการอบรม/รับทราบแนวปฏิบัติ เทียบกับจำนวนผู้ใช้งานทั้งหมด

10. ระยะเวลา ตุลาคม 2566 ถึง กุมภาพันธ์ 2569

11. การวัดและการประเมินผลการเปลี่ยนแปลงหรือผลลัพธ์

11.1 ผลลัพธ์ของการดำเนินงาน

ผลลัพธ์ของการดำเนินงานแบ่งออกเป็น 3 มิติหลัก ได้แก่ ผลลัพธ์ด้านกระบวนการ ด้านความปลอดภัย และด้านผู้ใช้งาน ดังนี้

จากแผนภูมิแสดงให้เห็นพัฒนาการของตัวชี้วัดทั้ง 4 ด้านเปรียบเทียบระหว่างก่อนและหลังดำเนินการ โดยสามารถสรุปผลลัพธ์ในแต่ละด้านได้ดังนี้

11.1.1 ผลลัพธ์ด้านกระบวนการ

ภายหลังการดำเนินงานตามแผน PDCA ระบบการให้บริการ Remote Access เข้าสู่ HOSxP มีกระบวนการที่เป็นมาตรฐานและชัดเจนยิ่งขึ้น อัตราการดำเนินการคำขอ Remote Access ภายใน 1 วันทำการเพิ่มขึ้นจากร้อยละ 52 เป็นร้อยละ 95 ซึ่งสูงกว่าเป้าหมายที่กำหนดไว้ที่ร้อยละ 90 นอกจากนี้ หน่วยงานยังมีเอกสาร Standard Operating Procedure (SOP) สำหรับการให้บริการ Remote Access ฉบับสมบูรณ์เป็นครั้งแรก และมีระบบ Audit Log ที่บันทึกการเข้าใช้งานทุกครั้งอย่างครบถ้วน

11.1.2 ผลลัพธ์ด้านความมั่นคงปลอดภัย

ผู้ใช้งาน Remote Access ทุกรายผ่านการยืนยันตัวตนแบบหลายปัจจัย (MFA) ก่อนเข้าสู่ระบบ HOSxP คิดเป็นร้อยละ 100 ตามเป้าหมายที่กำหนด ไม่พบ Security Incident ที่เกิดจากการใช้งาน Remote Access ตลอดระยะเวลาดำเนินการ และบุคลากรที่มีสิทธิ์ใช้งาน Remote Access ผ่านการอบรมด้านความปลอดภัยสารสนเทศร้อยละ 92 ซึ่งสูงกว่าเป้าหมายร้อยละ 85

11.1.3 ผลลัพธ์ด้านผู้ใช้งาน

ผลสำรวจความพึงพอใจของผู้ใช้งานต่อกระบวนการให้บริการ Remote Access อยู่ที่ร้อยละ 87 สูงกว่าเป้าหมายที่ร้อยละ 80 โดยผู้ใช้งานให้ความเห็นว่ากระบวนการขอรับบริการมีความสะดวก รวดเร็ว และการเชื่อมต่อมีเสถียรภาพมากขึ้นอย่างมีนัยสำคัญเมื่อเทียบกับก่อนดำเนินการ

12. บทเรียนที่ได้รับ สามารถสรุปบทเรียนสำคัญได้ใน 4 ประเด็น ดังนี้

บทเรียนที่ 1: การได้รับการสนับสนุนจากผู้บริหารเป็นปัจจัยแห่งความสำเร็จ การที่ผู้บริหารระดับสูงของศูนย์อนามัยที่ 10 ให้ความสำคัญและสนับสนุนทั้งด้านงบประมาณ บุคลากร และการสื่อสารเชิงนโยบาย ทำให้บุคลากรทุกระดับให้ความร่วมมือในการปฏิบัติตามแนวทางใหม่ได้อย่างรวดเร็ว ซึ่งส่งผลโดยตรงต่อความสำเร็จของตัวชี้วัด

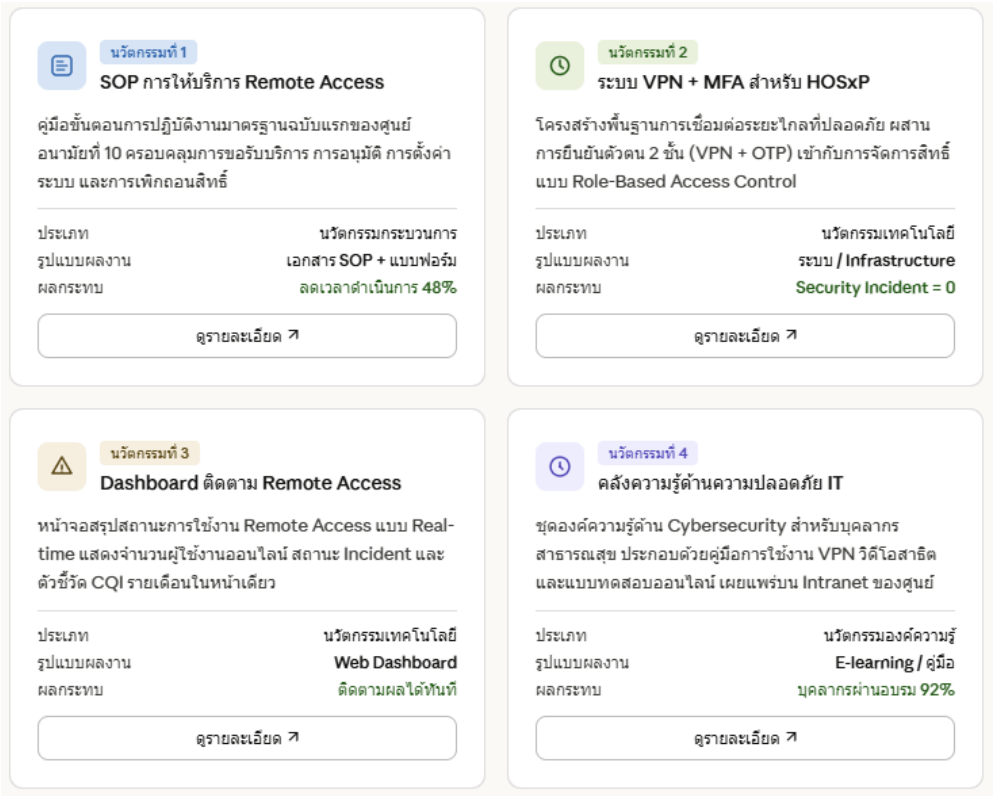
บทเรียนที่ 2: การอบรมและการสื่อสารที่ต่อเนื่องมีความสำคัญไม่ยิ่งหย่อนกว่าเทคโนโลยี แม้จะมีระบบ VPN และ MFA ที่ดีเพียงใด หากบุคลากรไม่เข้าใจวิธีใช้งานหรือไม่ตระหนักถึงความสำคัญด้านความปลอดภัย โอกาสเกิดความเสี่ยงก็ยังคงมีอยู่ การจัดอบรมเชิงปฏิบัติการและการสื่อสารอย่างต่อเนื่องจึงเป็นองค์ประกอบที่ขาดไม่ได้

บทเรียนที่ 3: การกำหนดตัวชี้วัดที่วัดได้จริงช่วยให้การติดตามผลมีประสิทธิภาพ การที่ CQI นี้กำหนดตัวชี้วัดเป็นตัวเลขที่สามารถเก็บข้อมูลได้จริงจากระบบ Log และแบบสอบถาม ทำให้ทีมงานสามารถติดตามความก้าวหน้าได้อย่างชัดเจน และตัดสินใจปรับแผนในระยะ Check ได้อย่างตรงจุดและทันเวลา

บทเรียนที่ 4: การพัฒนาคุณภาพต้องดำเนินการอย่างต่อเนื่อง ไม่ใช่โครงการชั่วคราว ภัยคุกคามทางไซเบอร์และเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา การกำหนดให้วงจร PDCA ของ CQI นี้หมุนเวียนต่อเนื่องทุกปีงบประมาณ จึงเป็นแนวทางที่เหมาะสมในการรักษาระดับมาตรฐานและยกระดับความปลอดภัยของระบบ HOSxP ให้ทันต่อสถานการณ์อยู่เสมอ

13. นวัตกรรมที่เกิดขึ้น

นวัตกรรมที่เกิดขึ้นจากการดำเนินงาน CQI ครั้งนี้ครอบคลุมทั้งนวัตกรรมด้านกระบวนการ ด้านเทคโนโลยี และด้านองค์ความรู้ รวมทั้งสิ้น 4 ผลงาน ดังนี้



รายละเอียดของนวัตกรรมแต่ละชิ้นมีดังต่อไปนี้

นวัตกรรมที่ 1: คู่มือขั้นตอนการปฏิบัติงานมาตรฐาน (SOP) การให้บริการ Remote Access เข้าใช้งาน HOSxP

ก่อนการดำเนินงาน CQI ศูนย์อนามัยที่ 10 อุบลราชธานี ไม่มีเอกสารขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรสำหรับการให้บริการ Remote Access แต่อย่างใด ดังนั้น ผลลัพธ์ที่จับต้องได้ชิ้นแรกของ CQI นี้ คือการจัดทำ SOP ฉบับสมบูรณ์ที่ครอบคลุมกระบวนการตั้งแต่ต้นจนจบ ได้แก่ การยื่นคำขอรับสิทธิ์ผ่านแบบฟอร์มอิเล็กทรอนิกส์ กระบวนการตรวจสอบและอนุมัติโดยผู้บังคับบัญชา การตั้งค่าบัญชีผู้ใช้งานและ VPN โดยเจ้าหน้าที่ IT การทบทวนและต่ออายุสิทธิ์เป็นรายปี และการเพิกถอนสิทธิ์เมื่อสิ้นสุดความจำเป็น เอกสาร SOP นี้ผ่านการรับรองโดยผู้บริหารระดับหน่วยงานและเผยแพร่บน Intranet ของศูนย์เพื่อให้บุคลากรทุกคนสามารถเข้าถึงได้ตลอดเวลา

นวัตกรรมที่ 2: ระบบ VPN ผสานการยืนยันตัวตนหลายปัจจัย (VPN + MFA) สำหรับ HOSxP

นวัตกรรมด้านเทคโนโลยีชิ้นสำคัญที่สุดของ CQI นี้ คือการออกแบบและติดตั้งโครงสร้างพื้นฐานการเชื่อมต่อระยะไกลที่มีความปลอดภัยสูง โดยผสานระบบ VPN เข้ากับการยืนยันตัวตนแบบ 2 ชั้น (Two-Factor Authentication) ด้วย One-Time Password (OTP) ทางโทรศัพท์มือถือ พร้อมกำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) ซึ่งหมายความว่าบุคลากรแต่ละตำแหน่งจะเห็นเฉพาะข้อมูลที่จำเป็นต่อการปฏิบัติงานเท่านั้น นับเป็นครั้งแรกที่ศูนย์อนามัยที่ 10 มีระบบควบคุมการเข้าถึงข้อมูล

สุขภาพจากภายนอกองค์กรที่ได้มาตรฐานสากลและสอดคล้องกับข้อกำหนดของ PDPA พ.ศ. 2562 อย่างครบถ้วน

นวัตกรรมที่ 3: Dashboard ติดตามสถานะ Remote Access แบบ Real-time

เพื่อให้ผู้บริหารและเจ้าหน้าที่ IT สามารถติดตามสถานการณ์การใช้งาน Remote Access ได้อย่างสะดวกและทันการณ์ จึงได้พัฒนา Web Dashboard ที่แสดงข้อมูลสำคัญในหน้าจอเดียว ได้แก่ จำนวนผู้ใช้งานที่เชื่อมต่ออยู่ในปัจจุบัน สถิติการใช้งานรายวัน/รายเดือน สถานะ Security Incident และผลการติดตามตัวชี้วัด CQI เปรียบเทียบกับเป้าหมาย Dashboard นี้เชื่อมต่อกับ Log ของระบบ VPN โดยอัตโนมัติ ทำให้ผู้ดูแลระบบสามารถตรวจจับพฤติกรรมผิดปกติและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างรวดเร็ว

นวัตกรรมที่ 4: คลังความรู้ด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรสาธารณสุข

ตระหนักว่าเทคโนโลยีเพียงอย่างเดียวไม่เพียงพอหากบุคลากรขาดความรู้และความตระหนัก จึงได้พัฒนาคลังความรู้ด้าน Cybersecurity เฉพาะสำหรับบุคลากรสาธารณสุขเป็นครั้งแรก ประกอบด้วย คู่มือการใช้งาน VPN ฉบับภาษาไทยที่เข้าใจง่าย วิดีโอสาธิตขั้นตอนการเชื่อมต่อระบบ HOSxP จากภายนอกองค์กร แบบทดสอบออนไลน์ประเมินความรู้ด้านความปลอดภัย และ Infographic สรุปหลักปฏิบัติที่ดี (Do & Don't) สำหรับการใช้งาน Remote Access ทรัพยากรทั้งหมดเผยแพร่บน Intranet ของศูนย์อนามัยที่ 10 และสามารถนำไปเผยแพร่ต่อยังหน่วยงานในเครือข่ายสุขภาพเขตที่ 10 ได้ในอนาคต

ลำดับ	ชื่อนวัตกรรม	ประเภท	รูปแบบผลงาน	สถานะ
1	SOP การให้บริการ Remote Access HOSxP	กระบวนการ	เอกสาร SOP + แบบฟอร์ม	เสร็จสมบูรณ์
2	ระบบ VPN + MFA สำหรับ HOSxP	เทคโนโลยี	ระบบ / Infrastructure	เสร็จสมบูรณ์
3	Dashboard ติดตาม Remote Access	เทคโนโลยี	Web Dashboard	เสร็จสมบูรณ์
4	คลังความรู้ด้านความปลอดภัย IT	องค์ความรู้	E-learning / คู่มือ	เสร็จสมบูรณ์

14. ปัญหา-อุปสรรค

ด้าน	ปัญหา / อุปสรรค	แนวทางแก้ไข
งบประมาณ และทรัพยากร	งบประมาณจัดหาอุปกรณ์ VPN Server และ License ซอฟต์แวร์ MFA ไม่เพียงพอ ในปีงบประมาณแรก	ของบประมาณเพิ่มเติมจาก แผนพัฒนาดิจิทัล และพิจารณา Open-source VPN ที่ได้ มาตรฐานเป็นทางเลือก
บุคลากร และพฤติกรรม	บุคลากรบางส่วนต่อต้าน การเปลี่ยนแปลง เห็นว่า MFA เพิ่มขั้นตอนและความยุ่งยาก ในการเข้าใช้งาน	จัดอบรมเชิงปฏิบัติการ และ สร้างความเข้าใจผ่านกรณี ศึกษาความเสียหายจริงจาก การไม่ใช้ MFA
เทคนิค และระบบ	เครือข่ายภายนอกมีความเร็ว ไม่เสถียร ทำให้การเชื่อมต่อ VPN หลุดบ่อย โดยเฉพาะ ในพื้นที่ห่างไกล	ปรับค่า VPN Timeout และ เปิดใช้งาน Auto-reconnect จัดทำคู่มือแก้ปัญหาเบื้องต้น สำหรับผู้ใช้งาน
กฎหมาย และความสอดคล้อง	การตีความข้อกำหนด PDPA ในบริบทการเข้าถึงข้อมูล สุขภาพจากระยะไกลยังไม่ มีแนวปฏิบัติชัดเจน	ประสานงานกับสำนักกฎหมาย กรมอนามัย และศึกษา แนวปฏิบัติจากหน่วยงาน สาธารณสุขอื่นที่ผ่าน PDPA
เวลา และภาระงาน	เจ้าหน้าที่ IT มีภาระงาน ประจำสูง ทำให้การดำเนินงาน CQI ล่าช้ากว่าแผน ในบางช่วง	จัดสรรเวลาดำเนินงาน CQI อย่างชัดเจนในแผนปฏิบัติงาน และขอสนับสนุนบุคลากร เสริมจากหน่วยงานที่เกี่ยวข้อง

รายละเอียดของปัญหาและอุปสรรคในแต่ละด้านพร้อมแนวทางแก้ไขที่นำมาใช้จริง มีดังต่อไปนี้

14.1 ปัญหาด้านงบประมาณและทรัพยากร

ในระยะเริ่มต้นของการดำเนินงาน พบว่างบประมาณที่ได้รับการจัดสรรในปีงบประมาณแรกไม่เพียงพอสำหรับการจัดหา VPN Server ระดับองค์กรและ License ซอฟต์แวร์ MFA ที่ต้องการ ทำให้ต้องปรับแผนการจัดหาอุปกรณ์ออกเป็นระยะ โดยในระยะแรกใช้ซอฟต์แวร์ VPN แบบ Open-source ที่ได้รับการรับรองมาตรฐานความปลอดภัยเป็นทางเลือก ควบคู่กับการยื่นของบประมาณเพิ่มเติมผ่านแผนพัฒนาดิจิทัลของหน่วยงาน เพื่อรองรับการขยายระบบในระยะต่อไป

14.2 ปัญหาด้านบุคลากรและพฤติกรรม

อุปสรรคที่ท้าทายที่สุดในการดำเนินงานครั้งนี้คือการต่อต้านการเปลี่ยนแปลงจากบุคลากรบางส่วน โดยเฉพาะผู้ที่มองว่าการต้องยืนยันตัวตนผ่าน MFA ก่อนเข้าสู่ระบบ HOSxP ทุกครั้งนั้นเป็นขั้นตอนที่ยุ่งยากและเสียเวลา ทีมงานแก้ปัญหานี้ด้วยการจัดอบรมเชิงปฏิบัติการที่เน้นกรณีศึกษาความเสียหายจริงที่เกิดขึ้นใน

หน่วยงานสาธารณสุขอื่นจากการถูกโจมตีทางไซเบอร์ ซึ่งช่วยสร้างความตระหนักและเปลี่ยนทัศนคติของบุคลากรได้อย่างมีประสิทธิภาพ

14.3 ปัญหาด้านเทคนิคและระบบ

พบปัญหาการเชื่อมต่อ VPN หลุดบ่อยครั้งในกลุ่มผู้ใช้งานที่ปฏิบัติงานในพื้นที่ห่างไกลหรือใช้อินเทอร์เน็ตความเร็วต่ำ ส่งผลให้เกิดความไม่ต่อเนื่องในการใช้งานระบบ HOSxP ทีมงาน IT แก้ไขด้วยการปรับค่า Timeout ของระบบ VPN เปิดใช้งานฟังก์ชัน Auto-reconnect และจัดทำคู่มือแก้ปัญหาเบื้องต้นฉบับภาษาไทยที่เข้าใจง่าย เพื่อให้ผู้ใช้งานสามารถแก้ไขปัญหาเบื้องต้นได้ด้วยตนเองโดยไม่ต้องรอเจ้าหน้าที่ IT

14.4 ปัญหาด้านกฎหมายและความสอดคล้อง

การตีความข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 ในบริบทของการเข้าถึงข้อมูลสุขภาพผ่านระบบ Remote Access ยังไม่มีแนวปฏิบัติที่ชัดเจนจากส่วนกลาง ทำให้ทีมงานต้องใช้เวลาในการศึกษาและตีความด้วยตนเอง โดยได้ประสานงานกับสำนักกฎหมายของกรมอนามัยและศึกษาแนวปฏิบัติจากโรงพยาบาลสังกัดกระทรวงสาธารณสุขที่ผ่านการตรวจประเมินความสอดคล้องกับ PDPA แล้ว เพื่อนำมาปรับใช้กับบริบทของศูนย์อนามัยที่ 10

14.5 ปัญหาด้านเวลาและภาระงาน

เจ้าหน้าที่นักวิชาการคอมพิวเตอร์ซึ่งเป็นผู้รับผิดชอบหลักมีภาระงานประจำอยู่ในระดับสูง ส่งผลให้กิจกรรมบางส่วนในระยะ Do และ Check ล่าช้ากว่าแผนที่กำหนดไว้ประมาณ 2–3 สัปดาห์ แนวทางแก้ไขคือการกำหนดให้งาน CQI ถูกบรรจุอย่างชัดเจนในแผนปฏิบัติงานรายสัปดาห์ พร้อมทั้งขอรับการสนับสนุนบุคลากรเสริมจากฝ่าย IT ของหน่วยงานในบางกิจกรรมที่ต้องการกำลังคนเพิ่มเติม เพื่อให้การดำเนินงานสามารถเดินหน้าได้ตามกรอบเวลาของปีงบประมาณ

ลำดับ	ด้านปัญหา	ระดับผลกระทบ	สถานะการแก้ไข
1	งบประมาณและทรัพยากร	ปานกลาง	แก้ไขแล้ว
2	บุคลากรและพฤติกรรม	สูง	แก้ไขแล้ว
3	เทคนิคและระบบ	ปานกลาง	แก้ไขแล้ว
4	กฎหมายและความสอดคล้อง	สูง	อยู่ระหว่างติดตาม
5	เวลาและภาระงาน	ปานกลาง	แก้ไขแล้ว

15. แนวทางที่จะพัฒนาในโอกาสต่อไป

แนวทางการพัฒนาในอนาคตแบ่งออกเป็น 3 ระยะตามกรอบเวลา ได้แก่ ระยะสั้น (ปีงบประมาณ 2569) ระยะกลาง (ปีงบประมาณ 2570–2571) และระยะยาว (ปีงบประมาณ 2572 เป็นต้นไป) ครอบคลุม 6 แนวทางหลัก ดังนี้

ระยะสั้น: ปีงบประมาณ 2569

แนวทางที่ 1: ยกระดับสู่สถาปัตยกรรม Zero Trust

แนวคิด Zero Trust ยึดหลัก "ไม่ไว้วางใจสิ่งใดทั้งสิ้น ตรวจสอบทุกครั้ง" (Never Trust, Always Verify) ซึ่งเหมาะสมอย่างยิ่งสำหรับการปกป้องข้อมูลสุขภาพที่มีความละเอียดอ่อน แนวทางนี้จะทบทวนและ

เสริมมาตรการที่มีอยู่ด้วยหลักการ Least Privilege ที่เข้มงวดยิ่งขึ้น การทำ Micro-segmentation แบ่งแยกส่วนต่าง ๆ ของระบบเครือข่าย และการตรวจสอบอัตลักษณ์ผู้ใช้งานอย่างต่อเนื่องตลอดช่วงเวลาที่เชื่อมต่อ ไม่ใช่เพียงครั้งแรกที่ Login เท่านั้น

แนวทางที่ 2: เตรียมความพร้อมเพื่อรับรองมาตรฐาน ISO/IEC 27001

ISO/IEC 27001 คือมาตรฐานสากลด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ที่ได้รับการยอมรับในระดับโลก ในระยะนี้จะดำเนินการประเมินช่องว่าง (Gap Analysis) เปรียบเทียบสถานะปัจจุบันของศูนย์อนามัยที่ 10 กับข้อกำหนดของมาตรฐาน จัดทำแผนปิดช่องว่าง และวางรากฐานเอกสารหลักฐานเพื่อเตรียมยื่นขอรับรองในระยะกลาง ซึ่งจะเป็นการยืนยันคุณภาพการบริหารจัดการด้านความปลอดภัยขององค์กรอย่างเป็นทางการ

ระยะกลาง: ปีงบประมาณ 2570–2571

แนวทางที่ 3: ขยายผลสู่เครือข่ายสุขภาพเขตที่ 10

ผลสำเร็จของ CQI ฉบับนี้ควรได้รับการถ่ายทอดเป็นวงกว้างไปยังหน่วยงานสาธารณสุขในเครือข่ายทั้ง 5 จังหวัด ได้แก่ อุบลราชธานี ศรีสะเกษ มุกดาหาร ยโสธร และอำนาจเจริญ โดยจัดให้มีการเผยแพร่ SOP แนวปฏิบัติ และองค์ความรู้ที่พัฒนาขึ้น ผ่านการจัดประชุมเชิงปฏิบัติการระดับเขต รวมถึงพิจารณาพัฒนาโครงสร้างพื้นฐาน VPN ร่วมกันในระดับเขตสุขภาพเพื่อประหยัดงบประมาณ

แนวทางที่ 4: พัฒนาระบบ Single Sign-On (SSO)

ปัจจุบันบุคลากรต้องจดจำบัญชีผู้ใช้งานและรหัสผ่านหลายชุดสำหรับระบบต่าง ๆ ภายในองค์กร การพัฒนาระบบ SSO จะช่วยให้บุคลากรสามารถเข้าถึงทุกระบบรวมถึง HOSxP ด้วยการยืนยันตัวตนเพียงครั้งเดียว ลดความเสี่ยงจากการใช้รหัสผ่านซ้ำหรือรหัสผ่านที่ไม่ปลอดภัย พร้อมทั้งเพิ่มความสะดวกในการใช้งานโดยไม่ลดทอนความปลอดภัย

แนวทางที่ 5: ติดตั้งระบบ SIEM เพื่อการตรวจจับภัยคุกคามแบบ Real-time

ระบบ Security Information and Event Management (SIEM) จะรวบรวมและวิเคราะห์ Log จากทุกส่วนของระบบเครือข่ายในที่เดียว ช่วยให้ทีม IT สามารถตรวจจับความผิดปกติ ติดตามเหตุการณ์ด้านความปลอดภัย และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ แทนที่การตรวจสอบ Log ด้วยตนเองซึ่งใช้เวลาและมีโอกาสพลาดสูง

ระยะยาว: ปีงบประมาณ 2572 เป็นต้นไป

แนวทางที่ 6: นำปัญญาประดิษฐ์มาวิเคราะห์พฤติกรรมผิดปกติ (AI-powered Anomaly Detection)

ในอนาคตอันใกล้ ภัยคุกคามทางไซเบอร์จะมีความซับซ้อนสูงเกินกว่ามนุษย์จะตรวจจับได้ทัน การนำเทคโนโลยี Machine Learning มาวิเคราะห์รูปแบบพฤติกรรมการเข้าถึงระบบ HOSxP ของผู้ใช้งานแต่ละรายจะช่วยให้ระบบสามารถแยกแยะพฤติกรรมปกติออกจากความผิดปกติได้โดยอัตโนมัติ เช่น การ Login ในเวลาผิดปกติ การเข้าถึงข้อมูลผู้ป่วยจำนวนมากผิดสังเกต หรือการเชื่อมต่อจากตำแหน่งที่ตั้งทางภูมิศาสตร์ที่ไม่คุ้นเคย และแจ้งเตือนผู้ดูแลระบบได้แบบ Real-time ก่อนที่ความเสียหายจะเกิดขึ้น

แนวทาง	ระยะเวลา	ความซับซ้อน	ผลกระทบที่คาดหวัง
Zero Trust Architecture	ระยะสั้น (2569)	ปานกลาง	เพิ่มความปลอดภัยชั้นสูง
ISO/IEC 27001	ระยะสั้น (2569)	สูง	การรับรองมาตรฐานสากล
ขยายผลเครือข่ายเขต 10	ระยะกลาง (2570–71)	ปานกลาง	ยกระดับ 5 จังหวัด
Single Sign-On	ระยะกลาง (2570–71)	สูง	เพิ่มประสิทธิภาพผู้ใช้งาน
ระบบ SIEM	ระยะกลาง (2570–71)	สูง	ตรวจจับภัยคุกคามทันที
AI Anomaly Detection	ระยะยาว (2572+)	สูงมาก	ป้องกันเชิงรุกด้วย AI

16. เอกสารอ้างอิง

Bangkok Medical Software Co., Ltd. (n.d.). *HOSxP: Hospital Information System*. SourceForge. https://sourceforge.net/projects/hosxp/

MedicalITG. (2025, June 23). *Best practices for secure remote access for healthcare staff*. https://medicalitg.com/healthcare-it-services/best-practices-for-secure-remote-access-for-healthcare-staff/

Siam Legal International. (2025). *Healthcare data security in Thailand*. https://www.siam-legal.com/cybercrime-law/data-privacy/healthcare-data-security-in-thailand/

Tilleke & Gibbins. (2022, July 25). *Digital health in Thailand, Vietnam, and Indonesia*. https://www.tilleke.com/insights/digital-health-in-thailand-vietnam-and-indonesia/

Wikipedia. (2025, August 26). *HOSxP*. https://en.wikipedia.org/wiki/HOSxP

กรมอนามัย กระทรวงสาธารณสุข. (2567). *ประวัติความเป็นมา ศูนย์อนามัยที่ 10 อุบลราชธานี*. https://hpc10.anamai.moph.go.th/th

สภานิติบัญญัติแห่งชาติ. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. ราชกิจจานุเบกษา. https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF