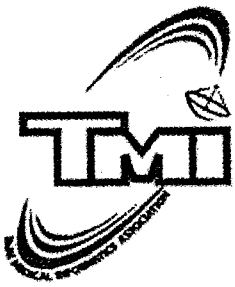
วพ. มหิดล

แนวทางการพัฒนาคุณภาพ
ระบบเทคโนโลยีสารสนเทศโรงพยาบาล



ตาม Thai Medical Informatics – TMI
Hospital IT Maturity Model

แนวทางการพัฒนาคุณภาพ
ระบบเทคโนโลยีสารสนเทศโรงพยาบาล
ตาม Thai Medical Informatics – TMI
Hospital IT Maturity Model

บรรณาธิการ

นายแพทย์ ชุษณะ มะกรสาร

นายแพทย์ วรรษา เปาอินทร์

ISBN : 978-616-91475-3-4

พิมพ์ครั้งที่ 1 มิถุนายน พ.ศ. 2561 1,000 เล่ม

ราคา 200 บาท

จัดทำโดยสมาคมเวชสารสนเทศไทย

สารบัญ

คำนำ

สมาคมเวชสารสนเทศไทย (Thai Medial Informatics Association – TMI) ได้เริ่มกิจกรรมส่งเสริมการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลตั้งแต่ ปี พ.ศ. 2550 โดยได้สร้างกรอบแนวทางการพัฒนาคุณภาพคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล (Hospital Information Technology Quality Improvement Framework – HITQIF) เพื่อใช้เป็นกรอบแนวทางให้โรงพยาบาลได้สำรวจตนเองและวางแนวทางพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศ

ต่อมาในปี พ.ศ. 2557 สมาคมเวชสารสนเทศได้ลงนามบันทึกข้อตกลงร่วมกับ สถาบันพัฒนาและรับรองคุณภาพสถานพยาบาล (The Healthcare Accreditation Institute –HA) เพื่อร่วมกันพัฒนาแนวทางตรวจสอบและรับรองคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล และจัดทำรูปแบบระดับการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย (TMI Hospital IT Maturity Model) ทำให้เริ่มมีการรับรองคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลตั้งแต่ปี พ.ศ. 2557 เป็นต้นมา

ปลายปี พ.ศ. 2560 คณะกรรมการบริหารสมาคมเวชสารสนเทศไทยได้มีโอกาสนำเสนอกิจกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศโรงพยาบาลต่อ ฯพณฯ รัฐมนตรีว่าการกระทรวงสาธารณสุข ทำให้เกิดการสนับสนุนให้โรงพยาบาลในสังกัดกระทรวงสาธารณสุขดำเนินการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโดยทั่วกัน โดยเริ่มดำเนินการปี พ.ศ. 2561 เป็นต้นไป

การดำเนินการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลให้สำเร็จ จะต้องมีแนวทางที่ชัดเจนเพื่อให้ผู้ที่รับผิดชอบได้ดำเนินการกิจกรรมต่างๆให้ครบทุกด้านที่จำเป็น ในการนี้สมาคมจึงได้จัดทำคู่มือแนวทางการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลฉบับนี้ขึ้น เพื่อให้คณะทำงานของโรงพยาบาลได้ใช้เป็นแนวทางปฏิบัติ รวมทั้งเป็นคู่มือให้ผู้เยี่ยมสำรวจคุณภาพได้ใช้ในการติดตามการทำงานพัฒนาคุณภาพของโรงพยาบาลอีกด้วย

การพัฒนาแนวทางคุณภาพฉบับนี้จะสำเร็จไปไม่ได้ หากไม่ได้ตัวอย่างจากโรงพยาบาลที่เข้าร่วมโครงการพัฒนาคุณภาพระยะที่ 1 และ 2 ของสมาคมเวชสารสนเทศไทย ได้แก่ โรงพยาบาลหาดใหญ่ ละงู โรคผิวหนังเขตร้อนจังหวัดตรัง สุไหงโกลก น่าน แพร่ สมเด็จพระสังฆราชองค์ที่ 19 สมเด็จพระนางเจ้าสิริกิติ์ วัด

เพลง นครพนม คูเมือง บ้านใหม่ไชยพจน์ จึงขอขอบคุณผู้บริหารและทีมงานของโรงพยาบาลดังกล่าวที่ได้แบ่งปันต้นแบบความรู้อันมีค่า และได้นำตัวอย่างบางส่วนมาแสดงไว้ในคู่มือฉบับนี้ด้วย

การพัฒนาคู่มือฉบับนี้ ดำเนินไปในช่วงที่กำลังจะมีการรับรองคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลในระดับที่ 3 ของรูปแบบระดับการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล จึงอาจจะยังขาดเนื้อหาในส่วนตัวอย่างของผลการดำเนินการในระดับที่ 3 ซึ่งจะได้ดำเนินการปรับปรุงเนื้อหาให้ครอบคลุมมากขึ้นในการจัดพิมพ์ครั้งต่อไป สำหรับข้อผิดพลาดที่อาจเกิดขึ้นในการพิมพ์หรือตัวสะกด ความผิดพลาดในข้อความต่างๆ บรรณาธิการขอน้อมรับในการผิดพลาดและจะดำเนินการแก้ไขต่อไปในอนาคต

บรรณาธิการ
นายแพทย์ ชุษณะ มะกรสาร
นายแพทย์ วรรษา เปาอินทร์
มิถุนายน พ.ศ. 2561

TMI Hospital IT Maturity Model (March 2016)

System	Level 1	Level 2	Level 3
0. General Status	เริ่มมีทีมงานและกระบวนการจัดการให้เกิดคุณภาพ โดยเริ่มเห็นผลบางส่วน	ทีมงานจากฝ่ายต่าง ๆ (ฝ่ายบริหาร ผู้ปฏิบัติงานและฝ่าย IT) ร่วมกันดำเนินการพัฒนาอย่างต่อเนื่องและเชื่อมโยง ในสาขาต่าง ๆ เกิดระบบการพัฒนาคุณภาพด้าน IT	มีการพัฒนาคุณภาพอย่างกว้างขวางทั้งองค์กร เกิดการพัฒนาคุณภาพอย่างต่อเนื่องและเชื่อมโยง มีผู้รับผิดชอบในประเด็นสำคัญต่างโดยเฉพาะ เริ่มเกิดวัฒนธรรมคุณภาพ IT
1. IT Master Plan	แผน IT สอดคล้องกับแผนโรงพยาบาล ตอบสนองยุทธศาสตร์หลักของโรงพยาบาล มีกระบวนการพัฒนาแผนที่ได้มาตรฐาน	มีการดำเนินการตามแผน IT ที่สอดคล้องกับแผนโรงพยาบาล เกิดผลสำเร็จในบางโครงการ	มีการดำเนินการตามแผน IT ที่สอดคล้องกับแผนโรงพยาบาล เกิดผลสำเร็จ โดย IT เป็นเครื่องมือหลักในการผลักดันยุทธศาสตร์สำคัญของโรงพยาบาล
2. IT Risk Management System	มีการประเมินความเสี่ยงในระบบ IT ดำเนินการจัดการความเสี่ยงจนประเมินได้ว่าความเสี่ยงลดลง	นำผลการจัดการความเสี่ยงในรอบปีที่ผ่านมา มาใช้ปรับแผนการจัดการความเสี่ยงในปีต่อไป ทำให้ความเสี่ยงลดลงได้ต่อเนื่อง	มีกลไกการจัดการความเสี่ยงที่ดำเนินครบวงจร PDCA อย่างต่อเนื่อง ไม่พบความเสี่ยงที่จัดการได้และ ครอบคลุมความเสี่ยงที่มีผลกระทบต่อการดูแลผู้ป่วย
3. Information Security Management	มีนโยบายและระเบียบปฏิบัติด้านความมั่นคงในระบบ IT ผู้ที่เกี่ยวข้องรับทราบ เข้าใจ และปฏิบัติตามระเบียบปฏิบัติอย่างเคร่งครัด มีการจัดการ Data Center จนมั่นคงปลอดภัยทุกด้าน	มีการจัดการการเข้าถึงข้อมูลผู้ป่วยให้เข้าถึงได้เฉพาะผู้ที่รับผิดชอบการดูแลรักษาผู้ป่วยในช่วงดังกล่าวเท่านั้น ไม่มีการใช้ช่องทางที่ไม่มั่นคง (LINE, Social Media) ในการรับส่งข้อมูลผู้ป่วย และสอดคล้องกับกฎหมายที่เกี่ยวข้อง	มีกลไกการจัดการความมั่นคงที่ดำเนินครบวงจร PDCA อย่างต่อเนื่อง มีความสามารถในการตรวจจับการละเมิดความมั่นคง แก้ไขและกู้คืนระบบที่เสียหายได้อย่างรวดเร็ว

TMI Hospital IT Maturity Model (continue)

System	Level 1	Level 2	Level 3
4. Service Desk, Service Level Agreement, Incident and Problem Management	มีการจัด service desk มีการประกาศ SLA ในเรื่องที่สำคัญอย่างยิ่งสำหรับผู้ใช้ระบบ IT มีระบบเก็บข้อมูล IT Activity and Incident Report and Monitoring	ประกาศ SLA ที่สำคัญได้ครบทุกด้านการบริการ (Hardware, Software, Network, Data Service, New Requirement) มีข้อมูลในระบบ Incident และ Activity Monitoring มากกว่า 95% ของเหตุการณ์ เริ่มมีกระบวนการจัดการ Incident และ Problem Management	มี SLA ที่สอดคล้องกับกิจการหลัก มีกลไกการประเมินการให้บริการ Service Desk และผลการให้บริการตาม SLA นำผลการประเมิน มาใช้ปรับคุณภาพบริการ ที่ดำเนินครบวงจร PDCA อย่างต่อเนื่องผู้ใช้ระบบมีความพึงพอใจมาก
5. Clinical Data Quality Control	มีการเก็บข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยในทุกราย ไม่น้อยกว่าร้อยละ 80 มีระบบตรวจสอบคุณภาพความครบถ้วน และความถูกต้องของข้อมูล OPD, IPD	มีการเก็บข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยในทุกราย ไม่น้อยกว่าร้อยละ 95 เริ่มมีการจัดเก็บข้อมูลอยู่ในรูปแบบ Structured Data in database (Not Scanned Record)	มีข้อมูลที่สามารถนำมาวิเคราะห์เพื่อเพิ่มคุณภาพด้าน Quality and Safety of Care, Improve Clinical Outcomes

TMI Hospital IT Maturity Model (continue)

6. Software Development Quality Control (if available)	มีกระบวนการและ เอกสารการวิเคราะห์และออกแบบระบบที่สำคัญในโปรแกรมที่พัฒนาเอง ไม่น้อยกว่าร้อยละ 80	มีกระบวนการและเอกสารการวิเคราะห์และออกแบบระบบที่สำคัญในโปรแกรมที่พัฒนาเอง ทุกโปรแกรม มีการทำ Software Version Control มีการ Comment Source codes เริ่มมีกระบวนการตรวจสอบและทบทวนคุณภาพของโปรแกรม	มีกลไก Requirement Management, Project Management, Software Quality Assurance ในการพัฒนาโปรแกรมหลัก ทุก ๆโปรแกรม
7. Capacity Management and Change Management	มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis, มีการจัดทำแผนเพิ่มศักยภาพ ด้าน Hardware, Software, Network, People ware มีการกำหนดสมรรถนะที่จำเป็นของบุคลากรสำคัญในฝ่าย IT	มีการดำเนินการพัฒนาศักยภาพตามแผน เกิดผลสำเร็จในบางด้าน ใช้ข้อมูลตามสภาพการปฏิบัติจริงมาจัดทำแผนเพิ่มศักยภาพ เริ่มมีระบบ Change Management	มีกลไกการพัฒนาศักยภาพครบทุกด้าน ดำเนินครบวงจร PDCA อย่างต่อเนื่องพบความก้าวหน้าอย่างต่อเนื่อง มีระบบ Change Management ที่มีประสิทธิภาพ

บทที่ 1

การจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ

โดย นายแพทย์ชุษณะ มะกรสาร

การใช้เทคโนโลยีสารสนเทศย่อมมีจุดมุ่งหมายเพื่อให้องค์การ (โรงพยาบาล) สามารถบรรลุจุดมุ่งหมาย วิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่สำคัญ การที่เทคโนโลยีสารสนเทศจะตอบสนองต่อจุดมุ่งหมายดังกล่าว ย่อมต้องการแผนการที่ชัดเจน เปรียบเหมือนการสร้างบ้าน ย่อมต้องเริ่มจากการกำหนดความต้องการของบ้าน นำมาเขียนเป็นแบบพิมพ์เขียวในการสร้างบ้าน จึงจะสามารถดำเนินการก่อสร้างให้เป็นไปตามวัตถุประสงค์

แผนยุทธศาสตร์หรือแผนแม่บทเทคโนโลยีสารสนเทศ ย่อมใช้เพื่อเป็นแนวทางให้การนำ IT ไปใช้เพื่อเกิดประโยชน์สูงสุดต่อผู้ป่วย (และ stakeholder อื่นๆ) อย่างเหมาะสม โดยคำนึงถึงความเป็นไปได้ ความคุ้มค่า และความเสียหายที่จะเกิดขึ้น (ความเสี่ยง) โดยรวมคือการทำให้เกิด IT Governance ขึ้นในองค์การนั่นเอง

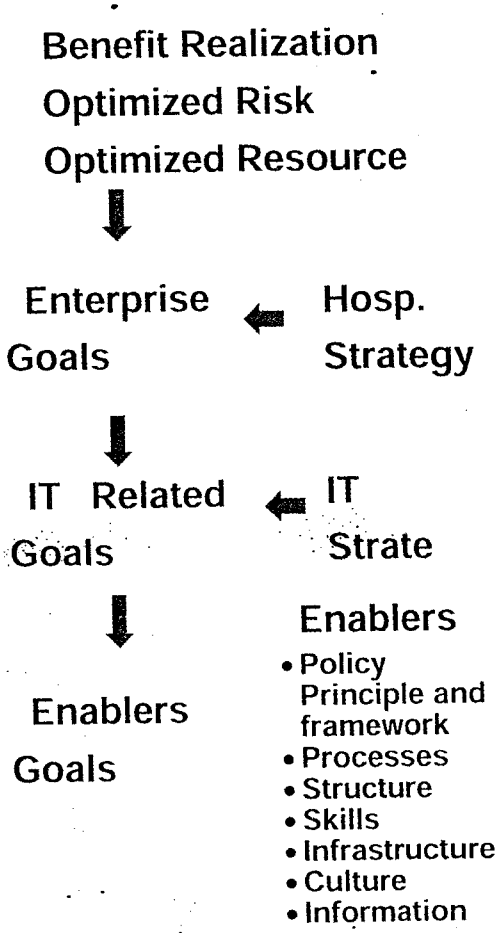
IT Governance

> **[Governance is] the set of *organizational regulations* and standards exercised by management to provide strategic direction and ensure that objectives are achieved, risks are managed appropriately, and resources are used responsibly**

ตามคำจำกัดความข้างต้น IT governance ก็คือรากฐานของการใช้ IT ให้เกิดประโยชน์อย่างคุ้มค่าเหมาะสมในองค์การ โดยมีหลักการที่สำคัญ 3 อย่างประกอบกันคือ

1. Benefit Realization - Stakeholder ได้รับประโยชน์ที่ต้องการ
2. Optimized Risks - ภายใต้ระดับความเสี่ยงที่เหมาะสม
3. Optimized Resource - ภายใต้ทรัพยากรที่เหมาะสม

โดยมี concept ของการเชื่อมโยงดังนี้



1. **Enterprise Goal** เป้าหมาย และยุทธศาสตร์ของโรงพยาบาลถูกกำหนดจากการทำแผนยุทธศาสตร์ที่ชัดเจน โดยคำนึงถึงหลักการที่สำคัญทั้ง 3 อย่างข้างต้น (หากเป้าหมายและแผนยุทธศาสตร์ของโรงพยาบาลมีความคลุมเครือ ย่อมสงผลให้แผนแม่บท IT ไม่มีความชัดเจนด้วย)
2. ถ่ายทอด (cascade) Enterprise Goal และ Strategy มาเป็น **IT Related Goal** หรือเป้าหมายของ IT
3. กำหนด **IT Strategy** ยุทธศาสตร์ด้าน IT จากเป้าหมายดังกล่าว
4. จาก IT Related Goal และ Strategy กำหนดเป็น **Enablers Goals**

<u>คุณค่าของเทคโนโลยีสารสนเทศ</u> **(the Ability of IT to Produce Business Value)**

ในการจัดทำแผนแม่บท IT มักพบเสมอๆ ว่าผู้เกี่ยวข้องโดยเฉพาะผู้บริหารมักนึกถึงคุณค่าของ IT มุ่งเน้นเพียงเรื่องการนำข้อมูลมาใช้ประโยชน์ในการบริหารจัดการ ซึ่งก็เป็นจริงตามนั้น แต่เมื่อคำนึงถึงการใช้ IT ให้เกิดประโยชน์ คุ้มค่า พาองค์การไปสู่เป้าหมายแล้ว IT สามารถสร้างประโยชน์ได้ในหลายรูปแบบ ซึ่งการจัดทำแผนควรคำนึงถึงประเด็นนี้ให้ชัดเจน

คุณค่าของ IT

- การสร้างคุณค่าให้องค์การ **(Value creation)**
  - ใช้ IT เป็นเครื่องมือสร้างคุณค่า **(enabler)**
  - ใช้ IT เป็นเครื่องมือปรับกระบวนการทำงาน **(process optimization)**
  - ใช้ IT เป็นเครื่องปรับองค์กร **(enterprise transformation)**
- ลดค่าใช้จ่าย เพิ่มประสิทธิภาพขององค์การ
- การใช้ข้อมูลเพื่อการบริหารจัดการ

จากคุณสมบัติของ IT ที่จัดการกับข้อมูลจำนวนมาก จัดเก็บ ค้นหา แลกเปลี่ยน ประมวลผลข้อมูลได้อย่างรวดเร็ว กว้างขวาง ทำให้สามารถใช้สร้างคุณค่าให้กับองค์การได้หลากหลาย

IT as Service Enabler กระบวนการทาง IT สร้างให้เกิดบริการ (service) ใหม่ๆ ได้หลากหลาย ซึ่งหากไม่มี IT จะไม่สามารถสร้างกระบวนการเหล่านั้นขึ้นได้ ตัวอย่างเช่น

- การเปิดบริการ satellite clinic โดยเชื่อมโยงกับข้อมูลหลักของโรงพยาบาลทำให้ผู้ป่วยมีข้อมูลเพียงชุดเดียว ทำให้ผู้ป่วยไม่ต้องมาแออัดที่โรงพยาบาล และสามารถ monitor ผลการตรวจของผู้ป่วยที่มีภาวะผิดปรกติได้อย่างรวดเร็ว เป็นต้น
- การใช้ mobile และ telemedicine
- การสร้างระบบ Clinical Decision Support ช่วยการตัดสินใจของแพทย์ เป็นต้น

Process Optimization เราสามารถใช้ IT ปรับกระบวนการทำงานเพื่อลดขั้นตอน เพิ่มคุณภาพ และประสิทธิภาพได้ เช่น การใช้ CPOE (Computerized Provider Order Entry) หมายถึงระบบสั่งการรักษา (รวมทั้งสั่งยา) ผ่านคอมพิวเตอร์ จากการศึกษาพบว่า การสังการรักษาผ่านคอมพิวเตอร์จะช่วยลดความผิดพลาดลงได้ถึง 60% เช่นการสั่งยาที่ผู้ป่วยแพ้ การสั่งยาหรือการรักษาซ้ำซ้อน การให้ยา 2 ตัวที่ไม่เข้ากัน เป็นต้น และหากใช้ร่วมกับ CDSS จะลดความผิดพลาดได้ถึง 75%

Enterprise Transformation IT สามารถช่วยปรับรื้อระบบการทำงานใหม่ (System Re-engineering) ได้ หากใช้โดยถูกต้องจะเป็นการสร้างคุณค่าอย่างเด่นชัด

จะเห็นได้ว่า หากจะใช้คุณค่าของ IT โดยเต็มประสิทธิภาพแล้ว จะต้องมีการปรับระบบงานร่วมด้วยเสมอ ดังนั้นจึงเป็นการยาก ต้องอาศัยความร่วมมือของทุกภาคส่วนในองค์การ leadership และ change management และวัฒนธรรมองค์การที่เหมาะสมร่วมด้วย

ลดค่าใช้จ่ายและเพิ่มประสิทธิภาพองค์การ จากคุณสมบัติดังกล่าว IT สามารถช่วยเพิ่มประสิทธิภาพและลดค่าใช้จ่ายขององค์การได้เป็นอย่างดี

การใช้ข้อมูลเพื่อการบริหารจัดการ ส่วนนี้เป็นส่วนที่เราคุ้นเคยกันดี แต่โดยทั่วไปเรายังใช้ข้อมูลได้ไม่เต็มที่ เนื่องจากขาดการวิเคราะห์ข้อมูล วิเคราะห์ความต้องการของข้อมูล และคุณภาพข้อมูล ดังจะกล่าวต่อไป จากคุณค่าของ IT ในทางการแพทย์และสาธารณสุข เราสามารถนำมาใช้ประโยชน์ ดังสรุปประเด็นที่สำคัญ ไว้ในตารางต่อไปนี้

ประโยชน์ของ Health IT

- Alert, Reminder
- Avoid duplicate and unnecessary tests
- Support Dx, Rx plan
- ↑ Use of Best Practices
- ↓ ADR + drug interaction
- Better Care Co-ordination
- ↑ Compliance
- ↑ Patient Safety
- Effective Rx
- Cost-Effective Rx
- ↓ Pt. time + travel
- Monitor Pt. conditions
- ↑ Patient Engagement
- ↑ Pt. responsibility
- ↓ Cost + Workload
- ↑ Accessibility
- ↑ Coverage
- ↑ Equity

เราแบ่งการนำ IT มาใช้ให้เกิดประโยชน์เป็นการใช้ IT เชิงรับ และ เชิงรุก เป็นการแบ่งอย่างไม่เป็นทางการ เพื่อให้เกิดความเข้าใจง่ายๆ เชิงรับหมายถึงนำ IT มาใช้ทำงานเดิมๆ ที่ทำอยู่ประจำวัน ส่วนเชิงรุกหมายถึงการนำ IT มาใช้ปรับปรุงหรือสร้างงาน สร้างคุณค่าและแนวทางใหม่ๆ เพื่อให้โรงพยาบาลบรรลุวิสัยทัศน์ พันธกิจ และเป้าหมายที่วางไว้อย่างมีประสิทธิภาพ ในการวางแผนแม่บท IT ควรคำนึงถึงทั้งเชิงรับและเชิงรุกด้วย

คุณภาพ 3 ด้าน การพัฒนาคุณภาพโรงพยาบาลนั้น อาจแบ่งได้เป็น 3 ด้านคือ

คุณภาพ 3 ด้าน

- คุณภาพด้านคลินิก
- คุณภาพด้านการบริการ
- คุณภาพด้านบริหารจัดการ

คุณภาพด้านคลินิก มุ่งที่ผลการรักษาผู้ป่วย (clinical outcome) โดยส่วนใหญ่จะมุ่งเน้นที่ความปลอดภัยของผู้ป่วย เช่น ลดการแพ้ยา การสั่งรักษาซ้ำซ้อน ลดการติดเชื้อ เพิ่มประสิทธิผลการรักษา

คุณภาพด้านบริการ ทำให้ผู้ป่วยได้รับบริการที่ดีขึ้น (แต่อาจไม่เกี่ยวกับผลการรรักษา) เช่น ลดเวลารอคอย ลดการมาโรงพยาบาล ลดการแออัด

คุณภาพด้านบริหารจัดการ เช่น ลดการรั่วไหล ลดขั้นตอนการทำงาน เพิ่มรายรับ ลดค่าใช้จ่าย เพิ่มประสิทธิภาพ

การจัดทำแผน IT ควรมุ่งเน้นที่คุณภาพด้านคลินิกเป็นอันดับแรก เนื่องจากเป็นจุดประสงค์หลักของโรงพยาบาล แต่อย่างไรก็ดีต้องคำนึงถึงคุณภาพในทั้ง 3 ด้านอย่างเหมาะสม กิจกรรมบางอย่างอาจทำให้เกิดคุณภาพ 2 หรือ 3 ด้านร่วมกัน แต่กิจกรรมบางอย่างอาจเกิดคุณภาพด้านหนึ่งและลดคุณภาพอีกด้านหนึ่งก็ได้ จึงต้องวิเคราะห์ จัดทำแผนอย่างเหมาะสม

ในโรงพยาบาลที่มีการเรียน การสอน อาจมีคุณภาพด้านวิชาการเพิ่มขึ้นด้วย เช่น ระบบข้อมูลเพื่อการวิจัย การจัดการหลักสูตร e-learning e-journal e-textbook โปรแกรมช่วยการวิจัยและสถิติต่างๆ เป็นต้น

ดังนั้นในการวางแผนแม่บท IT จะต้องคำนึงถึงการใช้ IT อย่างสมดุลย์เพื่อคุณภาพในด้านต่างๆ ด้วย

<u>แผน IT ที่พึงประสงค์</u> (ตามกรอบ HITQIF ของ TMI)

ตามกรอบพัฒนาคุณภาพโรงพยาบาล (HITQIF) ของ TMI ได้กำหนดการจัดทำแผนแม่บท IT ของโรงพยาบาลไว้ ในข้อ 1.1 โดยมีประเด็นคุณภาพหลักดังนี้

ประเด็นคุณภาพของแผนแม่บท IT

1. **กำหนดเป้าหมาย และแนวทางการพัฒนาและใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน**
2. **แผนแม่บทมีความสอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และเข็มมุ่งของโรงพยาบาล**
3. **ตอบสนองต่อความต้องการของผู้ปฏิบัติงานในการดูแลผู้ป่วย/บริการสุขภาพให้มีคุณภาพยิ่งขึ้น**
4. **การจัดทำแผนฯ จัดทำโดยการมีส่วนร่วมของบุคลากรที่เกี่ยวข้องทั้ง ผู้บริหารและผู้ปฏิบัติซึ่งเป็นผู้ใช้งานระบบ เทคโนโลยีสารสนเทศในด้านต่างๆ**
5. **มีการสื่อสารแผนแม่บทให้ผู้เกี่ยวข้องรับทราบ และดำเนินการในแนวเดียวกัน**

เมื่อพิจารณาดูตามกรอบการพัฒนา จะพบว่าการจัดทำแผนแม่บท IT ไม่ใช่เพียงแค่มีแผนว่า IT จะทำอะไรเท่านั้น แต่สิ่งที่ทำจะต้องสอดคล้อง (align) กับเป้าหมายของโรงพยาบาล เพื่อให้โรงพยาบาลสามารถใช้ ITเป็นเครื่องมือผลักดันให้บรรลุเป้าประสงค์ที่ต้องการ และสิ่งนี้จะเกิดขึ้นได้ แผนจำเป็นต้องมีความชัดเจน ต้องเกิดขึ้นโดยการมีส่วนร่วมของทุกภาคส่วนของโรงพยาบาล ทุกส่วนโรงพยาบาลรับทราบและปฏิบัติในแนวทางเดียวกัน รวมทั้งมีการประเมินผล ตรวจสอบและปรับปรุงแผนให้ดีขึ้นตามลำดับ (ตามกระบวนการ PDCA) ด้วย

ความสอดคล้องของแผนยุทธศาสตร์โรงพยาบาลกับแผนแม่บท IT (Business-IT Alignment)

ความสอดคล้องของแผน IT กับยุทธศาสตร์โรงพยาบาล หมายถึงการที่กำหนดแผนงานด้าน IT ที่ส่งเสริมสนับสนุนโรงพยาบาลให้สามารถดำเนินการสู่เป้าหมายยุทธศาสตร์ที่กำหนด ปัจจุบัน IT สามารถสร้างคุณค่าและเข้าไปมีบทบาทได้เกือบทุกกระบวนงานจึงสามารถกำหนดความสอดคล้องนี้ได้อย่างกว้างขวาง ในเกือบทุกยุทธศาสตร์ พันธกิจ และเข็มมุ่งของโรงพยาบาล

ความสอดคล้องนี้ สามารถเป็นได้สองทาง ทางหนึ่งคือ IT สอดคล้องและสนับสนุนยุทธศาสตร์ของโรงพยาบาลเพื่อสร้างคุณค่าให้โรงพยาบาลมุ่งสู่เป้าหมาย และอีกทางหนึ่งคือ IT เองเป็นตัวกำหนดแผนยุทธศาสตร์ของโรงพยาบาล หมายถึงโรงพยาบาลได้พิจารณาคุณค่าของ IT เพื่อนำไปกำหนดเป็นยุทธศาสตร์ของโรงพยาบาล ดังนั้นหากให้เกิดผลดีที่สุด IT จะต้องมีส่วนร่วมตั้งแต่ขั้นตอนการวางยุทธศาสตร์ของโรงพยาบาล หรือต้องนำปัจจัยความก้าวหน้าและคุณค่าของ IT เป็นส่วนหนึ่งของปัจจัยนำเข้าในการจัดทำยุทธศาสตร์โรงพยาบาล เพื่อให้เกิดคุณค่าสูงสุด

หากแผนแม่บท IT ไม่สอดคล้องกับแผนยุทธศาสตร์ของโรงพยาบาลก็จะทำให้การใช้ IT ไม่คุ้มค่า ไม่สามารถอธิบายได้ว่ามีระบบ IT ไว้เพื่ออะไรหรือจะลงทุนด้าน IT ไปเพื่ออะไร เรื่องของความสอดคล้องนี้มีความสำคัญมากต่อการพัฒนาคุณภาพเทคโนโลยีสารสนเทศของโรงพยาบาลซึ่งจะกล่าวถึงต่อไป

การมีส่วนร่วมของบุคลากรผู้เกี่ยวข้อง เนื่องจาก IT เข้าไปเกี่ยวข้องกับทุกหน่วยงาน และกระบวนงานต่างๆ จำนวนมาก การวางแผนแม่บท IT จึงจำเป็นต้องอาศัยการมีส่วนร่วมจากบุคลากรทั้ง 3 ส่วน คือผู้บริหาร ผู้ใช้งาน และฝ่าย IT

- หากแผน IT กำหนดจากฝ่าย IT แผนจะกำหนดแต่การพัฒนา software, hardware, network และบุคลากรเป็นหลัก เนื่องจากฝ่าย IT ไม่เข้าใจลึกซึ้งถึง business process ยุทธศาสตร์ และเป้าหมายที่แท้จริงของโรงพยาบาล
- หากแผน IT กำหนดจากผู้บริหาร แผนจะกำหนดด้านข้อมูล หรือคุณภาพการบริหารจัดการเป็นหลัก ผู้บริหารอาจไม่เข้าใจกระบวนงานอย่างถ่องแท้ จนบางครั้งอาจสร้างระบบ IT ที่เกิดปัญหากับผู้ใช้งานได้ รวมทั้งอาจไม่เข้าใจคุณค่าของ IT เพียงพอ ทำให้เสียโอกาสพัฒนาให้เกิดประสิทธิภาพสูงสุดได้
- หากแผน IT กำหนดโดยผู้ใช้งาน แผนจะกำหนดการแก้ปัญหาหน้างานเป็นหลัก อาจไม่ตอบสนองหรือไม่เรียงลำดับความสำคัญตามวิสัยทัศน์ พันธกิจ และยุทธศาสตร์ของโรงพยาบาลได้ครบถ้วน

ดังนั้น การจัดทำแผนแม่บท IT จึงต้องอาศัยการทำงานเป็นทีม โดยความร่วมมือของทุกส่วน ทั้งผู้บริหาร ผู้ใช้งาน และฝ่าย IT เพื่อให้เกิดการใช้ IT อย่างคุ้มค่า สอดคล้องกับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์ของโรงพยาบาล

การสื่อสารและดำเนินการ และ การติดตามประเมินผล เมื่อมีการกำหนดแผนแม่บทแล้ว จำเป็นต้องมีกระบวนการให้สามารถดำเนินการตามแผน และติดตามประเมินผล เพื่อการปรับปรุงซึ่งจะกล่าวถึงในลำดับต่อๆ

<u>ปัญหาการจัดทำแผนแม่บท IT ที่พบจากการเยี่ยมสำรวจ</u>

1. โรงพยาบาลไม่มีแผนยุทธศาสตร์ที่ชัดเจน
   - ไม่จัดทำแผน
   - มีแต่ยุทธศาสตร์กว้างๆ ไม่มีกลยุทธ เข็มมุ่ง
   - ขาดความเชื่อมโยงแผน (strategic map) ที่ชัดเจน
   - ขาดการ implement แผน

โรงพยาบาลหลายแห่ง ยังไม่ได้จัดทำแผนยุทธศาสตร์ของโรงพยาบาล โดยไม่ได้ให้ความสำคัญหรือกำลังอยู่ระหว่างจัดทำ ยังไม่แล้วเสร็จ กรณีนี้การวางแผนแม่บท IT เป็นไปได้ยาก เพราะไม่ทราบจะตอบสนองอะไร

บางครั้งแผนยุทธศาสตร์โรงพยาบาลระบุไว้เพียงกว้างๆ เช่น เป็นโรงพยาบาลที่เป็นเลิศด้านรักษาพยาบาล แต่พอลงลึกกลับไม่สามารถบอกได้ว่าเป็นเลิศหมายความว่าอะไร วัดอย่างไร และจะไปถึงความเป็นเลิศได้อย่างไร เมื่อไร

บางครั้งแผนยุทธศาสตร์ไม่ระบุความเชื่อมโยงของแต่ละยุทธศาสตร์ ว่าแต่ละยุทธศาสตร์ กลยุทธ โครงการต่างๆ ส่งผลถึงกันอย่างไร ในทั้งสองกรณีนี้ จะยากต่อการวิเคราะห์ปัจจัยแห่งความสำเร็จของยุทธศาสตร์นั้นๆ และยากต่อการวางแผน IT ให้สอดคล้องกับแผนดังกล่าว

หลายโรงพยาบาลมีแผนยุทธศาสตร์และเก็บไว้เฉยๆ ไม่ได้ดำเนินการตามแผนที่วางไว้อย่างจริงจัง กรณีนี้ย่อมยากที่จะมีแผนแม่บท IT ที่บรรลุผลได้

หากโรงพยาบาลยังไม่มีแผนยุทธศาสตร์ที่ชัดเจน แนะนำว่าควรพิจารณาเรื่องแผนยุทธศาสตร์ของโรงพยาบาลเป็นลำดับแรก เพราะเป็นเรื่องสำคัญในการทำงานอย่างมีเป้าประสงค์และทิศทาง สามารถควบคุม กำกับ ติดตาม และวัดผลสำเร็จได้ และควรถือเป็นโอกาสที่จะจัดทำแผนแม่บท IT ไปพร้อมกันเพื่อให้เกิดความสอดคล้องตั้งแต่ต้น

2. โรงพยาบาลไม่มีแผนแม่บท IT

- O ไม่จัดทำแผน
- o มีแผนอยู่ในใจ ไม่มีเอกสาร
- o ระบุการพัฒนา IT ในแผนยุทธศาสตร์โรงพยาบาล แต่ไม่มีแผน IT ที่ชัดเจน

โรงพยาบาลหลายแห่งไม่มีแผนแม่บท IT ส่วนใหญ่เป็นเพราะไม่เห็นความสำคัญ ทำให้ทำงานเป็นชิ้นๆ และอาจไม่ตอบสนองต่อทิศทางของโรงพยาบาลอย่างเหมาะสม

บ่อยครั้งที่โรงพยาบาลแจ้งว่ามีแผนแม่บท IT อยู่แล้ว และสามารถเล่าให้ฟังได้ว่าจะทำอะไรบ้าง แต่ไม่มีเอกสาร กรณีนี้หัวหน้าหน่วย IT มักรู้รายละเอียดแผนอยู่คนเดียว (หรือกลุ่มเดียว) ทำให้ขาดการสื่อสารให้ทุกคนที่เกี่ยวข้องปฏิบัติตามแผนในแนวเดียวกัน รวมทั้งมีปัญหาในการควบคุม กำกับ ติดตาม ให้เป็นไปอย่างไม่เป็นระบบ และมีประสิทธิภาพ

หลายครั้งพบว่า แผนยุทธศาสตร์ของโรงพยาบาล มียุทธศาสตร์หนึ่งที่ระบุว่า โรงพยาบาลจะพัฒนาระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ แต่ไม่กำหนดแผนที่ชัดเจน

3. แผน IT ไม่สอดคล้องกับแผนยุทธศาสตร์ของโรงพยาบาล

- o พัฒนา IT แยกส่วนจากแผนงานอื่นๆ ของโรงพยาบาล โดยไม่ได้คำนึงถึงเป้าหมายของโรงพยาบาล
- o แผนโรงพยาบาล และแผน IT ต่างคนต่างทำ แล้วมาจับโยงกันภายหลัง
- o พัฒนาตามผู้บริหารและผู้ใช้ขอมาเป็นหลัก

โรงพยาบาลหลายแห่ง กำหนดแผนแม่บท IT โดยพัฒนา IT เพื่อ IT กล่าวคือกำหนดการพัฒนา hardware software network และบุคลากร โดยไม่ได้เกี่ยวข้องกับยุทธศาสตร์ของโรงพยาบาลเลย ไม่ทราบว่าแผนนั้นมุ่งตอบสนองต่อเป้าหมายยุทธศาสตร์อะไรของโรงพยาบาล ทำให้ IT ไม่สามารถตอบสนองต่องานของโรงพยาบาลได้อย่างแท้จริง

ในเมื่อกรอบพัฒนาคุณภาพกำหนดให้มีการเชื่อมโยงแผนแม่บท IT กับแผนยุทธศาสตร์โรงพยาบาล หลายแห่งไม่ได้วิเคราะห์แผนยุทธศาสตร์โรงพยาบาลและนำมากำหนดแผนแม่บท IT แต่กำหนดแผนแม่บท IT ขึ้นมาแล้วจับนำมาโยงกับแผนยุทธศาสตร์ในภายหลัง เช่น แผนยุทธศาสตร์โรงพยาบาลกำหนดเป้าหมายสู่ความเป็นเลิศด้านการรักษาพยาบาล ก็จับมาโยงแผนแม่บท IT ว่าจะนำเอาโปรแกรม HosXp มาใช้ ไม่ระบุแน่ชัดว่าจะช่วยให้โรงพยาบาลเป็นเลิศได้อย่างไร

แผนแม่บท IT อีกประเภทหนึ่งที่พบ คือพัฒนา IT เพื่อแก้ปัญหาเฉพาะหน้า ตามความต้องการของผู้บริหารและผู้ใช้ต้องการแต่เป็นหลัก อันที่จริงการพัฒนาตามความต้องการนี้เป็นส่วนสำคัญที่ต้องคำนึงถึงในการจัดทำแผนแม่บท IT แต่จะต้องวิเคราะห์ว่าเป็นไปตามยุทธศาสตร์ของโรงพยาบาลหรือไม่ และจัดลำดับความสำคัญของการพัฒนาอย่างเหมาะสมด้วย

4. แผน IT สอดคล้องกับแผนของโรงพยาบาลบางส่วน
   - Focus แต่เรื่องข้อมูล MIS หรือใช้ IT ตอบสนองคุณภาพด้านการบริหารแต่เพียงอย่างเดียว ขาดการใช้ IT เป็น enabler และการใช้ IT พัฒนาคุณภาพด้านคลินิก
   - กำหนดแผน IT ตามแผนโรงพยาบาล แต่ไม่ใช่ key success factor ในเรื่องนั้นๆ

ในโรงพยาบาลที่มีการพัฒนามากยิ่งขึ้น เริ่มมีความสอดคล้องของแผนแม่บท IT กับแผนยุทธศาสตร์ของโรงพยาบาล โดยมีแผนยุทธศาสตร์ของโรงพยาบาลว่าจะนำ IT มาช่วยตอบสนองความต้องการของแผนยุทธศาสตร์ และนำไปช่วยงานของโรงพยาบาลได้อย่างไร

ระยะแรกๆ มักวิเคราะห์ว่า IT จะช่วยให้เกิดข้อมูลที่นำไปใช้ในการบริหารจัดการ เพื่อให้บรรลุเป้าหมายยุทธศาสตร์ของโรงพยาบาล และส่วนใหญ่เน้นข้อมูลด้านการบริหาร เช่น ข้อมูลการใช้ยา ข้อมูลการเบิกจ่ายจากกองทุน ข้อมูลตัวชี้วัดต่างๆ (กรณีนี้รวมผลลัพธ์ทางคลินิก เช่น ตัวชี้วัด HA ด้วย) ถ้าพิจารณาตาม PDCA cycle กระบวนการในลักษณะนี้คือการ Check เพื่อตรวจสอบผลการปฏิบัติงาน แต่ยังไม่ได้นำมาปรับปรุงให้ดีขึ้น (Act Plan Do) กล่าวคือยังไม่ใช้ IT เชิงรุกโดยใช้คุณค่า IT as Service Enabler เพื่อสร้างคุณค่าและแนวทางใหม่ๆ ในการนำโรงพยาบาลไปสู่เป้าหมายที่วางไว้

บางครั้งนำ IT ไปดูแลปัญหาเล็กๆ ในยุทธศาสตร์ ซึ่งไม่ใช้ปัจจัยหลักที่ทำให้ยุทธศาสตร์สำเร็จ (Critical Success Factor - CSF) เช่น ในกระบวนการดูแลผู้ป่วยโรคเรื้อรัง กลับนำ IT ไปวัดความพึงพอใจของผู้ป่วย ซึ่งไม่ใช่ CSF ของกระบวนการนี้

<u>การพัฒนาแผนแม่บท IT</u>

1. **สร้างทีมที่ร่วมกันพัฒนา และ implement แผน IT**
   - ผู้บริหาร
   - ฝ่าย IT
   - ผู้ใช้งาน

ดังที่กล่าวมาข้างต้นแล้ว แผนแม่บท IT ต้องเกิดจากความร่วมมือของทุกฝ่าย ทั้งผู้บริหาร ฝ่าย IT และผู้ใช้งาน ผู้บริหารอาจเป็น CIO หรือผู้อำนวยการเองก็ได้ ส่วนผู้ใช้งานควรรวบรวมผู้เกี่ยวข้องกับกิจกรรมหลักๆ ของ IT เช่น องค์กรแพทย์ พยาบาล เภสัชกร ฝ่ายแผนงาน ฝ่ายการเงินและบัญชี ฝ่ายทรัพยากรบุคคล ศูนย์พัฒนาคุณภาพโรงพยาบาล และฝ่ายอื่นๆ ที่เห็นสมควร ร่วมกันเป็นทีมพัฒนา (และ implement) แผนแม่บท IT

อันดับแรก**ผู้บริหาร**ต้องมีความมุ่งมั่น เข้าใจ ผลักดัน และสนับสนุน กำหนดทิศทางและนโยบาย รวมทั้งติดตามและกำกับดูแลการนำ IT มาใช้ในโรงพยาบาลอย่างจริงจัง ภาวะการนำ (Leadership) เป็นปัจจัยสำเร็จที่สำคัญของการใช้ IT ในหน่วยงาน โดยเฉพาะอย่างยิ่งในระยะเริ่มแรกของการนำ IT มาใช้

ฝ่าย IT ต้องมีความรู้ทั้งด้าน IT และทิศทางของโรงพยาบาล เพื่อสามารถเสนอแนะและดำเนินการให้แผน IT ประสบความสำเร็จ นอกจากนั้นต้องมีปฏิสัมพันธ์อันดีกับทั้งผู้บริหาร และผู้ใช้งาน

ผู้ใช้งาน จะต้องเข้าใจเป้าหมายของหน่วยงานในการเป็นส่วนหนึ่งของยุทธศาสตร์โรงพยาบาล และร่วมมือในการนำ IT มาใช้เพื่อบรรลุวัตถุประสงค์ดังกล่าว ถ้ามี champion user อาจนำมาร่วมวางแผนแต่ต้น แต่ควรมีระดับบริหารหน่วยของงานร่วมด้วย เพื่อให้กำหนดทิศทางและประสานความร่วมมือของหน่วยงาน ทั้งนี้ขึ้นกับวัฒนธรรมองค์กร ของโรงพยาบาลและหน่วยงานนั้นๆ ด้วย

ปัจจัยความสำเร็จของแผนแม่บท IT

- **ผู้บริหารระดับสูงต้องเข้าใจ มีส่วนร่วม และผลักดันงาน IT**
- **ความสัมพันธ์อันดีระหว่างหน่วย IT กับทีมบริหาร**
- **ความรู้ด้าน IT และ ด้านการวางแผน และการบริหารเป็นอย่างดี**
- **ความร่วมมือของทุกส่วนของโรงพยาบาล ทั้งผู้บริหาร ผู้ใช้งาน และ หน่วยงาน IT**

2. **วิเคราะห์แผนยุทธศาสตร์โรงพยาบาล**
   - เป้าหมายยุทธศาสตร์ของ ร.พ. เป็นอย่างไร
   - ในการกำหนดยุทธศาสตร์โรงพยาบาล ได้คำนึงถึงคุณค่าของ IT หรือไม่
   - แผนที่ยุทธศาสตร์ ความเชื่อมโยงของปัจจัยต่างๆ เป็นอย่างไร
   - วางลำดับความสำคัญไว้อย่างไร เข็มมุ่งคืออะไร
   - ปัจจัยแห่งความสำเร็จคืออะไร

เมื่อกำหนดทีมพัฒนาและ implement แผนแม่บท IT แล้ว ลองวิเคราะห์ดูว่าทีมมีความพร้อมดังกล่าวข้างต้นในการนำ IT มาใช้ในโรงพยาบาลหรือไม่เพียงไร อาจต้องมีการสร้างความรู้ความเข้าใจให้ทีม และจัดเป้าหมาย โครงสร้างหน้าที่ กฎกติกา และกระบวนการทำงานร่วมกัน เพื่อให้ทีมพร้อมที่จะทำงานอย่างมีประสิทธิภาพ โดยทั่วไปแล้ว CIO จะมีบทบาทสำคัญในการประสานและพัฒนาทีมดังกล่าว

การพัฒนาแผนแม่บท IT ต้อง cascade มาจากแผนยุทธศาสตร์ของโรงพยายาล ดังนั้นเมื่อได้ทีมพัฒนาแล้ว ให้นำแผนยุทธศาสตร์ของโรงพยาบาลมาทำการวิเคราะห์ แนะนำให้วิเคราะห์ดังนี้

เป้าหมายยุทธศาสตร์ของโรงพยาบาล โดยทั่วไปเป้าหมายสูงสุดของโรงพยาบาล (อาจเรียก เป้าประสงค์) คือเป้าหมายที่นำไปสู่วิสัยทัศน์ของโรงพยาบาล เช่น เป็นโรงพยาบาลที่มีความเชี่ยวชาญระดับสูงของประเทศ แปลเป็นเป้าหมายคือ 1.ความเป็นเลิศในการดูแลรักษาผู้ป่วยยุ่งยากซับซ้อน 4 โรคหลัก (หัวใจ มะเร็ง อุบัติเหตุ ทารกแรกเกิด) 2.ความสามารถในการทำหัตถการที่ใช้เทคโนโลยีสูง (retina surgery, cardiac catheterization etc.) 3.ความสามารถในการแก้ปัญหาโรคของท้องถิ่นอย่างเป็นระบบ (เบาหวาน ความดัน COPD) เป็นต้น นอกจากนี้อาจมีเป้าหมายด้านการบริหารที่ช่วยสนับสนุนเป้าหมายหลัก เช่น การมี

สถานะการเงินที่มั่นคง เพิ่มรายรับ ลดรายจ่าย เป้าหมายด้านการพัฒนาบุคลากร เช่นกำหนดและพัฒนาสมรรถนะบุคลากร เป้าหมายด้านการพัฒนาคุณภาพ เช่นการจัดการความเสี่ยงของผู้ป่วย ร่วมด้วยยุทธศาสตร์โรงพยาบาลที่ดีจะแสดง**ความเชื่อมโยง**ให้เห็นชัดว่า แต่ละยุทธศาสตร์ส่งผลต่อยุทธศาสตร์อื่นอย่างไร และรวมกันแล้วนำไปสู่เป้าประสงค์และวิสัยทัศน์ของโรงพยาบาลได้อย่างไร การเชื่อมโยงนี้สามารถแสดงได้ดีโดยใช้**แผนที่ยุทธศาสตร์**ซึ่งจะมีความสำคัญต่อการวิเคราะห์ปัจจัยแห่งความสำเร็จของแผนโดยรวมและวางแผนแม่บท IT ต่อไป

การวิเคราะห์ยุทธศาสตร์โรงพยาบาล จะทำให้เห็นว่า ยุทธศาสตร์โรงพยาบาลเอง มีความสอดคล้องกันหรือไม่ ระหว่างเป้าหมายยุทธศาสตร์ ยุทธศาสตร์ กลยุทธ และโครงการต่างๆ รวมทั้งความเชื่อมโยงระหว่างยุทธศาสตร์ด้วย ที่ให้ทำการวิเคราะห์ในส่วนนี้เพราะบ่อยครั้ง ปัญหาของการวางแผนแม่บท IT อยู่ที่ความไม่ชัดเจนของแผนยุทธศาสตร์โรงพยาบาลเอง

นอกจากนี้เนื่องจากความสอดคล้องของยุทธศาสตร์โรงพยาบาลและแผนแม่บท IT เป็นไปได้ทั้งสองทางจึงควรวิเคราะห์ว่าในการทำแผนยุทธศาสตร์โรงพยาบาลนั้น IT ได้เข้าไปมีส่วนร่วมในการทำแผนหรือไม่ และยุทธศาสตร์ที่วางไว้ได้**คำนึงถึงคุณค่าของ IT เป็นส่วนหนึ่งของการวางแผนยุทธศาสตร์โรงพยาบาล**ด้วยหรือไม่ และหากคำนึงคุณค่าของ IT แล้วจะสามารถเปลี่ยนแปลงยุทธศาสตร์โรงพยาบาลให้ดีขึ้นหรือไม่

หากมีปัญหาที่ระดับยุทธศาสตร์โรงพยาบาล ให้ลองพิจารณาดูว่าจะปรับยุทธศาสตร์โรงพยาบาลใหม่ (หลายโรงพยาบาลเลือกวิธีนี้) หรือทำแผนแม่บท IT เท่าที่จะทำได้ไปก่อน และปรับยุทธศาสตร์โรงพยาบาลในภายหลัง ทั้งนี้ขึ้นอยู่กับการพิจารณาของฝ่ายบริหาร โดยทีมรายงานผลการวิเคราะห์ให้ฝ่ายบริหารทราบ

เมื่อได้เป้าหมายยุทธศาสตร์แล้ว วิเคราะห์**ลำดับความสำคัญของแต่ละเป้าหมาย** ว่าโรงพยาบาลกำหนดความสำคัญไว้อย่างไร บางครั้งถ้ามีการกำหนดเข็มมุ่ง (ส่วนมากจะกำหนดไว้แต่ละปี) จะเป็นการดีเพราะเป็นสิ่งที่มีลำดับความสำคัญสูงซึ่ง IT จะต้องนำมาพิจารณาเป็นลำดับต้นๆ ในการพัฒนาแผนแม่บท IT ต่อไป

เมื่อได้เป้าหมาย และลำดับความสำคัญแล้ว ให้ **วิเคราะห์ปัจจัยแห่งความสำเร็จ** (Critical Success Factor - CSF) ของแต่ละเป้าหมายว่ามีอะไรบ้าง (ปัจจัยแห่งความสำเร็จนี้ อาจเรียกว่า business driver หมายถึงสิ่งที่ต้องมีหรือต้องปฏิบัติเพื่อให้บรรลุเป้าหมาย) การวิเคราะห์ปัจจัยแห่งความสำเร็จนี้มีความสำคัญมาก เพราะบ่อยครั้งพบว่ามีการจัดทำแผน IT ที่ไม่ได้มุ่งที่ปัจจัยแห่งความสำเร็จทำให้แผน IT นั้นไม่ประสบผล ตัวอย่างเช่น ตั้งเป้าหมายเพื่อลดอัตราตายของผู้ป่วยโรคหัวใจขาดเลือด แต่ใช้ IT ไปวัดความพึงพอใจของผู้ป่วยและญาติ ซึ่งไม่ใช่ปัจจัยแห่งความสำเร็จของเรื่องนี้

การหาปัจจัยแห่งความสำเร็จอาจทำได้หลายวิธี เช่น

- ดูจากตัวชี้วัด (KPI) ว่ากิจกรรมใดที่ทำให้ตัวชี้วัดประสบผลสำเร็จ วิธีนี้ต้องอาศัยการกำหนดตัวชี้วัดที่เหมาะสมแต่ต้นมิฉะนั้นจะได้ CSF ที่ไม่ถูกต้อง วิธีนี้เป็นวิธีง่ายๆ แต่อาจมีปัญหาเพราะกระบวนการที่ทำให้ได้สำเร็จผลตามตัวชี้วัดอาจไม่ใช่ CSF ก็ได้เนื่องจากตัวชี้วัดตัวนั้นๆ อาจจะสามารถบรรลุผลได้หลายวิธี การเทียบเคียงจากแผนที่ยุทธศาสตร์ของโรงพยาบาลอาจพอบอกได้ว่า ปัจจัยแห่งความสำเร็จที่สัมพันธ์กับตัวชี้วัดนั้นมาจากกระบวนการอะไร
- วิเคราะห์กระบวนการทั้งหมด และดูว่าส่วนไหนเป็นปัจจัยสำคัญ หากมีข้อมูลประกอบจะช่วยให้การวิเคราะห์แม่นยำขึ้น เช่น ขั้นตอนการดูแลผู้ป่วยเบาหวาน เริ่มจากการคัดกรองกลุ่มเป้าหมาย ผู้ป่วยที่ป่วยมารับการรักษา (coverage) กลุ่มที่ป่วยมาตรวจตามนัดสม่ำเสมอ การได้รับยาและกินยาตามสั่ง การปฏิบัติตนของผู้ป่วย การตรวจ lab ต่างๆ (glucose HbA1c microalbuminuria) การคัดกรองภาวะแทรกซ้อน การตรวจรักษาภาวะแทรกซ้อน การส่งต่อ เป็นต้น แต่ละขั้นตอนจะมี CSF เช่น ผลสำเร็จของการคัดกรอง อยู่ที่การจัดให้มีข้อมูลประชากรที่ถูกต้องครบถ้วนและจัดกระบวนการคัดกรองที่มีประสิทธิภาพ ผลสำเร็จของการมาตรวจตามนัด อยู่ที่จัดระบบการมาตรวจให้สะดวกรวดเร็ว มีระบบแจ้งเตือน มีการคืนข้อมูลให้ผู้ป่วยและชุมชนเพื่อช่วยกระตุ้นให้ผู้ป่วยมารับการรักษาอย่างสม่ำเสมอ เป็นต้น นำปัจจัยแห่งความสำเร็จทั้งหมดมาวิเคราะห์ลำดับความสำคัญ อาจเลือก CSF ที่สำคัญ (เช่นไม่เกิน 5 ตัว) เพื่อใช้ในการวางแผน IT ต่อไป
- สอบทานจากผู้ปฏิบัติ เก็บข้อมูลหน้างาน และนำผลมาวิเคราะห์หาปัจจัยแห่งความสำเร็จ อาจทำในรูปแบบ survey focus group งานวิจัย หรือ R2R ก็ได้

ผลการวิเคราะห์ทั้งหมดทุกหัวข้อข้างต้นควรจัดทำเป็นเอกสารให้ชัดเจน เพื่อใช้อ้างอิงและป้องกันการตกหล่นหรือเข้าใจคลาดเคลื่อนเมื่อนำไปกำหนดเป็นแผนแม่บท IT รวมทั้งมีประโยชน์ในการสร้างความเข้าใจเมื่อมีการเผยแพร่และ implement แผน และสามารถนำกลับมาทบทวนเมื่อมีการจัดทำแผนยุทธศาสตร์โรงพยาบาลหรือจัดทำแผนแม่บท IT ครั้งต่อไปด้วย

3. **กำหนดเป้าหมายของ IT ที่สอดคล้องกับโรงพยาบาล**

- วิเคราะห์ pain points, root causes, drivers และ gaps
- วิเคราะห์สภาพแวดล้อม ภายใน-ภายนอก
- IT สร้างคุณค่า และช่วยให้ ร.พ.ถึงเป้าหมายได้อย่างไร
- กำหนดเป้าหมายของแผนแม่บท IT ประชุมเพื่อตกลงเป้าหมายร่วมกัน

การกำหนดเป้าหมายของ IT นั้น นอกจากอาศัยการวิเคราะห์ยุทธศาสตร์โรงพยาบาลดังกล่าวข้างต้นแล้ว ต้องวิเคราะห์ปัจจัยด้าน IT และความต้องการของผู้ใช้งานด้วย เพื่อให้แผนมีความเป็นไปได้และตอบสนองผู้ใช้งานอย่างครบถ้วน

Pain point คือปัญหาที่พบเกี่ยวกับการทำงานด้าน IT ในโรงพยาบาล เป็นสิ่งที่ stakeholder ต่างๆ เดือดร้อน (หรือต้องการเพิ่มเติม) จากการใช้งาน IT เช่น แพทย์มีปัญหาเรื่องการพิมพ์ข้อมูลจำนวนมากเข้าใน EHR ทำให้มีเวลากับผู้ป่วยน้อยลง เวชระเบียนมีปัญหาที่แพทย์ไม่ลงการวินิจฉัยโรคและตรวจร่างกาย และลงรหัส ICD ผิดพลาดจำนวนมาก นำมาพิจารณาหา **Root causes** ของ pain point ดังกล่าว เช่นในกรณีนี้อาจมาจาก application program ที่ไม่เหมาะสม การให้ความรู้แพทย์ไม่เพียงพอ หลังจากนั้นวิเคราะห์หา success factor (driver) ในการแก้ปัญหา (หรือพัฒนาตามความต้องการ) และเลือก pain point ที่สำคัญ มาเป็น input สำหรับการกำหนดเป้าหมายของแผนแม่บท IT ต่อไป

ทำการวิเคราะห์สภาพแวดล้อม ภายใน-ภายนอก (SWOT analysis) วิเคราะห์จุดแข็ง จุดอ่อน โอกาส และภัยคุกคามที่เกี่ยวข้องกับ IT โดยนำมาพิจารณาร่วมกับเป้าหมาย เพื่อวิเคราะห์ถึงความเป็นไปได้และเหมาะสมในการกำหนดเป้าหมาย IT ต่อไป

การที่ไม่ให้ทำการวิเคราะห์ SWOT ก่อนหน้านี้ แต่ให้ทำหลังจากทราบเป้าหมายและปัจจัยแห่งความสำเร็จของแผนแล้ว ก็เพื่อให้แผนแม่บท IT ที่กำหนดขึ้นเป็นไปตามเป้าหมายที่สอดคล้องกับแผนยุทธศาสตร์และความต้องการของ stakeholder เป็นหลัก ไม่ใช่เป็นไปตามการวิเคราะห์ SWOT แต่เพียงอย่างเดียว นอกจากนั้นยังพบว่าหากวิเคราะห์ SWOT โดยไม่ทราบเป้าหมายที่แน่ชัดจะไม่สามารถบอกว่าอะไรเป็นจุดแข็งหรือจุดอ่อนได้อย่างแท้จริง

นำผลการวิเคราะห์ทั้งหมด ทั้งจากเป้าหมายยุทธศาสตร์โรงพยาบาลและปัจจัยแห่งความสำเร็จ รวมกับผลวิเคราะห์ความต้องการของ stakeholder และ SWOT มาพิจารณาแนวทางการนำ IT มาสนับสนุนให้บรรลุเป้าหมายดังกล่าว โดย**คำนึงถึงคุณค่าของ IT ทั้งเชิงรับ และเชิงรุก** โดยพิจารณาแต่ละเป้าหมายว่าสามารถมีโครงการด้าน IT เข้าไปสนับสนุนให้เกิดผลตามเป้าหมายได้หรือไม่อย่างไร มีความเป็นไปได้และคุ้มค่าเพียงไร เลือกที่เหมาะสมมา**กำหนดร่วมกันเป็นเป้าหมายของแผนแม่บท IT**

4. กำหนดแผนแม่บท IT

- Infrastructure (hardware, application software, network)
- โครงสร้างองค์กรด้าน IT
- Workforce (skill, Culture)
- IT services
- MIS

เมื่อกำหนดเป้าหมายของแผนแม่บท IT แล้ว นำมาวิเคราะห์แนวทางการดำเนินงานเพื่อให้บรรลุเป้าหมายดังกล่าวแล้ว ทำการวิเคราะห์ปัจจัยแห่งความสำเร็จของแนวทางการดำเนินงานข้างต้น ว่าต้องมีการพัฒนา infrastructure (hardware, application, software, network) พัฒนากำลังคน (จำนวน สมรรถนะ culture) การฝึกอบรม (ทั้งบุคลากร IT และผู้ใช้งาน) ต้องพัฒนา IT service และระบบข้อมูลข่าวสารเพื่อการบริหาร (MIS) อะไรบ้าง (คือการกำหนด enablers goals ด้าน IT ตามกรอบของ IT Governance นั่นเอง)

นำทั้งหมดข้างต้นกำหนดเป็นยุทธศาสตร์ กลยุทธ แผนงาน/โครงการต่างๆ ด้าน IT ควรจัดทำแผนที่ยุทธศาสตร์ของแผนแม่บท IT ด้วย เพื่อแสดงความเชื่อมโยงของแต่ละแผนงาน โครงการ กลยุทธ ยุทธศาสตร์ว่าเชื่อมโยงกันอย่างไร ส่งผลถึงกันอย่างไร เพื่อความเข้าใจ และสะดวกในการสื่อสารแผนแม่บท IT ต่อไป กำหนดผู้รับผิดชอบ (เจ้าภาพ) แนวทางและระยะเวลาการ implement การติดตามและประเมินผลในแต่ละส่วนของแผนให้ชัดเจนเพื่อให้สามารถดำเนินการและติดตามแผนได้อย่างมีประสิทธิภาพ

<u>การดำเนินการตามแผน (Implement)</u>

แผนที่ไม่ถูก implement จะถูกวางไว้บนหิ้ง เสียทั้งเงินทั้งเวลาในการทำแผนโดยไม่เกิดประโยชน์ใดใด เป็นที่น่าเสียดายจากการศึกษาพบว่า แผนแม่บท IT 60 – 90% implement ไม่สำเร็จ ดังนั้นการ implement แผนจึงเป็นเรื่องสำคัญและยากกว่าการวางแผนแม่บท IT ที่ดีเสียอีก

จากการศึกษาพบว่า อุปสรรคที่ทำให้การ implement แผนไม่ประสบความสำเร็จมีดังตารางข้างล่าง ได้แก่ การต่อต้านการเปลี่ยนแปลง ความไม่ชัดเจนของแผน ขาดกระบวนการสนับสนุน ขาดการสื่อสาร ยุทธศาสตร์ขัดกัน และขาดผู้รับผิดชอบ ดังนั้นสิ่งที่ต้องทำเพื่อให้การ implement แผนให้สำเร็จมีดังนี้

อุปสรรคของการ Implement แผน

- ไม่สามารถจัดการกับการเปลี่ยนแปลงและการต่อต้าน **(Inability to manage change and resistance)**
- แผนไม่มีความชัดเจน **(Poor or vague strategy)**
- ขาดแนวทางและรูปแบบในการสนับสนุนกระบวนการ **implement (No guidelines or models available to support the implementation process)**
- ปัญหาการสื่อสารภายใน **(Weak or inadequate communication within organization)**
- พยายาม **implement** ยุทธศาสตร์ที่ขัดกัน **(Attempt to implement a strategy in conflict with existing power structures)**
- ขาดผู้รับผิดชอบที่ชัดเจนในการ **implement** แผน **(Unclear responsibilities within the implementation process)**

ทีมที่รับผิดชอบการ implement มีความสำคัญยิ่ง เนื่องจากการปฏิบัติตามแผน IT มักมีการเปลี่ยนแปลงเกิดขึ้นในกระบวนงาน ภาระงานที่เพิ่มขึ้นหรือลดลง เกี่ยวข้องกับคนและระบบงานจำนวนมาก และอาจใช้เวลาพอสมควรในการจัดการให้ระบบเป็นไปได้ราบรื่น ดังนั้นจำเป็นต้องอาศัย Leadership และทีมที่เข้มแข็ง ทีมบริหารและหัวหน้าหน่วยงานต่างๆ จะต้องให้การ support ทีม IT และผู้ใช้งานต้องมีปฏิสัมพันธ์อันดีต่อกัน จึงจะสามารถ implement แผนแม่บท IT ได้อย่างราบรื่น ทีมนี้ส่วนใหญ่จะเป็นทีมที่ร่วมกันจัดทำแผนแม่บท IT มาแต่ต้น โดยต้องให้ทุกคนทราบและเห็นพ้องร่วมกันว่า ภารกิจไม่ได้เสร็จสิ้นลงแค่จัดทำแผน แต่หมายถึงต้อง implement ประเมินแผน และปรับปรุงต่อเนื่องให้ IT ก่อประโยชน์แก่โรงพยาบาลอย่างแท้จริงด้วย

กำหนดแผนการ implement ให้ชัดเจน ควรมีการกำหนดแผนการให้ชัดเจนว่า แต่ละแผนงาน/โครงการจะ implement อย่างไร เมื่อไร โดยกำหนดเป็น Gantt chart พร้อมทั้งกำหนดเป้าหมาย ผู้รับผิดชอบ ระยะเวลา และกระบวนการในการ implement ให้ครบถ้วน โดยคำนึงถึงผลกระทบต่องานประจำให้เกิดน้อยที่สุด หรือจัดการลดผลกระทบดังกล่าวด้วย รวมทั้งแนวทางในการประเมินความสำเร็จของแผน การกำหนดแผนการ implement นี้ควรคำนึงถึง success factor ของการ implement เป็นส่วนสำคัญของแผนด้วย

เนื่องจากแผนแม่บท IT ส่วนใหญ่การ implement ทำในรูปของ project และอาจมีผลกระทบต่อระบบงานต่างๆของโรงพยาบาลจำนวนมาก ดังนั้นจึงควรนำกระบวนการ **Project Management** และ **IT change management** มาใช้ร่วมด้วยเสมอ

สื่อสารแผนให้ทุกคนที่เกี่ยวข้อง (ทั้งโรงพยาบาล) รับทราบ เข้าใจ และปฏิบัติตาม แผนแม่บท IT รวมทั้งเอกสารที่เกี่ยวข้องต้องจัดทำเป็นเอกสารที่ผู้เกี่ยวข้องสามารถเข้าถึงได้โดยสะดวก สรุปเป็นภาษาที่เข้าใจได้ง่าย จะเป็นการดีหากสามารถสรุปแผนแม่บท IT เป็นข้อความที่เข้าใจง่าย จำนวน 1-2 หน้าเพื่อให้คนส่วนใหญ่เข้าใจ ควรใช้ข้อความที่ชัดเจน บ่งบอกถึงความเปลี่ยนแปลงที่จะเกิดขึ้น โดยเน้นถึงประโยชน์ที่จะเกิดขึ้นกับผู้ป่วย และโรงพยาบาล รวมทั้งผลที่อาจเกิดกับผู้ปฏิบัติงานและการเตรียมตัวเพื่อตอบรับกับสิ่งใหม่ๆ เหล่านี้ การสื่อสารอาจใช้หลายๆ ช่องทางร่วมกัน เช่นการแจ้งในการประชุมระดับต่างๆ โปสเตอร์ web และ social media เป็นต้น

การสื่อสารแผนแม่บทนี้มีความจำเป็นเพื่อให้เกิดการปฏิบัติตามแผนในแนวทางเดียวกัน รวมทั้งให้ฝ่ายต่างๆ เกิดความเข้าใจ ลดการต่อต้าน และดำเนินการตามแผนยุทธศาสตร์ของโรงพยาบาลและของแต่ละแผนกสอดคล้องไปกับแผนแม่บท IT ด้วย

<u>การติดตามประเมินผล</u>

เมื่อ implement แผนงาน โครงการ ตามแผนแม่บท IT แล้ว ต้องมีการติดตามประเมินผล เพื่อดูว่าแผนที่ implement ไปนั้นบรรลุวัตถุประสงค์หรือไม่เพียงไร มีปัญหาอุปสรรคอย่างไร และนำผลการติดตามมาปรับปรุงแผนในรอบต่อไป ตาม PDCA (plan – do – check – act) cycle เพื่อให้สามารถบรรลุผลตามที่ต้องการ

บทที่ 2

การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

Hospital IT Risk Management

การจัดการความเสี่ยง (Risk Management) เป็นกลไกสำคัญ สำหรับการควบคุมคุณภาพระบบงานทุกระบบ เพราะหากเราต้องการให้ระบบงานมีคุณภาพ เราต้องประเมินและตรวจสอบความเสี่ยงที่จะให้ระบบงานของเราด้อยคุณภาพให้ครอบคลุมความเสี่ยงทุกด้าน แล้วจัดการป้องกันไม่ให้ความเสี่ยงเหล่านั้นมีโอกาสมารบกวนและทำให้ระบบงานของเราด้อยคุณภาพลงไปได้

ระบบเทคโนโลยีสารสนเทศโรงพยาบาลก็เป็นระบบหนึ่งที่ต้องใช้การจัดการความเสี่ยงเป็นกลไกสำคัญในการควบคุมเพื่อให้มั่นใจว่าระบบดำเนินไปได้อย่างมีคุณภาพ ดังนั้น ผู้บริหาร และผู้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศโรงพยาบาลจึงต้องมีความเข้าใจวิธีการจัดการความเสี่ยงเป็นอย่างดี เพื่อให้สามารถดำเนินการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่ (Vulnerabilities)
2. ภัยคุกคาม (Threats)

จุดอ่อน (Vulnerabilities) หมายถึง ข้อบกพร่องทางด้าน กายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคลากร การบริหารจัดการ ครุภัณฑ์ โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีการติดตั้งกุญแจประตูห้องเครื่องแม่ข่าย
- ไม่มีระบบดักจับควัน และระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบเครื่องแม่ข่าย
- ไม่กำหนดขั้นตอนมาตรฐานในการสำรองข้อมูล
- บุคลากรไม่ทำตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีเครื่องแม่ข่ายสำรอง
- ใช้โปรแกรมระบบงานสำคัญร่วมกับโปรแกรมส่วนตัว
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ
- ไม่มีการควบคุมการเข้าถึงข้อมูล สารสนเทศที่สำคัญ

ภัยคุกคาม (Threats) หมายถึง ภัยอันตรายต่างๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่นๆ อันมีโอกาสจะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังตัวอย่างต่อไปนี้

- ไฟไหม้
- น้ำท่วม
- ขโมย

- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

ความเสี่ยง (Risk) คือความเป็นไปได้หรือโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบ โดยจุดอ่อนของระบบจะเพิ่มโอกาสให้ภัยคุกคามเข้ามาสร้างความเสียหายให้กับระบบเทคโนโลยีสารสนเทศได้ การจัดการความเสี่ยงจึงมีเป้าหมายสำคัญเพื่อ ลดโอกาส ที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบนั่นเอง

ขั้นตอนสำคัญในการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วย ขั้นตอนดังต่อไปนี้

1. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)
2. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management Strategic Planning)
3. การดำเนินการจัดการความเสี่ยง (Risks Treatment)

1. การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป

มาตรฐาน ISO/IEC 27001 : 2013 [1] ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS) ได้กล่าวถึงความเสี่ยงในระบบเทคโนโลยีสารสนเทศไว้มากมาย ดังตัวอย่างเช่น

- acts of terrorism การก่อการร้าย
- air conditioning failure ระบบปรับอากาศหยุดทำงาน
- airborne particles/dust ฝุ่นละออง
- bomb attack การวางระเบิด
- breach of legislation or regulations การละเมิดนโยบายและระเบียบปฏิบัติด้านความปลอดภัย
- breaches of contractual obligations การละเมิดข้อตกลงหรือสัญญาที่ผูกพัน
- compromise of security ความย่อหย่อนในระบบรักษาความปลอดภัย
- damage caused by penetration tests ความเสียหายจากการทดลองเจาะเข้าระบบ
- damage caused by third parties ความเสียหายจากบุคคลที่สาม
- destruction of records ข้อมูลถูกทำลาย

- destruction of the business continuity plans แผนกู้คืนถูกทำร้าย
- deterioration of media สื่อที่เก็บข้อมูลเสื่อมสภาพ
- disasters (natural or man-made) ภัยพิบัติ (จากธรรมชาติ หรือจากมนุษย์)
- ฯลฯ

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจาก การตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้แบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่พัฒนาโดย สมาคมเวชสารสนเทศไทย [2] (ดูแบบประเมินในหน้าถัดไป) โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

1. โอกาสที่จะเกิดความเสี่ยงนั้น (Probability)
2. ความเสียหายที่จะเกิดขึ้น (Impact)

การคำนวนคะแนนความเสี่ยง

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

ประเมินผลเสียหาย มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

คะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

การประเมินความเสี่ยง โอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1 ต่ำมาก	มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2 ต่ำ	มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3 ปานกลาง	มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4 สูง	มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5 สูงมาก	มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

1 ต่ำมาก	ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2 ต่ำ	มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3 ปานกลาง	มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1-2 แผนก
4 สูง	มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก
5 สูงมาก	มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล พัฒนาโดยสมาคมเวชสารสนเทศไทย ปีพ.ศ. ***2556***

TMI Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware	1 2 3 4 5	1 2 3 4 5	
1.1 Servers Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.2 Network Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.3 Workstations Failure	1 2 3 4 5	1 2 3 4 5	
1.4	1 2 3 4 5	1 2 3 4 5	
2. IT – System Software	1 2 3 4 5	1 2 3 4 5	
2.1 Operating System Failure	1 2 3 4 5	1 2 3 4 5	
2.2	1 2 3 4 5	1 2 3 4 5	
3. IT – Applications	1 2 3 4 5	1 2 3 4 5	
3.1 Front Offices	1 2 3 4 5	1 2 3 4 5	
3.2 Back Offices	1 2 3 4 5	1 2 3 4 5	
3.3	1 2 3 4 5	1 2 3 4 5	
4. IT – Communications, Connectivity	1 2 3 4 5	1 2 3 4 5	
4.1 Intranet	1 2 3 4 5	1 2 3 4 5	
4.2 Internet	1 2 3 4 5	1 2 3 4 5	
4.3	1 2 3 4 5	1 2 3 4 5	
5. IT – Operational (Human) Error	1 2 3 4 5	1 2 3 4 5	
5.1 Backup Error	1 2 3 4 5	1 2 3 4 5	
5.2 Data Loss Error	1 2 3 4 5	1 2 3 4 5	
5.3	1 2 3 4 5	1 2 3 4 5	
6. IT –Project Failure	1 2 3 4 5	1 2 3 4 5	
6.1 Inappropriate System Analysis	1 2 3 4 5	1 2 3 4 5	
6.2 Inappropriate System Design	1 2 3 4 5	1 2 3 4 5	
6.3 Inadequate Resources	1 2 3 4 5	1 2 3 4 5	
6.4 Poor Project Management	1 2 3 4 5	1 2 3 4 5	
6.5	1 2 3 4 5	1 2 3 4 5	
7. IT –Future Development	1 2 3 4 5	1 2 3 4 5	
7.1 No Data Dictionary	1 2 3 4 5	1 2 3 4 5	
7.2 No System Blueprint	1 2 3 4 5	1 2 3 4 5	
7.3 No Program Document or Comments	1 2 3 4 5	1 2 3 4 5	
7.4	1 2 3 4 5	1 2 3 4 5	
8. IT – Vendor and Outsource Failure	1 2 3 4 5	1 2 3 4 5	
8.1 Vendor Stop Support	1 2 3 4 5	1 2 3 4 5	
8.2	1 2 3 4 5	1 2 3 4 5	
9. IT – Hacking, Unauthorized Intrusions	1 2 3 4 5	1 2 3 4 5	
10. Environment Factors	1 2 3 4 5	1 2 3 4 5	
10.1 Flooding – Internal	1 2 3 4 5	1 2 3 4 5	
10.2 Flooding – External	1 2 3 4 5	1 2 3 4 5	
10.3 Fire – Internal	1 2 3 4 5	1 2 3 4 5	
10.4 Fire – External	1 2 3 4 5	1 2 3 4 5	
10.5 Utilities – Electricity	1 2 3 4 5	1 2 3 4 5	
10.6 Criminal – Theft	1 2 3 4 5	1 2 3 4 5	
10.7 Criminal – Break-ins	1 2 3 4 5	1 2 3 4 5	
10.8 Civil Unrest – Protest, Mob	1 2 3 4 5	1 2 3 4 5	
10.9	1 2 3 4 5	1 2 3 4 5	
11. Other	1 2 3 4 5	1 2 3 4 5	
	1 2 3 4 5	1 2 3 4 5	

เมื่อคำนวนคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยงดังนี้

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15		
	High	4	4	8	12	16	
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เราต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)

2. การวางแผนกลยุทธ์จัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

เมื่อเสร็จสิ้นขั้นตอนการประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปจะเป็นการวางแผนกลยุทธ์จัดการความเสี่ยง โดยเริ่มการจัดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยงดังนี้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

ความเสี่ยง	คะแนน	แถบสี	ความหมาย
ต่ำ	1 - 3		Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	4 - 9		Tolerable but caution or Management Discretion/Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	10 - 16		Intolerable or Attention Required/High Risk ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	17 - 25		Intolerable or Immediate Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ทันที

จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยง เราจะสามารถเรียงลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้ โดย เหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูงมาก (17-25) จะถือว่ามีค่าความเสี่ยงในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้โดยทันที จึงต้องเขียนแผนจัดการความเสี่ยงเหตุการณ์ระดับนี้โดยกำหนดลำดับความสำคัญเป็นลำดับแรก ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูง และปานกลาง จะกำหนดลำดับความสำคัญไว้เป็นลำดับต่อมา

เมื่อกำหนดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้แล้ว ขั้นตอนต่อไป คือการกำหนดวิธีแก้ไขความเสี่ยง (Risk Treatment) ให้กับเหตุการณ์ต่างๆ โดยมีทางเลือกกลยุทธ์ในการแก้ไขความเสี่ยง [3] ทั้งหมด 4 กลยุทธ์ดังนี้

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง เป็นการกำหนดมาตรการควบคุมให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง และ/หรือ ร่วมกับมาตรการควบคุมให้ผลเสียหายลดลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. ไฟไหม้เครื่องแม่ข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งเครื่องตัดไฟอัตโนมัติเมื่อเกิดกระแสไฟรั่วหรือกระแสไฟเกินในห้องเครื่องแม่ข่าย 2. เปลี่ยนฝ้าเพดานและผนังห้องเครื่องแม่ข่ายให้เป็นวัสดุไม่ติดไฟ 3. ห้ามสูบบุหรี่ ห้ามนำวัสดุติดไฟง่ายเข้าใกล้เครื่องแม่ข่าย
	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ติดตั้งเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันทีเมื่อเครื่องแม่ข่ายจริงหยุดทำงาน โดยติดตั้งไว้อีกตึกหนึ่งของโรงพยาบาล 2. สำรองข้อมูลลงแถบแม่เหล็กทุกวัน นำแถบแม่เหล็กออกไปเก็บไว้นอกโรงพยาบาล 3. จัดทำแผนกู้คืนเครื่องแม่ข่าย และซ้อมแผนกู้คืนปีละ 2 ครั้ง
2. ไวรัสโจมตีระบบเครือข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. แยกระบบเชื่อมต่ออินเทอร์เน็ตออกจากระบบงานโรงพยาบาล 2. ติดตั้งโปรแกรมสำรวจ ป้องกันและกำจัดไวรัสในระบบเครือข่าย 3. ห้ามผู้ใช้งานระบบ นำ USB Drive มาถ่ายโอนข้อมูลกับเครื่องคอมพิวเตอร์ของโรงพยาบาล
	ลดผลเสียหายเมื่อเกิดเห่ตุการณ์	1. ติดตั้งเครือข่ายสำรองที่สามารถกำหนดให้เป็นเครือข่ายจริงได้ทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้เป็นอิสระจากเครือข่ายจริง 2. ทำสัญญากับบริษัทผู้เชี่ยวชาญด้านระบบเครือข่าย ให้ส่งผู้เชี่ยวชาญมาแก้ปัญหาให้ภายใน 4 ชั่วโมง 3. จัดทำแผนดำเนินงานเมื่อระบบเครือข่ายล่ม ซ้อมแผนปีละ 2 ครั้ง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง เป็นการย้ายผลเสียหายที่เกิดขึ้นจากเหตุการณ์ที่ทำให้เกิดความเสี่ยงไปสู่บุคคลอื่น มักใช้ในกรณีที่องค์กรไม่สามารถลดความเสี่ยงได้ หรือไม่คุ้มค่าที่จะลงทุนลดความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. เครื่องคอมพิวเตอร์ถูกขโมย	ย้ายผลเสียหายไปอยู่ในความรับผิดชอบของบริษัทประกันภัย	ทำประกันภัยเครื่องคอมพิวเตอร์ทุกเครื่องจากภัยโจรกรรม
2. เครื่องแม่ข่ายชำรุด	ย้ายกระบวนการกู้คืนเครื่องแม่ข่ายไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญากับบริษัทขายเครื่องแม่ข่ายให้ต้องจัดเครื่องสำรองเตรียมไว้ให้ตลอด 24 ชม. ถ้าเครื่องเสียต้องยกเครื่องสำรองมาทดแทนทันที 2. ทำสัญญาจ้างบริษัทภายนอกให้รับผิดชอบกรณีเครื่องแม่ข่ายชำรุด ต้องรับดำเนินการกู้คืนให้สำเร็จภายใน 1 ชั่วโมง
3. เครื่องพิมพ์เสีย	ย้ายกระบวนการซ่อมและกระบวนการบริการเครื่องพิมพ์ให้พร้อมใช้ไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้บริษัทต้องตั้งเครื่องพิมพ์สำรองพร้อมทดแทนไว้ 5 เครื่อง ถ้ามีเครื่องเสียต้องยกเครื่องอื่นมาให้ใช้แทนได้ภายใน 24 ชั่วโมง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง เป็นการเปลี่ยนแปลงวิธีการทำงาน หรือกำหนดกิจกรรมเพิ่มเติมเพื่อให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. พัฒนาโปรแกรมเสร็จโดยเปล่าประโยชน์ (ผู้ใช้ไม่นำไปใช้งาน)	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ในขั้นตอนวิเคราะห์ความต้องการของผู้ใช้ เพิ่มการทำรายงานผลการวิเคราะห์ความต้องการให้ผู้ใช้ตรวจสอบและรับรอง 2. ในการออกแบบระบบ เพิ่มการทำเอกสารการออกแบบหน้าจอ ขั้นตอนการบันทึกข้อมูล และการทำรายงานให้ผู้ใช้ตรวจสอบ ปรับปรุงแก้ไข และรับรอง
2. เครื่องคอมพิวเตอร์ติดไวรัส	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ปิดการใช้งาน USB Drive 2. ตั้งเวลาให้โปรแกรมสแกนหาไวรัสในเครื่องทุกๆวัน ในช่วงเวลาพักรับประทานอาหารกลางวัน
3. เจ้าหน้าที่ลบข้อมูลผิดรายการ	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	เปลี่ยนแปลงโปรแกรมโดยกำหนดให้ไม่สามารถลบข้อมูลออกจากฐานข้อมูลได้ โดยให้ใช้การยกเลิกข้อมูลที่ผิดพลาดและเพิ่มข้อมูลใหม่ที่ถูกต้องเข้าไปทดแทนได้

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง เป็นการบันทึกผลการวิเคราะห์และยอมรับความเสี่ยงในเรื่องที่มีโอกาสเกิดได้น้อยและ/หรือไม่คุ้มค่าที่จะลงทุนในการจัดการความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	เหตุผลในการยอมรับความเสี่ยง
1. การสูญเสียข้อมูลในฐานข้อมูลและข้อมูลที่สำรองไว้จนหมดในเวลาเดียวกัน	ยอมรับความเสี่ยง	ฐานข้อมูลของโรงพยาบาลและข้อมูลที่สำรองเก็บไว้ที่คนละตึกของโรงพยาบาล ที่ไม่ได้อยู่ในหมู่ตึกเดียวกัน มีระยะห่างกัน 800 เมตร โอกาสที่จะสูญเสียข้อมูลทั้งสองพร้อมกัน เช่น ไฟไหม้ทั้งสองตึก มีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง
2. สายเชื่อมต่ออินเทอร์เน็ตขาดการเชื่อมต่อพร้อมกันทั้ง 2 สาย	ยอมรับความเสี่ยง	การเชื่อมต่ออินเทอร์เน็ตของโรงพยาบาลมี 2 จุดเชื่อมต่อ คือบริษัท A และบริษัท B โอกาสที่จุดเชื่อมต่อ 2 จุดจะขาดการเชื่อมต่อพร้อมกันมีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง

3. การดำเนินการจัดการความเสี่ยง

การดำเนินการจัดการความเสี่ยงเริ่มจากการจัดสรรทรัพยากร บุคคล เงิน และเวลา ที่ต้องใช้ในการจัดการความเสี่ยงแต่ละเรื่อง โดยอาจจัดทำเป็นโครงการ และใช้การจัดการโครงการ (Project Management) เป็นเครื่องมือช่วยให้การดำเนินการจัดการความเสี่ยงประสบผลสำเร็จต่อไป โดยอาจใช้แผนกิจกรรมจัดการความเสี่ยง ดังตัวอย่างในหน้าถัดไป เป็นเครื่องมือในการติดตามและควบคุมการดำเนินการจัดการความเสี่ยง

การประเมินผลและการพัฒนาคุณภาพอย่างต่อเนื่อง

เมื่อหน่วยงานดำเนินการจัดการความเสี่ยงไปแล้ว ควรมีการประเมินผลกิจกรรมจัดการความเสี่ยงที่ได้ดำเนินการไปแล้วว่าได้ผลหรือไม่ทุกๆ 3-6 เดือน โดยการเก็บข้อมูลอุบัติการณ์ต่างๆอันเป็นเหตุการณ์ที่ทำให้เกิดความเสี่ยงทุกรายการ ทำสถิติอุบัติการณ์ และวิเคราะห์แนวโน้มการเปลี่ยนแปลงว่า มีการเปลี่ยนแปลงไปในทางที่ดีขึ้นหรือไม่ โดยต้องประเมินคะแนนความเสี่ยงใหม่ เพื่อตรวจสอบว่าคะแนนความเสี่ยงลดลงหรือไม่ ถ้าพบว่าแนวโน้มดีขึ้น ย่อมแสดงว่ากิจกรรมจัดการความเสี่ยงที่ได้ดำเนินมาแล้วเป็นไปอย่างถูกต้องสมควร แต่หากแนวโน้มความเสี่ยงใดไม่ลดลง หรือเพิ่มขึ้น ก็สมควรปรับแก้ไข หรือเพิ่มกิจกรรมจัดการความเสี่ยง ให้ดีขึ้นกว่าเดิมอย่างต่อเนื่อง

การพัฒนาระบบจัดการความเสี่ยงการจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล สามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระยะ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

ระดับที่ 1

กระบวนการทำงาน	ผลผลิต
1. การจัดทำทะเบียนทรัพยากรด้านเทคโนโลยีสารสนเทศ 2. การประเมินความเสี่ยงที่จะเกิดขึ้นต่อทรัพยากรด้านเทคโนโลยีสารสนเทศ 3. การวางกลยุทธ์เพื่อจัดการความเสี่ยง 4. การจัดทำแผนปฏิบัติการเพื่อจัดการความเสี่ยง 5. การประเมินผลการจัดการความเสี่ยง 6. การวิเคราะห์ผลการจัดการความเสี่ยงและพัฒนาเป็นแผนการจัดการความเสี่ยงในรอบปีต่อไป	1. ทะเบียน Hardware, Software, Network และข้อมูลสำคัญ 2. รายงานผลการประเมินความเสี่ยง 3. แผนกลยุทธ์การจัดการความเสี่ยง 4. แผนปฏิบัติการเพื่อจัดการความเสี่ยง 5. รายงานผลการประเมินตามดำเนินการแผนจัดการความเสี่ยง 6. แผนการจัดการความเสี่ยงในรอบปีต่อไป

ระดับที่ 2

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. การประเมินความเสี่ยงที่จะเกิดขึ้นต่อทรัพยากรด้านเทคโนโลยีสารสนเทศในปัจจุบัน 3. วิเคราะห์เปรียบเทียบรายการความเสี่ยงเดิมกับรายการความเสี่ยงที่ประเมินใหม่ 4. การจัดทำแผนปฏิบัติการเพื่อจัดการความเสี่ยง 5. การประเมินผลการจัดการความเสี่ยง 6. การวิเคราะห์ผลการจัดการความเสี่ยงและพัฒนาเป็นแผนการจัดการความเสี่ยงในรอบปีต่อไป	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. รายงานผลการประเมินความเสี่ยง 3. รายงานผลการวิเคราะห์เปรียบเทียบ 4. แผนปฏิบัติการเพื่อจัดการความเสี่ยง 5. รายงานผลการประเมินตามดำเนินการแผนจัดการความเสี่ยง 6. แผนการจัดการความเสี่ยงในรอบปีต่อไป

ระดับที่ 3

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. การประเมินความเสี่ยงที่จะเกิดขึ้นต่อทรัพยากรด้านเทคโนโลยีสารสนเทศในปัจจุบัน 3. เพิ่มการประเมินความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดอันตรายต่อการดูแลรักษาผู้ป่วย 4. วิเคราะห์เปรียบเทียบรายการความเสี่ยงเดิมกับรายการความเสี่ยงที่ประเมินใหม่ 5. การจัดทำแผนปฏิบัติการเพื่อจัดการความเสี่ยง 6. การประเมินผลการจัดการความเสี่ยง 7. การวิเคราะห์ผลการจัดการความเสี่ยงและพัฒนาเป็นแผนการจัดการความเสี่ยงในรอบปีต่อไป	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. รายงานผลการประเมินความเสี่ยง 3. รายงานผลการวิเคราะห์เปรียบเทียบ 4. แผนปฏิบัติการเพื่อจัดการความเสี่ยง 5. รายงานผลการประเมินตามดำเนินการแผนจัดการความเสี่ยง 6. แผนการจัดการความเสี่ยงในรอบปีต่อไป

REFERENCES

1. ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements. (2013). Retrieved November 2, 2013, from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

2. สมาคมเวชสารสนเทศไทย. (2556). แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล. นนทบุรี. สมาคมเวชสารสนเทศไทย.

3. จิรพร สุเมธีประสิทธิ์, มัทธนา พิพิธเนาวรัตน์ และ กิตติพันธ์ คงสวัสดิ์เกียรติ. (2556). การบริหารความเสี่ยงอย่างมืออาชีพ. กรุงเทพ. สำนักพิมพ์แมคกรอ-ฮิล.

4. Brown, Carol. (2012). Managing Information Technology, 7th Edition. New Jersey: Prentice Hall.

(ตัวอย่าง) แผนดำเนินการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน เวชระเบียนและสถิติ หน่วยงาน เวชระเบียนผู้ป่วยนอกใน วันที่จัดทำ 1 มกราคม 2556

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 1. ข้อมูลและเอกสารสำคัญ, อ้างอิง เวชระเบียนผู้ป่วยใน	ไฟไหม้ เปียกน้ำ ถูกขโมย ปลวกกัดกิน หนู แมลงสาบ แทะ	1. จัดซื้อกุญแจล็อคแทนระบบล็อคเดิมที่ใช้การไม่ได้ ติดตั้งระบบกุญแจ		5,000 บาท	มค. – กพ. 2556
		2. จัดซื้อเครื่อง scanner ความเร็วสูงเพื่อ scan เอกสารเข้าสู่ระบบอิเล็กทรอนิกส์		80,000 บาท	มค. – กพ. 2556
		3. scan เอกสารที่สำคัญเข้าระบบเวชระเบียนอิเล็กทรอนิกส์ (ประมาณการเอกสาร จำนวน 500,000 หน้า)		200,000 บาท	กพ. – มีค. 2556
		4. จัดทำตารางการเข้าตรวจสอบกำจัดหนู เพื่อให้บริษัทดำเนินการทุกเดือน ควบคุมดูแล		--	กพ. 2556
หมวด 2. ครุภัณฑ์ระบบสารสนเทศ 2.1 เครื่องคอมพิวเตอร์ หมายเลข 1 2.2 เครื่องคอมพิวเตอร์ หมายเลข 2 2.3 เครื่องพิมพ์ HP2010 หมายเลข 1 2.4 เครื่องพิมพ์ EpsonLX800 หมายเลข 2	ถูกไวรัส ข้อมูลถูกลบโดยไม่ตั้งใจ	5. มอบนโยบายและระเบียบปฏิบัติการใช้เครื่องคอมพิวเตอร์ ตามมาตรฐานความปลอดภัยให้กับผู้ปฏิบัติงานทุกคน		--	กพ. 2556
		6. กำกับดูแลให้เกิดการปฏิบัติตามระเบียบ สุ่มตรวจสอบการกระทำที่ละเมิดระเบียบ		--	มีค. – ธค. 2556

บทที่ 3

การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล (Security Management in Hospital Information System)

การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทำงานได้อย่างราบรื่น ไม่หยุดชะงัก หรือสะดุดติดขัด โดยหัวใจหลักคือการสร้างระบบจัดการความมั่นคงปลอดภัย (Security Management System) ให้มั่นใจว่ามาตรการต่างๆที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยดำเนินไปได้อย่างต่อเนื่องและยั่งยืนอ

การจัดการความมั่นคงปลอดภัยเป็นกิจกรรมที่สัมพันธ์กับการจัดการความเสี่ยง เพราะกิจกรรมจัดการความเสี่ยงเป็นส่วนหนึ่งของระบบจัดการความมั่นคงปลอดภัย แต่ในรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย (Thai Medical Informatics Association Hospital Information System Maturity Model) ได้แยกการจัดการความเสี่ยงไว้เป็นหัวข้อหลักอีกหัวข้อหนึ่ง เพื่อให้เห็นว่า การจัดการความเสี่ยงเป็นกิจกรรมที่ต้องให้ความสำคัญโดยเฉพาะในระยะเริ่มต้นของการพัฒนาคุณภาพ

การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล สามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระดับ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

กระบวนการสำคัญ	ผลผลิต
1. การจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัย	1. ประกาศนโยบาย
2. การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติไปสู่ผู้ใช้ระบบทุกคน	2. ประกาศระเบียบปฏิบัติ
3. การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน	3. เอกสารประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ
4. การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน	4. รายงานผลการประเมินความรับรู้
5. การวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ	5. รายงานผลการประเมินความเข้าใจ
6. การปรับระเบียบปฏิบัติให้ผู้ใช้ระบบเข้าใจได้ง่าย ไม่กำกวม	6. รายงานการวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ
7. การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน	7. รายงานผลการเพิ่มความรับรู้และเข้าใจ

ระดับที่ 1 (ต่อ)

กระบวนการสำคัญ	ผลผลิต
8. การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 9. การวิเคราะห์ผลการประเมินการปฏิบัติตามระเบียบ 10. การปรับปรุงศูนย์ข้อมูล (Data center – server room) 11. จัดทำแผนการดำเนินการของหน่วยงานต่างๆเมื่อระบบล่ม (Business Continuity Plan – BCP) และแผนดำเนินการเมื่อเกิดภัยพิบัติ เช่น อัคคีภัย	8. รายงานผลการประเมินการปฏิบัติตามระเบียบปฏิบัติ 9. รายงานการวิเคราะห์ผลการประเมินตามระเบียบปฏิบัติ 10. รายงานผลการปรับปรุงศูนย์ข้อมูล 11. แผน BCP แผนรับภัยพิบัติ

ระดับที่ 2

กระบวนการสำคัญ	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. ปรับปรุงนโยบายและระเบียบปฏิบัติที่ยังไม่ชัดเจน กำกวม 3. เพิ่มระเบียบปฏิบัติด้านการเข้าถึงข้อมูลผู้ป่วย การป้องกันความลับและความเป็นส่วนตัวของข้อมูลผู้ป่วย รวมถึงการส่งข้อมูลผู้ป่วยผ่านสื่อโซเชียลมีเดีย 4. รประชาสัมพันธ์นโยบายและระเบียบปฏิบัติไปสู่ผู้ใช้ระบบทุกคน 5. การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 6. การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 7. การวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ 8. การปรับระเบียบปฏิบัติให้ผู้ใช้ระบบเข้าใจได้ง่าย ไม่กำกวม 9. การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 10. การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 11. การวิเคราะห์ผลการประเมินการปฏิบัติตามระเบียบ 12. ทบทวนผลการปรับปรุงศูนย์ข้อมูลในระยะที่ 1 13. การปรับปรุงศูนย์ข้อมูลระยะที่ 2 14. ปรับปรุงแผน BCP และแผนรับภัยพิบัติ	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. ประกาศนโยบายฉบับปรับปรุงใหม่ 3. ประกาศระเบียบปฏิบัติฉบับปรับปรุงใหม่ 4. เอกสารประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ 5. รายงานผลการประเมินความรับรู้ 6. รายงานผลการประเมินความเข้าใจ 7. รายงานการวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ 8. รายงานผลการเพิ่มความรับรู้และเข้าใจ 9. รายงานผลการประเมินการปฏิบัติตามระเบียบปฏิบัติ 10. รายงานการวิเคราะห์ผลการประเมินตามระเบียบปฏิบัติ 11. รายงานผลการทบทวนการปรับปรุงศูนย์ข้อมูลในระยะที่ 1

ระดับที่ 2 (ต่อ)

กระบวนการสำคัญ	ผลผลิต
15. ซ้อมแผน BCP และแผนรับภัยพิบัติ	12. รายงานผลการปรับปรุงศูนย์ข้อมูลในระยะที่ 2 13. รายงานผลการซ้อมแผน BCP และ แผนภัยพิบัติ

ระดับที่ 3

กระบวนการสำคัญ	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. ปรับปรุงนโยบายและระเบียบปฏิบัติที่ยังไม่ชัดเจน กำกวม 3. การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 4. การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 5. การวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ 6. การปรับระเบียบปฏิบัติให้ผู้ใช้ระบบเข้าใจได้ง่าย ไม่กำกวม 7. การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 8. การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน 10. การวิเคราะห์ผลการประเมินการปฏิบัติตามระเบียบ 11. ทบทวนผลการปรับปรุงศูนย์ข้อมูลในระดับที่ 2 10. การปรับปรุงศูนย์ข้อมูลระดับที่ 3 11. จัดทำแผนกู้คืน และแผนการตรวจสอบความมั่นคง 12. ซ้อมดำเนินการตามแผนกู้คืน 13. วิเคราะห์ผลการซ้อมแผนกู้คืน	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. ประกาศนโยบายฉบับปรับปรุงใหม่ 3. ประกาศระเบียบปฏิบัติฉบับปรับปรุงใหม่ 4. เอกสารประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ 5. รายงานผลการประเมินความรับรู้ 6. รายงานผลการประเมินความเข้าใจ 7. รายงานการวิเคราะห์ผลการประเมินความรับรู้และเข้าใจ 8. รายงานผลการเพิ่มความรับรู้และเข้าใจ 9. รายงานผลการประเมินการปฏิบัติตามระเบียบปฏิบัติ 10. รายงานการวิเคราะห์ผลการประเมินตามระเบียบปฏิบัติ 11. รายงานผลการทบทวนการปรับปรุงศูนย์ข้อมูลในระยะที่ 2 12. รายงานผลการปรับปรุงศูนย์ข้อมูลในระยะที่ 3 13. แผนกู้คืน แผนการตรวจสอบ 14. รายงานผลการซ้อมแผนกู้คืน 15. รายงานการวิเคราะห์ผลการซ้อมแผนกู้คืน

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล
ระดับที่ 1 ของการพัฒนา

ระยะแรก เป็นการวางพื้นฐานที่จำเป็นในการสร้างความมั่นคงปลอดภัยให้เกิดขึ้นในระบบเทคโนโลยีสารสนเทศโรงพยาบาล ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

1.1 การจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัย

นโยบายด้านความมั่นคงปลอดภัย เป็นแนวทางที่ผู้บริหารระดับสูงกำหนดทิศทางการดำเนินงานเพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศนโยบายฉบับนี้จึงเป็นการแสดงเจตจำนงค์ให้ทุกฝ่ายที่เกี่ยวข้องกับโรงพยาบาล ไม่ว่าจะเป็นผู้ป่วย ญาติผู้ป่วย เจ้าหน้าที่ทุกฝ่ายในโรงพยาบาล ตลอดจนคู่สัญญาภายนอกของโรงพยาบาลได้รับรู้แนวทางและจุดยืนของโรงพยาบาล

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

- โรงพยาบาล จะดำเนินการจัดการเพื่อป้องกันความลับและความเป็นส่วนตัวของผู้ป่วยอย่างเคร่งครัด
- โรงพยาบาลมีนโยบายใช้ซอฟท์แวร์ที่ไม่ละเมิดลิขสิทธิ์เท่านั้น
- การใช้ทรัพยากรเทคโนโลยีสารสนเทศของโรงพยาบาล ต้องเป็นไปเพื่อการดำเนินกิจกรรมตามพันธกิจและภารกิจของโรงพยาบาลเท่านั้น

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัย เป็นข้อกำหนดที่ให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตาม เพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศระเบียบปฏิบัติจึงเป็นสิ่งที่เจ้าหน้าที่ทุกคนต้องรับรู้ และปฏิบัติตามโดยเคร่งครัด โดยหากไม่ปฏิบัติตามควรมีมาตรฐานตักเตือนหรือลงโทษตามสมควร

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

- (เจ้าหน้าที่ทุกคน) ต้องเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
- ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลเพื่อความบันเทิง เช่น ดูหนัง ฟังเพลง เล่นเกมส์ ฯลฯ
- ห้ามติดตั้งโปรแกรมใดๆเพิ่มเติมลงในเครื่องคอมพิวเตอร์ของโรงพยาบาล หากมีความจำเป็นให้ขออนุมัติจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายหน้าที่จากผู้อำนวยการเท่านั้น

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลสามารถแบ่งกลุ่มตามลักษณะผู้ใช้ได้ 3 กลุ่มดังนี้

1. ระเบียบปฏิบัติสำหรับผู้บริหาร (ระดับสูง ระดับกลาง ระดับต้น)
2. ระเบียบปฏิบัติสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ
3. ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน

ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน เป็นระเบียบที่สำคัญที่สุด เพราะต้องบังคับใช้กับบุคคลหมู่มาก จึงต้องเขียนโดยใช้ข้อความที่ชัดเจน ไม่กำกวม เข้าใจได้ง่าย ไม่ตีความบิดเบือนเป็นอย่างอื่นได้

ทั้งนโยบายและระเบียบปฏิบัติ ควรจัดทำเป็นประกาศของโรงพยาบาล โดยผู้อำนวยการลงนามและประกาศให้ผู้ที่เกี่ยวข้องทุกคนได้รับรู้โดยทั่วกัน โดยเมื่อประกาศใช้งานไปแล้ว สามารถทบทวนและปรับปรุงแก้ไขให้ทันสมัยหรือเหมาะสมต่อสถานการณ์ในอนาคตได้ต่อไป

1.2 การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติไปสู่ผู้ใช้ระบบทุกคน

เมื่อมีการประกาศนโยบายและระเบียบปฏิบัติออกมาแล้ว ต้องมีการประชาสัมพันธ์ให้มั่นใจว่า ผู้ใช้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลทุกคน ได้รับรู้ระเบียบปฏิบัติฉบับที่สำคัญที่สุด คือระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน กิจกรรมประชาสัมพันธ์เป็นกิจกรรมที่สำคัญมาก เพราะการประกาศเรื่องราวใดๆ ในโรงพยาบาลตามช่องทางปกติมักจะไม่สามารถสื่อสารไปสู่บุคลากรหมู่มากของโรงพยาบาลได้ โรงพยาบาลหลายแห่งใช้ช่องทางเครือข่ายภายใน (Intranet) เพื่อนำประกาศต่างๆไปใส่ไว้ แต่เรามักจะพบว่า เจ้าหน้าที่โรงพยาบาลส่วนใหญ่จะไม่สนใจอ่านประกาศต่างๆเหล่านั้น ดังนั้น หากนำระเบียบปฏิบัติที่สำคัญนี้ไปประกาศไว้ในช่องทางปกติ เจ้าหน้าที่ส่วนใหญ่จะยังคงไม่รับรู้ว่ามีระเบียบนี้ให้ปฏิบัติตาม

การประชาสัมพันธ์ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสำหรับผู้ใช้งานระบบทุกคน ควรใช้ช่องทางประชาสัมพันธ์หลายช่องทาง โดยช่องทางประชาสัมพันธ์ที่อาจเลือกใช้ ได้แก่

1. ประกาศตามช่องทางประชาสัมพันธ์ปกติของโรงพยาบาล เช่น บอร์ดติดประกาศ Intranet ฯลฯ
2. จัดทำเป็นโปสเตอร์ ทำไปติดไว้ในสถานที่ที่เจ้าหน้าที่ของโรงพยาบาลมองเห็นได้โดยง่าย
3. จัดอบรมเจ้าหน้าที่ นำเสนอระเบียบปฏิบัติ เปิดโอกาสให้ซักถาม อภิปรายร่วมกัน
4. มอบหมายให้หัวหน้าหน่วยงาน นำระเบียบไปแจ้งในที่ประชุมหน่วยงานให้เจ้าหน้าที่ทุกคนทราบ

ในกรณีที่ ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน มีข้อปฏิบัติมากเกินกว่า 1 หน้ากระดาษ เช่น มีข้อปฏิบัติ 30-50 ข้อ ควรคัดเลือกระเบียบปฏิบัติที่สำคัญที่สุด มาจัดทำเป็นหน้าเดียวดังตัวอย่างในภาพที่ 3.1

ประกาศโรงพยาบาล[redacted]
เรื่อง ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐
(ฉบับผู้ใช้งานทั่วไป)

.....

ข้อ ๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

ข้อ ๒ ผู้ใช้งานห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก เช่น Flash Drive , External Drive , CD-Rom เป็นต้น กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย HOSxP, X-Ray และ Lab ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานห้ามทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔ ห้ามผู้ใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๕ ผู้ใช้งานห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖ ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook), ไลน์ (Line), เว็บไซต์ (Website) หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยหรือญาติซึ่งยินยอมเผยแพร่ได้เป็นครั้งคราว

ข้อ ๗ ผู้ใช้งานต้องรับผิดชอบป้องกันความเสียหาย ที่อาจจะเกิดขึ้น กับเครื่องคอมพิวเตอร์ , ปริ้นเตอร์, ปลั๊กไฟ หรืออุปกรณ์อิเลคทรอนิกส์ เช่น ไม่วางอาหารหรือน้ำดื่ม บนเครื่องคอมพิวเตอร์ ,ไม่ใช้งานปลั๊กที่ไฟชำรุด เป็นต้น

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศใช้ ณ วันที่ พฤศจิกายน พ.ศ.๒๕๖๐

ภาพที่ 3.1 ตัวอย่าง ระเบียบปฏิบัติฉบับคัดเลือกข้อปฏิบัติให้เหลือเนื้อหาอยู่ในหน้าเดียว

1.3 การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประชาสัมพันธ์ระเบียบปฏิบัติไปสู่ผู้ใช้ระบบแล้ว ต้องมีกระบวนการประเมินความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน เพื่อให้ทราบว่า การประชาสัมพันธ์ระเบียบนั้นได้ผลมากน้อยเพียงใด โดยก่อนการประเมินจะต้องรวบรวมข้อมูลจากผู้ดูแลระบบมาให้ครบถ้วนเสียก่อนว่าผู้ใช้งานระบบมีทั้งหมดกี่คน ทำงานอยู่ในหน่วยงานใดบ้าง เพื่อจะได้ดำเนินการประเมินได้ครบทุกคน

วิธีการประเมินความรับรู้ระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือ การให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความรับรู้เสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความรับรู้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 499 คน คิดเป็นร้อยละ 99.80

การรับรู้ระเบียบ

ข้อที่ 1	รู้ 400 คน ไม่รู้ 99 คน	การรับรู้คิดเป็นร้อยละ 80.16
ข้อที่ 2	รู้ 450 คน ไม่รู้ 49 คน	การรับรู้คิดเป็นร้อยละ 90.18
ข้อที่ 3	รู้ 420 คน ไม่รู้ 79 คน	การรับรู้คิดเป็นร้อยละ 84.17
ข้อที่ 4	รู้ 350 คน ไม่รู้ 149 คน	การรับรู้คิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่รับรู้มากที่สุดคือข้อที่ 2 ข้อที่ไม่รับรู้มากที่สุดคือข้อที่ 4

สาเหตุที่ไม่รู้ระเบียบ เป็นเพราะไม่ได้อ่านโดยละเอียด อ่านแล้วจำไม่ได้ ขาดสมาธิตอนเข้ารับการอบรม หรือ เข้ารับการอบรมไม่ครบทุกหัวข้อ

เสนอแนะแนวทางแก้ไข

เพิ่มการให้ความรู้แก่บุคลากรที่ยังขาดความรู้ด้านระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การรับรู้ทุกหัวข้อ มีสัดส่วนการรับรู้ไม่ต่ำกว่า ร้อยละ 95

1.4 การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประเมินความรับรู้แล้ว ต้องมีกระบวนการประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคนด้วย เพื่อให้ทราบว่า ผู้ใช้ระบบเข้าใจระเบียบแต่ละข้ออย่างถูกต้องหรือไม่ เพราะบางครั้ง ผู้ใช้อาจจะเข้าใจความหมายของระเบียบปฏิบัติแต่ละข้อไม่ถูกต้อง

วิธีการประเมินความเข้าใจระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือ การให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความเข้าใจเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความเข้าใจระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100

ความเข้าใจระเบียบ

ข้อที่ 1	เข้าใจ 400 คน ไม่เข้าใจ 99 คน	ความเข้าใจคิดเป็นร้อยละ 80.16
ข้อที่ 2	เข้าใจ 450 คน ไม่เข้าใจ 49 คน	ความเข้าใจคิดเป็นร้อยละ 90.18
ข้อที่ 3	เข้าใจ 420 คน ไม่เข้าใจ 79 คน	ความเข้าใจคิดเป็นร้อยละ 84.17
ข้อที่ 4	เข้าใจ 350 คน ไม่เข้าใจ 149 คน	ความเข้าใจคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่เข้าใจมากที่สุดคือข้อที่ 2 ข้อที่ไม่เข้าใจมากที่สุดคือข้อที่ 4

สาเหตุที่ไม่เข้าใจระเบียบ เป็นเพราะอ่านไม่รู้เรื่อง ไม่เข้าใจศัพท์ที่ใช้ ความหมายกำกวม

เสนอแนะแนวทางแก้ไข

ปรับปรุงแก้ไขข้อความที่ทำให้อ่านไม่รู้เรื่อง เพิ่มการอธิบายแก่บุคลากรที่ยังไม่เข้าใจระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้ความเข้าใจทุกหัวข้อ มีสัดส่วนความเข้าใจไม่ต่ำกว่า ร้อยละ 95

1.5 การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

ถ้าผลการประเมินการรับรู้และความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน ยังไม่เป็นที่น่าพอใจ ต้องพิจารณาว่าสาเหตุที่ทำให้ผู้ใช้ระบบไม่รับรู้หรือไม่เข้าใจระเบียบเกิดจากอะไร เพื่อจะได้ดำเนินการแก้ไขให้ถูกทาง เช่น ระเบียบที่ประกาศใช้ไปแล้วมีบางข้อที่ผู้ใช้อ่านไม่รู้เรื่อง ก็ควรปรับปรุงข้อความให้อ่านแล้วเข้าใจได้โดยง่าย หรือ ผู้ใช้ระบบจำระเบียบไม่ได้เพราะการอบรมมีเนื้อหามากเกินไป ก็ควรปรับปรุงวิธีการอบรมให้ดีขึ้นกว่าเดิม

การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติ ทำได้หลายวิธี เช่น การให้ความรู้ซ้ำหลายๆครั้ง เปลี่ยนช่องทางการให้ข้อมูล หรือเพิ่มช่องทางการให้ข้อมูล กำหนดมาตรการให้รางวัลแก่ผู้ที่สนใจและรับรู้ระเบียบได้อย่างดี ฯลฯ

1.6 การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อมั่นใจว่าผู้ใช้ระบบทุกคน มีความรู้และความเข้าใจระเบียบปฏิบัติเป็นอย่างดีแล้ว ก็ควรติดตามประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย เพราะถึงแม้จะมีความรู้และความเข้าใจเรื่องระเบียบแล้ว แต่บางคนก็ยังคงไม่ปฏิบัติตามระเบียบ ทีมงานพัฒนาคุณภาพจึงต้องสร้างระบบตรวจสอบประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย

วิธีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศของโรงพยาบาล สามารถดำเนินการได้หลายวิธี ได้แก่

1. แบบประเมินตนเอง ให้ผู้ใช้ระบบตอบคำถามว่า ระเบียบข้อใดบ้างที่ปฏิบัติตาม ระเบียบข้อใดที่ไม่ปฏิบัติ สาเหตุที่ทำให้ไม่ปฏิบัติตามระเบียบคืออะไร ฯลฯ การให้ตอบแบบประเมินตนเองนี้ มีข้อดีตรงที่ทำได้โดยง่าย และใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่นได้ แต่ข้อเสียของการประเมินด้วยวิธีนี้คือ การที่ผู้ประเมินตนเองอาจประเมินไม่ตรงตามการปฏิบัติจริง

2. การสังเกตโดยตรงจากผู้ประเมิน วิธีนี้ผู้ประเมินจะเข้าไปสังเกตวิธีปฏิบัติงานของผู้ใช้ระบบโดยตรง โดยอาจไม่บอกให้รู้ล่วงหน้าว่าจะมีการเข้าประเมิน การประเมินแบบนี้ มีข้อดีตรงที่ได้ข้อมูลเหตุการณ์การละเมิดระเบียบปฏิบัติที่เกิดขึ้นจริง ส่วนข้อเสียคือ อาจไม่สามารถประเมินด้วยวิธีนี้ได้ทุกหัวข้อของระเบียบที่ประกาศไป

3. การจำลองสถานการณ์ เป็นการสร้างสถานการณ์เพื่อทดสอบว่า ผู้ใช้ระบบปฏิบัติตามระเบียบปฏิบัติได้ตรงตามที่กำหนดไว้ เช่น มีระเบียบปฏิบัติให้ผู้ใช้ระบบต้อง log off จากระบบเมื่อไม่ได้ใช้งาน ก็อาจจะลองโทรศัพท์เรียกใช้ผู้ใช้ระบบให้ออกไปจากหน้าจอ แล้วสังเกตดูว่า ผู้ใช้ระบบ log off จากระบบหรือไม่ การจำลองสถานการณ์มีข้อดี คือ ใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่นๆ แต่มีข้อเสียคือต้องใช้บุคลากรในการประเมินหลายคน และเสียเวลาในการประเมินมาก

การประเมินผลการปฏิบัติตามระเบียบปฏิบัตินี้ ควรกำหนดให้มีการประเมินโดยสม่ำเสมอ เช่น ทุกๆ 1-3 เดือน เพื่อคอยติดตามสถานการณ์ว่า เกิดการละเมิดระเบียบปฏิบัติมากน้อยแค่ไหน หากเกิดการละเมิดระเบียบปฏิบัติเป็นจำนวนมาก ควรค้นหาสาเหตุและหาทางแก้ไขปัญหาโดยเร่งด่วน

เมื่อประเมินการปฏิบัติตามระเบียบปฏิบัติเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาล ..... ครั้งที่ 1/2561

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100

ความปฏิบัติตามระเบียบ

ข้อที่ 1	ปฏิบัติ 400 คน ไม่ปฏิบัติ 99 คน	การปฏิบัติตามคิดเป็นร้อยละ 80.16
ข้อที่ 2	ปฏิบัติ 450 คน ไม่ปฏิบัติ 49 คน	การปฏิบัติตามคิดเป็นร้อยละ 90.18
ข้อที่ 3	ปฏิบัติ 420 คน ไม่ปฏิบัติ 79 คน	การปฏิบัติตามคิดเป็นร้อยละ 84.17
ข้อที่ 4	ปฏิบัติ 350 คน ไม่ปฏิบัติ 149 คน	การปฏิบัติตามคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

สรุปผลการประเมิน

ระเบียบข้อที่ปฏิบัติตามมากที่สุดคือข้อที่ 2 ข้อที่ละเมิดมากที่สุดคือข้อที่ 4

สาเหตุที่ละเมิดระเบียบ เป็นเพราะไม่สนใจที่จะทำตาม ไม่ตระหนักถึงความสำคัญที่จะต้องดำเนินการตามระเบียบ

เสนอแนะแนวทางแก้ไข

ให้รางวัลแก่บุคลากรที่สามารถปฏิบัติตามระเบียบปฏิบัติได้เป็นอย่างดี กำหนดมาตรการลงโทษผู้ที่ละเมิดระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การปฏิบัติตามระเบียบทุกหัวข้อ มีสัดส่วนการปฏิบัติไม่ต่ำกว่าร้อยละ 95

1.7 การปรับปรุง Data Center ให้ได้มาตรฐาน

Data Center หากแปลเป็นภาษาไทยว่าศูนย์ข้อมูลอาจทำให้เข้าใจผิดว่าเป็นแหล่งเก็บเอกสารหรือห้องสมุด แต่ตามความเป็นจริงแล้วคำว่า Data Center ในที่นี้ ห้องที่ติดตั้งเครื่องแม่ข่าย (server) ของโรงพยาบาล นั่นเอง เป็นห้องที่จำกัดการเข้าถึง มีระบบควบคุมอุณหภูมิ และระบบรักษาความมั่นคงปลอดภัยต่างๆ

การปรับปรุง Data Center ให้ได้มาตรฐานควรมีการดำเนินการในด้านต่างๆดังต่อไปนี้

A. การจัดการทางกายภาพของสถานที่ ควรมีการจัดการทางกายภาพดังนี้

- ระบบล็อคประตูและการควบคุมติดตามการเข้าไปในห้อง เช่น สมุดบันทึกการเข้าออก
- ควรยกระดับพื้นห้องถ้ามีเครื่อง Server ใหญ่ที่วางแนบติดกับพื้นห้อง
- ระบบปรับอากาศที่ทำให้อุณหภูมิคงที่ ไม่ร้อนเกินไป ระบบสลับการทำงานของเครื่องปรับอากาศให้เหมาะสม
- เซ็นเซอร์ตรวจวัดอุณหภูมิ และระบบแจ้งเตือนเมื่ออุณหภูมิสูงเกินไป
- ระบบตรวจจับควัน และระบบแจ้งเตือนอัคคีภัย
- มีเครื่องดับเพลิงที่ใช้ดับเพลิงจากระบบคอมพิวเตอร์โดยเฉพาะ
- กำกับดูแลให้มีการทำความสะอาดภายในห้องอย่างสม่ำเสมอ

B. การจัดระเบียบของอุปกรณ์และสายสัญญาน ควรมีการจัดระเบียบดังนี้

- สายสัญญานทั้งด้านหน้าและด้านหลังควรจัดให้เป็นระเบียบเรียบร้อย ไม่เป็นขยุ้ม ไม่กองเป็นก้อนบนพื้นห้องจนไม่สามารถทำความสะอาดพื้นได้
- จัดทำป้ายกำกับสายสัญญานทุกเส้นให้รู้ว่าเป็นสายที่มาจากที่ใด หรือต่อไปที่ใด
- จัดทำแผนผังระบุตำแหน่งของสายสัญญานและช่องสัญญานทุกช่อง
- จัดทำป้ายกำกับ server ทุกเครื่อง รวมถึงอุปกรณ์เครือข่าย หรืออุปกรณ์หลักอื่นๆ

C. ระบบคงทนต่อความผิดพลาดและระบบความมั่นคงพื้นฐาน ควรมีการจัดระบบดังนี้

- ระบบสำรองข้อมูลแบบ online และ offline ของ server ที่เก็บข้อมูลทุกตัว
- ระบบคงทนต่อความผิดพลาดต่างๆ ของ server, hard disk ., backbone, main switch รวมถึงระบบเชื่อมต่ออินเทอร์เน็ต
- การจัดระบบเครือข่ายภายในให้เหมาะสม การจัด VLAN การแยกช่องทางการเข้าถึงอินเทอร์เน็ตไม่ให้เชื่อมต่อกับฐานข้อมูลหลักของการบริการผู้ป่วย
- ระบบ firewall ป้องกันการโจมตีจากภายนอก
- ระบบ log เก็บข้อมูลการติดต่อภายนอก รวมถึง Event ที่สำคัญในอุปกรณ์ต่างๆ
- กำกับดูแลให้มีการทำความตรวจสอบระบบอย่างสม่ำเสมอ

D. การควบคุมการดำเนินงานที่เกี่ยวข้องกับ Data Center ควรมีการควบคุมดังนี้

- การสำรองข้อมูลแบบ online และ offline ของ server อย่างสม่ำเสมอ รวมถึงการตรวจสอบข้อมูลที่สำรองไปว่าเป็นข้อมูลที่ไม่เสียหาย สามารถนำกลับมาใช้ได้เมื่อเกิดเหตุ
- การตรวจสอบอุปกรณ์สำคัญต่างๆ การเฝ้าติดตามการใช้ทรัพยากรระบบ เหตุการณ์ต่างๆ
- ควบคุมการดำเนินการของบริษัทภายนอกที่เกี่ยวข้องกับ Data Center อย่างใกล้ชิด

1.8 การจัดทำแผนดำเนินการเมื่อระบบคอมพิวเตอร์ใช้การไม่ได้

แผนดำเนินการเมื่อระบบคอมพิวเตอร์ใช้งานไม่ได้ (Business Continuity Plan – BCP) เป็นเอกสารแสดงขั้นตอนต่างๆที่ผู้ใช้ระบบคอมพิวเตอร์ในแผนกต่างๆของโรงพยาบาลสำหรับบริการผู้ป่วยจะต้องนำมาปฏิบัติตามเมื่อเกิดเหตุใดๆที่ทำให้ระบบล่ม หรือหยุดชะงัก การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่างๆที่เจ้าหน้าที่ในแต่ละตำแหน่งของทุกแผนกจะต้องเข้าใจและปฏิบัติตามได้ตลอดระยะเวลาที่ระบบล่ม จนกว่าระบบจะกลับมาใช้งานได้อีกครั้งหนึ่ง

แผน BCP ที่สำคัญที่สุด คือแผน BCP กรณีระบบคอมพิวเตอร์ที่ให้บริการผู้ป่วยนอกล่ม โดยระบบคอมพิวเตอร์ที่ให้บริการผู้ป่วยนอกส่วนใหญ่จะครอบคลุมหน่วยงานของโรงพยาบาลดังต่อไปนี้

1. แผนกเวชระเบียนผู้ป่วยนอก
2. พยาบาลห้องตรวจโรคผู้ป่วยนอก
3. แพทย์ที่ปฏิบัติหน้าที่ตรวจรักษาผู้ป่วยนอก
4. ห้องปฏิบัติการชันสูตร (Lab)
5. แผนกรังสีวิทยา (Radiology service)
6. ห้องจ่ายยา (Pharmacy service)
7. แผนกการเงินผู้ป่วยนอก

ทุกแผนกนี้ต้องมีแผน BCP ของตนเอง ที่ระบุรายละเอียดขั้นตอนที่สำคัญที่ใช้บริการผู้ป่วยนอกของแต่ละแผนกโดยไม่มีระบบคอมพิวเตอร์สนับสนุน เช่น ในแผน BCP ของแผนกเวชระเบียน ต้องกล่าวถึงขั้นตอนการให้บริการผู้ป่วยนอกดังนี้

- การลงทะเบียนผู้ป่วยใหม่ การออกเลข HN
- การค้นหาบัตรผู้ป่วยเก่า
- การส่งบัตรผู้ป่วยไปยังห้องตรวจต่างๆ
- การรับบัตรกลับมาเมื่อสิ้นสุดการบริการ
- การบันทึกข้อมูลย้อนหลังเมื่อระบบคอมพิวเตอร์กลับมาสู่สถานะปกติ

นอกจากแผน BCP แล้ว ทุกแผนกต้องจัดเตรียมแบบฟอร์มที่เกี่ยวข้องเพื่อใช้บริการผู้ป่วยโดยการเขียนกระดาษ ทั้งนี้ต้องเตรียมแบบฟอร์มในปริมาณที่เพียงพอและจัดให้มีครบทุกแบบฟอร์มที่จำเป็นด้วย

1.9 การจัดทำแผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center

แผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center เป็นเอกสารแสดงขั้นตอนต่างๆที่ผู้ดูแล Data Center จะต้องนำมาปฏิบัติตามเมื่อภัยพิบัติ เช่น อัคคีภัย อุทกภัย ฯลฯ การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่างๆที่เจ้าหน้าที่จะต้องเข้าใจและปฏิบัติตามได้อย่างรวดเร็ว ถูกต้องตามขั้นตอน เมื่อเกิดภัยพิบัติ มีขั้นตอนต่างๆที่ระบุรายละเอียดไว้อย่างชัดเจน เช่น

- เมื่อพบไฟไหม้ในห้อง Data Center จะทำอย่างไร แจ้งใครบ้าง
- ระหว่างดับไฟ ต้องดำเนินการอย่างไรเพิ่มเติม
- กรณีไฟไหม้นอกห้อง Data Center จะประเมินสถานการณ์อย่างไร
- หากดับไฟไม่ได้จะขนย้ายอุปกรณ์ใดก่อน ขนอย่างไร
- เมื่อดับไฟได้แล้ว จะมีขั้นตอนในการฟื้นฟูระบบให้กลับสู่สถานการณ์ปกติอย่างไร

1.10 การซ้อมปฏิบัติการตามแผน BCP และแผนปฏิบัติการเมื่อเกิดภัยพิบัติ

ควรจัดให้มีการซ้อมปฏิบัติการตามแผน BCP และแผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center อย่างน้อยปีละ 1 ครั้ง โดยระหว่างการซ้อมจะต้องมีการบันทึกสิ่งที่เกิดขึ้นจริง รวมทั้งระยะเวลาที่ใช้ไปในแต่ละขั้นตอน ให้ละเอียด เพื่อนำผลการซ้อมมาวิเคราะห์และหาทางปรับปรุงแผนให้ดีขึ้นต่อไป

ระดับ 2 การสร้างความแข็งแรงระบบความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 2 ของการพัฒนา

การยกระดับการจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 2 เป็นการสร้างความแข็งแรงให้กับระบบที่กำเนิดขึ้นมาในระดับที่ 1 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้จริงและทำให้งานดีขึ้น ระดับที่ 2 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

2.1 ทบทวนผลการดำเนินงานในระดับที่ 1

ก่อนที่จะมีการยกระดับการพัฒนา ควรทบทวนผลการดำเนินในระดับที่ 1 โดยใช้หลักการ Plan-Do-Check-Act กล่าวคือ การดำเนินงานในระดับที่ 1 เป็นขั้นตอนของ Plan และ Do เมื่อดำเนินการไปสักระยะหนึ่ง ก็ควร ทบทวนประเมินผล (Check) ก่อนจะที่ยกระดับเป็นระดับที่ 2 (Act) ต่อไปนั่นเอง การประเมินการดำเนินงานที่ผ่านมา จะทำให้เราเห็นโอกาสที่จะปรับปรุงนโยบายและระเบียบปฏิบัติที่ยังไม่ครอบคลุมประเด็นสำคัญ หรือไม่ชัดเจน ให้ครอบคลุมประเด็นสำคัญและชัดเจนมากขึ้น เพื่อทำให้ความรับรู้

ความเข้าใจ และการปฏิบัติตามระเบียบปฏิบัติมีผลลัพธ์ที่ดีขึ้น รวมถึงการปรับปรุงศูนย์ข้อมูลให้เป็นไปตามมาตรฐานมากขึ้น ดังนั้น การดำเนินการในระดับที่ 2 จึงเป็นการทำซ้ำการดำเนินการในระดับที่ 1 อีกรอบหนึ่ง แต่เป็นการหมุนวงล้อ PDCA ที่ทำให้ระดับคุณภาพสูงขึ้น

อย่างไรก็ตาม การดำเนินการในระดับที่ 2 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการเพิ่มระเบียบปฏิบัติด้านการเข้าถึงข้อมูลผู้ป่วย การป้องกันความลับและความเป็นส่วนตัวของข้อมูลผู้ป่วย เพื่อให้เกิดการป้องกันความลับและความเป็นส่วนตัวของข้อมูลผู้ป่วยโดยเคร่งครัด

2.2 การเพิ่มระเบียบปฏิบัติด้านการเข้าถึงข้อมูลผู้ป่วย การป้องกันความลับและความเป็นส่วนตัวของข้อมูลผู้ป่วย รวมถึงการส่งข้อมูลผู้ป่วยผ่านสื่อโซเชียลมีเดีย

ข้อมูลผู้ป่วยที่อยู่ในระบบเวชระเบียนไม่ว่าจะเป็นเวชระเบียนที่เป็นกระดาษหรือเวชระเบียนอิเล็กทรอนิกส์ถือเป็นข้อมูลส่วนตัวที่ต้องได้รับการป้องกันอย่างเคร่งครัด ตามคำประกาศสิทธิของผู้ป่วยและกฎหมายหลายฉบับ เช่น พรบ.สุขภาพแห่งชาติ มาตราที่ 7 ฯลฯ

อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศโรงพยาบาลในประเทศไทย ยังไม่มีกลไกป้องกันความเป็นส่วนตัวของข้อมูลผู้ป่วย แพทย์ที่เข้าสู่ระบบ สามารถเรียกดูข้อมูลผู้ป่วยทุกคนได้โดยไม่มีการป้องกัน ซึ่งตามหลักการที่ถูกต้องแล้ว แพทย์ไม่ทราบเรียกดูข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองได้ ดังนั้น จึงควรมีการกำหนดระเบียบปฏิบัติห้ามผู้ใช้ระบบ เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในหน้าที่ความรับผิดชอบของผู้ใช้ระบบในขณะนั้น

นอกจากนั้น การส่งข้อมูลผู้ป่วยผ่านสื่อโซเชียลมีเดีย ก็เป็นการกระทำที่สุ่มเสี่ยงต่อการทำให้ข้อมูลของผู้ป่วยรั่วไหลและอาจเกิดความเสียหายต่อผู้ป่วยได้ แต่ในปัจจุบัน โรงพยาบาลหลายแห่งมีการใช้โปรแกรม LINE ส่งข้อมูลหรือภาพของผู้ป่วยไปปรึกษาแพทย์ที่อยู่นอกโรงพยาบาล จึงควรจะมีการกำหนดระเบียบปฏิบัติในเรื่องนี้ให้รัดกุม เช่น การขออนุญาตผู้ป่วยก่อนส่งข้อมูลทุกๆครั้ง และควรมีระเบียบกำกับการส่งข้อมูลให้ปลอดภัยด้วย

ระยะที่ 3 การสร้างความยั่งยืน ระบบความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 3 ของการพัฒนา

การยกระดับการจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 3 เป็นการสร้างความแข็งแรงให้กับระบบที่พัฒนาจากระดับที่ 1 และ 2 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้อย่างมั่นคงและยั่งยืน ระดับที่ 3 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

3.1 ทบทวนผลการดำเนินงานในระดับที่ 2

เป็นการหมุนวงล้อ PDCA รอบต่อไปที่ทำให้ระดับคุณภาพสูงขึ้นอีก แต่อย่างไรก็ตาม การดำเนินการในระยะที่ 3 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการจัดทำแผนกู้คืนและซ้อมปฏิบัติตามแผนกู้คืน และการจัดทำแผนตรวจสอบติดตามความมั่นคงและปฏิบัติการติดตามตรวจสอบความมั่นคง

3.2 การจัดทำแผนกู้คืน

แผนกู้คืน (Disaster Recovery Plan – DRP) เป็นเอกสารแสดงขั้นตอนต่างๆที่เจ้าหน้าที่คอมพิวเตอร์จะต้องนำมาปฏิบัติตามเมื่อเกิดเหตุใดๆที่ทำให้ server หยุดทำงาน การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่างๆที่เจ้าหน้าที่คอมพิวเตอร์ทุกคนเข้าใจและปฏิบัติตามได้เพื่อทำให้ได้ server ที่มีข้อมูลเดิมครบถ้วนนำกลับมาให้บริการเหมือนสภาวะปกติ โดยในแผนกู้คืนต้องกล่าวถึงขั้นตอนการดำเนินการดังตัวอย่างต่อไปนี้

- วิธีการจัดหา server ตัวใหม่โดยวิธีการเร่งด่วน (ในกรณีที่ server เดิมถูกทำลายทั้งหมด)
- การติดตั้งระบบปฏิบัติการให้เหมือนเครื่องเก่าทุกประการ
- การตั้งค่า configuration ของระบบปฏิบัติการให้เหมือนเครื่องเก่าทุกประการ
- การติดตั้งระบบฐานข้อมูลให้เหมือนเครื่องเก่าทุกประการ
- การตั้งค่า configuration ของระบบฐานข้อมูลให้เหมือนเครื่องเก่าทุกประการ
- การนำข้อมูลสำรองลงให้เหมือนเครื่องเก่าทุกประการ
- การทดสอบว่าข้อมูลอยู่ครบทุกประการ
- การติดตั้งโปรแกรมให้เหมือนเครื่องเก่าทุกประการ
- การติดตั้ง driver ให้เหมือนเครื่องเก่าทุกประการ

3.3 การซ้อมปฏิบัติการตามแผนกู้คืน

ควรจัดให้มีการซ้อมปฏิบัติการตามแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง โดยระหว่างการซ้อมจะต้องมีการบันทึกสิ่งที่เกิดขึ้นจริง รวมทั้งระยะเวลาที่ใช้ไปในแต่ละขั้นตอน ให้ละเอียด เพื่อนำผลการซ้อมมาวิเคราะห์และหาทางปรับปรุงแผนให้ดีขึ้นต่อไป

3.4 การจัดทำแผนตรวจสอบติดตามความมั่นคง

แผนตรวจสอบติดตามความมั่นคง (Security Monitoring and Control Plan) เป็นเอกสารที่กำหนดกิจกรรมการตรวจสอบติดตามความมั่นคงด้านต่างๆของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล โดยต้องระบุกิจกรรม ความถี่ในการตรวจสอบ ผู้ตรวจสอบและผู้ควบคุมให้ชัดเจน กิจกรรมการตรวจสอบและติดตามความมั่นคงปลอดภัย ได้แก่

- การตรวจสอบและติดตามการสำรองข้อมูล
- การตรวจสอบและติดตามการเข้าใช้ทรัพยากรระบบของผู้ใช้งาน
- การตรวจสอบและติดตามการโจมตีระบบ
- การตรวจสอบและติดตามการเข้าสู่ระบบจากบริษัทคู่สัญญาภายนอก
- การตรวจสอบและติดตามการบำรุงรักษาระบบ

บทที่ 4

การจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล (Service Management in Hospital Information System)

การจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้ผู้ใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทำงานได้อย่างราบรื่น ไม่หยุดชะงัก หรือสะดุดติดขัด โดยหัวใจหลักคือการกำหนดข้อตกลงระดับบริการ (Service Level Agreement) ให้มั่นใจว่า ผู้ใช้งานระบบจะได้รับการสนับสนุนจากฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลในการแก้ปัญหาเทคโนโลยีสารสนเทศ และการให้บริการด้านต่างๆภายในระยะเวลาที่ตกลงไว้ร่วมกัน

การทำให้ได้ตามข้อตกลงระดับบริการ จะเกิดขึ้นได้เมื่อมีการจัดระบบบริการที่มีคุณภาพ ซึ่งประกอบไปด้วยการจัดตั้งจุดบริการ (Service Desk) การจัดการอุบัติการณ์และปัญหา (Incident and Problem Management) รวมไปถึงการเฝ้าระวังติดตามผลการดำเนินงานและกิจกรรมของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

การจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล สามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระดับ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

ระดับที่ 1

กระบวนการทำงาน	ผลผลิต
1. การจัดตั้งจุดบริการ	1. จุดบริการ
2. การจัดทำข้อตกลงระดับบริการ	2. ประกาศข้อตกลงระดับบริการ
3. การประชาสัมพันธ์ข้อตกลงระดับบริการไปสู่ผู้ใช้ระบบทุกคน	3. เอกสารประชาสัมพันธ์ข้อตกลงระดับบริการ
4. การประเมินผลการดำเนินงานตามข้อตกลงระดับบริการ	4. รายงานผลการประเมินการดำเนินงานตามข้อตกลงระดับบริการ
5. การรวบรวมข้อมูลอุบัติการณ์	5. รายงานอุบัติการณ์
6. การวิเคราะห์ข้อมูลอุบัติการณ์	6. รายงานกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ
7. การบันทึกข้อมูลกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ	7. รายงานผลการประเมินความพึงพอใจ

ระดับที่ 1 (ต่อ)

กระบวนการทำงาน	ผลผลิต
8. การวิเคราะห์กิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ 9. การประเมินความพึงพอใจของผู้ใช้บริการ	

ระดับที่ 2

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. ปรับปรุงข้อตกลงระดับบริการที่ยังไม่เหมาะสม 3. การประเมินการดำเนินการตามข้อตกลงระดับบริการ 4. การวิเคราะห์ผลการดำเนินการตามข้อตกลงระดับบริการ 5. การจัดระบบจัดการอุบัติการณ์ 6. การจัดระบบจัดการปัญหา 7. การวิเคราะห์กิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ 8. การประเมินความพึงพอใจของผู้ใช้บริการ	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. ประกาศข้อตกลงระดับบริการฉบับปรับปรุงใหม่ 3. รายงานผลการดำเนินการตามข้อตกลงระดับบริการ 4. รายงานอุบัติการณ์ 5. รายงานปัญหา 6. รายงานกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ 7. รายงานผลการประเมินความพึงพอใจ

ระดับที่ 3

กระบวนการทำงานหลัก	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. ปรับปรุงข้อตกลงระดับบริการที่ยังไม่เหมาะสม 3. การประเมินการดำเนินการตามข้อตกลงระดับบริการ 4. การวิเคราะห์ผลการดำเนินการตามข้อตกลงระดับบริการ 5. การปรับระบบจัดการอุบัติการณ์ 6. การปรับระบบจัดการปัญหา 7. การวิเคราะกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ 8. การประเมินความพึงพอใจของผู้ใช้บริการ	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. ประกาศข้อตกลงระดับบริการฉบับปรับปรุงใหม่ 3. รายงานผลการดำเนินการตามข้อตกลงระดับบริการ 4. รายงานอุบัติการณ์ 5. รายงานปัญหา 6. รายงานกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ 7. รายงานการประเมินความพึงพอใจ

ระดับที่ 1 การเริ่มต้นจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล
ระดับที่ 1 ของการพัฒนา

ระดับแรก เป็นการวางพื้นฐานที่จำเป็นของระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

1.1 การจัดตั้งจุดบริการ

จุดบริการ หรือ Service Desk เป็นจุดที่จัดให้มีเจ้าหน้าที่คอยรับแจ้งปัญหาที่ผู้ใช้ระบบเทคโนโลยีสารสนเทศแจ้งเข้ามา แล้วให้บริการแก้ไขปัญหาเบื้องต้น รวบรวมปัญหาที่ต้องแก้ไขระยะกลางและระยะยา เก็บรวบรวมข้อมูลเพื่อนำมาวิเคราะห์สถานภาพการให้บริการของระบบให้ดำเนินไปอย่างต่อเนื่อง จุดบริการควรเป็นจุดที่ติดต่อได้โดยสะดวกทั้งทางโทรศัพท์และการเดินทางมาขอรับบริการ ควรมีเจ้าหน้าที่ประจำจุดอย่างเพียงพอและอาจจัดให้บริการได้ตลอด 24 ชั่วโมง

เจ้าหน้าที่ประจำจุดบริการ อาจทำหน้าที่รับแจ้งปัญหาแล้วส่งมอบงานแก้ปัญหาต่อให้กับเจ้าหน้าที่ผู้ชำนาญงานแต่ละด้าน หรืออาจช่วยแก้ปัญหาเบื้องต้นให้กับผู้ใช้ระบบไปก่อน จนพบว่าไม่สามารถแก้ปัญหาได้โดยง่ายจึงค่อยส่งมอบปัญหาต่อให้กับเจ้าหน้าที่ผู้ชำนาญงาน งานที่สำคัญอีกด้านของเจ้าหน้าที่ในจุดนี้ คือต้องจดบันทึกกิจกรรมการให้บริการให้ละเอียด โดยต้องบันทึกชื่อและหน่วยงานของผู้ขอรับบริการ เรื่องที่เป็นปัญหา เวลาที่รับแจ้ง เวลาที่เริ่มแก้ปัญหา เวลาที่แก้ปัญหาเสร็จ และเวลาที่ส่งมอบงานให้แก่ผู้ใช้ระบบ โดยข้อมูลเหล่านี้จะต้องนำมาวิเคราะห์ให้เห็นผลการดำเนินงานของจุดบริการ

1.2 การจัดทำข้อตกลงระดับบริการ

ข้อตกลงระดับบริการ (Service Level Agreement) เป็นข้อตกลงที่ฝ่ายเทคโนโลยีสารสนเทศรับประกันว่าผู้ใช้งานระบบเทคโนโลยีสารสนเทศจะได้รับบริการที่มีคุณภาพ การจัดทำข้อตกลงควรจัดทำจากการประชุมร่วมกันระหว่างผู้ใช้งานระบบกับฝ่ายเทคโนโลยีสารสนเทศ ข้อตกลงที่เกิดขึ้นมาจึงเป็นการแสดงเจตจำนงค์ให้ทุกฝ่ายที่เกี่ยวข้องกับฝ่ายเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นผู้บริหาร ผู้ใช้ระบบ หรือบริษัทคู่สัญญาภายนอกได้รับรู้แนวทางและจุดยืนด้านคุณภาพการให้บริการของฝ่ายเทคโนโลยีสารสนเทศ

ข้อตกลงระดับบริการ ควรกล่าวถึง รายการบริการที่รับประกันผลงาน โดยในระยะเริ่มต้นควรเลือกบริการที่ผู้ใช้งานระบบต้องการอย่างยิ่ง เช่น บริการแก้ปัญหาเมื่อระบบเทคโนโลยีสารสนเทศขัดข้องใช้การไม่ได้ ฯลฯ โดยรับประกันผลการดำเนินงานให้ชัดเจนวัดผลได้ เช่น สัญญาว่าจะแก้ปัญหาให้เสร็จสิ้นภายในเวลา 15 นาที แต่อาจจะระบุข้อจำกัดหรือข้อยกเว้นในกรณีที่ไม่รับประกันไว้ในข้อตกลงได้

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในข้อตกลงระดับบริการเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

ข้อตกลงระดับบริการ	การรับประกัน
1. การแก้ปัญหาระบบเทคโนโลยีสารสนเทศขัดข้อง	แก้ปัญหาให้เสร็จสิ้นภายใน 15 นาที (*)
2. การขอรายงาน	ออกรายงานให้ได้ภายใน 2 วันทำการ (**)
3. การขอเปิดบัญชีผู้ใช้รายใหม่	เปิดบัญชีผู้ใช้รายใหม่ได้ภายใน 24 ชม.

* เฉพาะกรณีปัญหาในจุดที่ให้บริการผู้ป่วยนอก ส่วนกรณี back office รับประกันเวลา 30 นาที

** เฉพาะการออกรายงานจากฐานข้อมูลที่มีข้อมูลอยู่แล้วครบถ้วนเท่านั้น

เมื่อจัดทำข้อตกลงระดับบริการเสร็จแล้ว ต้องมีการประกาศออกมาอย่างเป็นทางการแล้วดำเนินการประชาสัมพันธ์ให้ผู้ใช้ระบบทุกคนได้รับทราบ

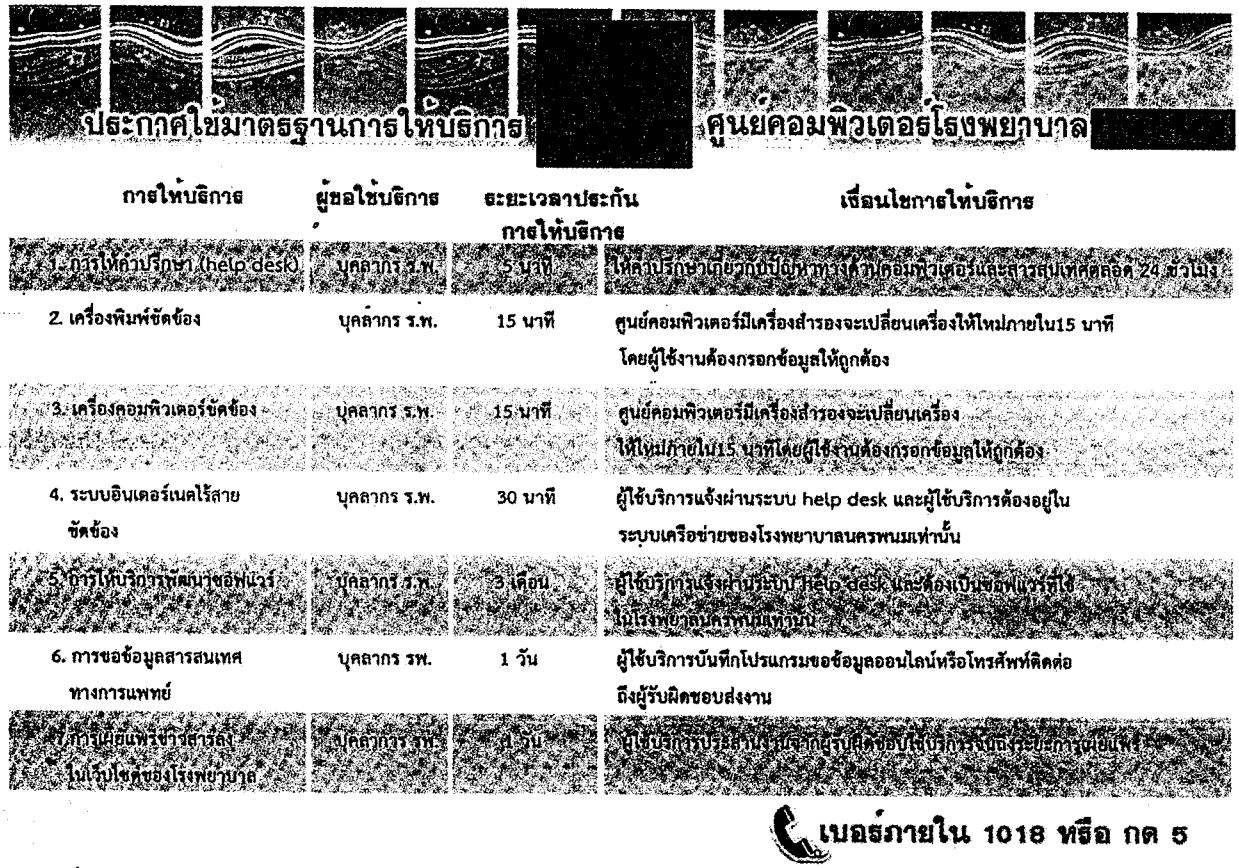
1.3 การประชาสัมพันธ์ข้อตกลงระดับบริการไปสู่ผู้ใช้ระบบทุกคน

การประชาสัมพันธ์ข้อตกลงระดับบริการ มีวัตถุประสงค์เพื่อทำให้มั่นใจว่า ผู้ใช้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลทุกคน ได้รับรู้ข้อตกลงระดับบริการซึ่งมีผลต่อผู้ใช้งานระบบทุกคน กิจกรรมประชาสัมพันธ์เป็นกิจกรรมที่สำคัญมาก เพราะการประกาศเรื่องราวใดๆในโรงพยาบาลตามช่องทางปกติมักจะไม่สามารถสื่อสารไปสู่บุคลากรหมู่มากของโรงพยาบาลได้ โรงพยาบาลหลายแห่งใช้ช่องทางเครือข่ายภายใน (Intranet) เพื่อนำประกาศต่างๆไปใส่ไว้ แต่เรามักจะพบว่า เจ้าหน้าที่โรงพยาบาลส่วนใหญ่จะไม่สนใจอ่านประกาศต่างๆเหล่านั้น ดังนั้น หากนำข้อตกลงระดับบริการนี้ไปประกาศไว้ในช่องทางปกติ เจ้าหน้าที่ส่วนใหญ่จะยังคงไม่รับรู้ว่ามีข้อตกลงนี้อยู่

การประชาสัมพันธ์ข้อตกลงระดับบริการด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสำหรับผู้ใช้งานระบบทุกคน ควรใช้ช่องทางประชาสัมพันธ์หลายช่องทาง โดยช่องทางประชาสัมพันธ์ที่อาจเลือกใช้ได้แก่

1. ประกาศตามช่องทางประชาสัมพันธ์ปกติของโรงพยาบาล เช่น บอร์ดติดประกาศ Intranet ฯลฯ
2. จัดทำเป็นโปสเตอร์ ทำไปติดไว้ในสถานที่ที่เจ้าหน้าที่ของโรงพยาบาลมองเห็นได้โดยง่าย
3. จัดอบรมเจ้าหน้าที่ นำเสนอข้อตกลงระดับบริการ เปิดโอกาสให้ซักถาม อภิปรายร่วมกัน
4. มอบหมายให้หัวหน้าหน่วยงาน นำข้อตกลงระดับบริการไปแจ้งในที่ประชุมหน่วยงานให้เจ้าหน้าที่ทุกคนทราบ

ควรจัดทำข้อตกลงระดับบริการ มาจัดทำเป็นเอกสารประชาสัมพันธ์หน้าเดียวดังตัวอย่างในภาพที่ 4.1



ภาพที่ 4.1 ตัวอย่าง ป้ายประชาสัมพันธ์ข้อตกลงระดับบริการ

1.4 การประเมินผลการดำเนินงานตามข้อตกลงระดับบริการ

เมื่อข้อตกลงระดับบริการไปสู่ผู้ใช้ระบบแล้ว ต้องมีกระบวนการประเมินผลการดำเนินการตามข้อตกลง เพื่อให้ทราบว่า การดำเนินการตามข้อตกลงนั้นได้ผลมากน้อยเพียงใด โดยก่อนการประเมินจะต้องจัดการให้เจ้าหน้าที่ในฝ่ายเทคโนโลยีสารสนเทศทุกคนที่ให้บริการผู้ใช้งาน ได้จดบันทึกกิจกรรมที่ให้บริการให้ครบทุกครั้ง โดยหัวข้อที่สำคัญ คือ ชื่อและหน่วยงานของผู้ขอรับบริการ เรื่องที่เป็นปัญหา เวลาที่รับแจ้ง เวลาที่เริ่มแก้ปัญหา เวลาที่แก้ปัญหาเสร็จ และเวลาที่ส่งมอบงานให้แก่ผู้ใช้ระบบ และชื่อของเจ้าหน้าที่ที่ให้บริการ

การวิเคราะห์ผลการดำเนินงานตามข้อตกลงระดับบริการ ควรนับจำนวนการให้บริการตามข้อตกลง วิเคราะห์ร้อยละความสำเร็จของการทำได้ตามข้อตกลง รวมถึงเวลาเฉลี่ย เวลาสูงสุด เวลาต่ำสุดที่ทำได้ และจัดทำรายการสรุปผลการดำเนินการตามข้อตกลงระดับบริการดังตัวอย่างต่อไปนี้

รายงานการดำเนินการตามข้อตกลงระดับบริการของฝ่ายเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561 มกราคม ถึง กุมภาพันธ์ 2561

ลำดับ	การให้บริการ	จำนวนปัญหา (ครั้ง)	จำนวนแก้ปัญหาได้ตามเวลา	ร้อยละความสำเร็จตามข้อตกลง
1	การให้คำปรึกษา (help desk)	585	585	100%
2	เครื่องพิมพ์ขัดข้อง	775	634	81.81%
3	เครื่องคอมพิวเตอร์ขัดข้อง	655	537	81.98%
4	ระบบอินเตอร์เน็ตไร้สายขัดข้อง	44	31	70.45%
5	การให้บริการพัฒนาซอร์ฟแวร์	54	39	72.22%
6	การขอข้อมูลสารสนเทศทางการแพทย์	686	667	97.23%
7	การให้บริการ เผยแพร่ข่าวสารลง website รพ.ฯ	191	190	100%

เวลาที่ใช้

ลำดับ	การให้บริการ	Max	Min	เวลาเฉลี่ย (นาที)
1	การให้คำปรึกษา (help desk)	10.5	2	4.5
2	เครื่องพิมพ์ขัดข้อง	25	10	15.5

(ยังมีต่อ)

สรุปผลการประเมิน

การดำเนินการตามข้อตกลงระดับบริการ ทำได้สำเร็จตามเป้าหมาย (80%) เกือบทุกหมวดยกเว้นหมวด 4 การแก้ปัญหาระบบอินเทอร์เน็ตไร้สาย และหมวด 5 การให้บริการพัฒนาซอฟท์แวร์ สาเหตุเกิดจากบุคลากรไม่เพียงพอ และภาระงานที่ยุ่งในบางช่วงเวลา

เสนอแนะแนวทางแก้ไข

ระยะสั้น ควรจัดทำ Problem Management เพื่อทำให้อุบัติการณ์คอมพิวเตอร์ขัดข้องลดน้อยลง เพื่อให้เจ้าหน้าที่มีเวลามากขึ้น ระยะยาว ควรจัดหาโปรแกรมเมอร์เพิ่มเติม

1.5 การรวบรวมข้อมูลอุบัติการณ์

อุบัติการณ์ (Incidence) หมายถึงเหตุการณ์ไม่พึงประสงค์ที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ ได้แก่ เหตุขัดข้องต่างๆ ภาวะที่ระบบหยุดชะงัก ความผิดพลาดที่เกิดขึ้นในระบบ ฯลฯ อุบัติการณ์ทำให้ผู้ใช้ระบบไม่สามารถทำงานได้อย่างราบรื่น มักจะต้องหยุดการทำงานเพื่อค้นหาสาเหตุและแก้ไขเหตุขัดข้องนั้นเสียก่อน จึงจะสามารถกลับมาทำงานต่อไปได้

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ต้องเก็บรวบรวมข้อมูลอุบัติการณ์ทั้งหมดที่เกิดขึ้นในระบบสารสนเทศ โดยผู้ที่รับแจ้งเหตุขัดข้องต้องจดบันทึกไว้ทุกครั้ง โดยบันทึกให้ครอบคลุมรายละเอียดที่สำคัญของอุบัติการณ์แต่ละครั้ง ได้แก่ ชื่อและหน่วยงานของผู้แจ้งเหตุขัดข้อง เรื่องที่เป็นปัญหา เวลาที่รับแจ้ง เวลาที่เริ่มแก้ปัญหา เวลาที่แก้ปัญหาเสร็จ และเวลาที่ส่งมอบงานให้แก่ผู้ใช้ระบบ และชื่อของเจ้าหน้าที่ที่ให้บริการ

1.6 การวิเคราะห์ข้อมูลอุบัติการณ์

ข้อมูลอุบัติการณ์ที่เก็บรวบรวมได้มานั้น ต้องทำการวิเคราะห์อย่างสม่ำเสมอ เพื่อให้รู้สถานการณ์ปัจจุบันว่า อุบัติการณ์ใดบ้างที่เกิดขึ้น เรื่องใดเกิดขึ้นมาก เกิดขึ้นกับหน่วยงานใด เป็นจากปัญหาด้านไหน ฯลฯ เมื่อวิเคราะห์เสร็จสิ้นแล้วก็ควรจัดทำรายงานอุบัติการณ์ ตามตัวอย่างต่อไปนี้

รายงานอุบัติการณ์ที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ

ของโรงพยาบาล ..... ครั้งที่ 1/2561 เดือน มกราคม 2561

Incidence	จำนวนครั้งที่เกิด
1. เครื่องคอมพิวเตอร์ขัดข้อง	65
2. เครื่องพิมพ์ขัดข้อง	55
3. ใช้งานอินเทอร์เน็ตไม่ได้	20
4. ข้อมูลที่บันทึกในระบบผิดพลาด	3

Incidence	สถานที่เกิดเหตุ
1. ห้องจ่ายยา	35
2. เวชระเบียนผู้ป่วยนอก	20
3. จุดพยาบาลคัดกรอง	18
4. งานการเงินผู้ป่วยนอก	15
5. ห้องตรวจของแพทย์	10

(รายงานผลแง่มุมอื่นๆ.....)

สรุปผลการประเมิน

อุบัติการณ์ที่เกิดขึ้นมากที่สุดคือเครื่องคอมพิวเตอร์ขัดข้อง รองลงมาเป็นเครื่องพิมพ์ขัดข้อง สาเหตุเกิดจากเครื่องคอมพิวเตอร์และเครื่องพิมพ์ที่มีอายุการใช้งาน 8 ปี

อุบัติการณ์เกิดขึ้นมากที่ห้องจ่ายยาและแผนกเวชระเบียนผู้ป่วยนอก เนื่องจากเป็นหน่วยงานที่มีเครื่องรุ่นเก่าจำนวนมาก

เสนอแนะแนวทางแก้ไข

ทยอยเปลี่ยนเครื่องคอมพิวเตอร์และเครื่องพิมพ์ใหม่ ให้กับหน่วยงานที่มีเครื่องที่มีอายุการใช้งานมากกว่า 7 ปี

1.7 การบันทึกข้อมูลกิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ

อุบัติการณ์ (Incidence) หมายถึงเหตุการณ์ไม่พึงประสงค์ที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ ได้แก่ เหตุขัดข้องต่างๆ ภาวะที่ระบบหยุดชะงัก ความผิดพลาดที่เกิดขึ้นในระบบ ฯลฯ อุบัติการณ์ทำให้ผู้ใช้ระบบไม่สามารถทำงานได้อย่างราบรื่น มักจะต้องหยุดการทำงานเพื่อค้นหาสาเหตุและแก้ไขเหตุขัดข้องนั้นเสียก่อน จึงจะสามารถกลับมาทำงานต่อไปได้

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ต้องเก็บรวบรวมข้อมูลอุบัติการณ์ทั้งหมดที่เกิดขึ้นในระบบสารสนเทศ โดยผู้ที่รับแจ้งเหตุขัดข้องต้องจดบันทึกไว้ทุกครั้ง โดยบันทึกให้ครอบคลุมรายละเอียดที่สำคัญของอุบัติการณ์แต่ละครั้ง ได้แก่ ชื่อและหน่วยงานของผู้แจ้งเหตุขัดข้อง เรื่องที่เป็นปัญหา เวลาที่รับแจ้ง เวลาที่เริ่มแก้ปัญหา เวลาที่แก้ปัญหาเสร็จ และเวลาที่ส่งมอบงานให้แก่ผู้ใช้ระบบ และชื่อของเจ้าหน้าที่ที่ให้บริการ

1.8 การวิเคราะห์กิจกรรมการทำงานของฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลอุบัติการณ์ที่เก็บรวบรวมได้มานั้น ต้องทำการวิเคราะห์อย่างสม่ำเสมอ เพื่อให้รู้สถานการณ์ปัจจุบันว่า อุบัติการณ์ใดบ้างที่เกิดขึ้น เรื่องใดเกิดขึ้นมาก เกิดขึ้นกับหน่วยงานใด เป็นจากปัญหาด้านไหน ฯลฯ เมื่อวิเคราะห์เสร็จสิ้นแล้วก็ควรจัดทำรายงานอุบัติการณ์ ตามตัวอย่างต่อไปนี้

1.9 การประเมินความพึงพอใจของผู้ใช้บริการ

เมื่อดำเนินการตามข้อตกลงระดับบริการได้สักระยะหนึ่ง ควรจัดให้มีการประเมินความพึงพอใจของผู้ใช้บริการ เพื่อให้ได้ข้อมูลว่าผู้ใช้บริการมีความรู้สึกอย่างไรต่อการดำเนินการตามข้อตกลงระดับบริการ และควรสำรวจประเด็นอื่นๆที่เกี่ยวข้องด้วย เช่น อยากให้มีข้อตกลงเพิ่มเรื่องใดหรือไม่ หรือระยะเวลาที่รับประกันควรมีปรับเปลี่ยนหรือไม่ อย่างไร ฯลฯ

ผลการประเมินความพึงพอใจและทำให้ฝ่ายเทคโนโลยีสารสนเทศได้เข้าใจความรู้สึกของผู้ใช้งาน และยังสามารถนำผลการประเมินนี้มาใช้เป็นตัวชี้วัดความสำเร็จและติดตามการพัฒนาในอนาคตต่อไปได้ด้วย

ระดับที่ 2 การสร้างความแข็งแรงการจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 2 ของการพัฒนา

การยกระดับการจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 2 เป็นการสร้างความแข็งแรงให้กับระบบที่กำเนิดขึ้นมาในระดับที่ 1 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้จริงและทำให้งานดีขึ้น ระดับที่ 2 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

2.1 ทบทวนผลการดำเนินงานในระดับที่ 1

ก่อนที่จะมีการยกระดับการพัฒนา ควรทบทวนผลการดำเนินในระดับที่ 1 โดยใช้หลักการ Plan-Do-Check-Act กล่าวคือ การดำเนินงานในระดับที่ 1 เป็นขั้นตอนของ Plan และ Do เมื่อดำเนินการไปสักระยะหนึ่ง ก็ควร ทบทวนประเมินผล (Check) ก่อนจะที่ยกระดับเป็นระดับที่ 2 (Act) ต่อไปนั่นเอง การประเมินการดำเนินงานที่ผ่านมา จะทำให้เราเห็นโอกาสที่จะปรับปรุงข้อตกลงระดับบริการที่ยังไม่ครอบคลุมบริการสำคัญ หรือไม่ชัดเจน ให้ครอบคลุมบริการสำคัญและชัดเจนมากขึ้น เพื่อทำให้การดำเนินการตามข้อตกลงระดับบริการมีผลลัพธ์ที่ดีขึ้น รวมถึงการปรับปรุงจุดบริการให้เป็นไปตามมาตรฐานมากขึ้น ดังนั้น การดำเนินการในระดับที่ 2 จึงเป็นการทำซ้ำการดำเนินการในระดับที่ 1 อีกรอบหนึ่งแต่เป็นการหมุนวงล้อ PDCA ที่ทำให้ระดับคุณภาพสูงขึ้น

อย่างไรก็ตาม การดำเนินการในระดับที่ 2 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการจัดระบบจัดการอุบัติการณ์และปัญหา เพื่อเพิ่มประสิทธิภาพของระบบ และลดบริการที่มีลักษณะเป็นการแก้ปัญหาเฉพาะหน้า

2.2 การจัดระบบจัดการอุบัติการณ์ (Incidence Management)

อุบัติการณ์ คือเหตุการณ์ที่ทำให้ระบบเทคโนโลยีสารสนเทศมีปัญหา ไม่สามารถดำเนินการได้ตามปกติ เช่น เครื่องแม่ข่ายทำงานช้าลง เครื่องลูกข่ายติดไวรัส ระบบเชื่อมต่ออินเทอร์เน็ตหยุดทำงาน เป็นต้น การจัดการอุบัติการณ์ (Incident Management) มีเป้าหมายเพื่อให้ระบบกลับมาดำเนินการตามปกติอย่างรวดเร็วที่สุดเท่าที่เป็นไปได้ โดยเกิดความเสียหายน้อยที่สุด

กระบวนการจัดการอุบัติการณ์ ประกอบไปด้วยกระบวนการที่สำคัญดังนี้

1. การรับแจ้งอุบัติการณ์ และบันทึกรายละเอียด (เป็นหน้าที่ของ Service Desk โดยตรง)
2. การแยกประเภทอุบัติการณ์ และการจัดการเฉพาะหน้า เพื่อลดความเสียหาย
3. การสืบสวนและวินิจฉัยอุบัติการณ์

4. การแก้ไขและจัดการให้ระบบกลับมาดำเนินการตามปกติ
5. การส่งมอบผลงาน
6. การติดตาม กำกับดูแล ควบคุมระบบจัดการอุบัติการณ์

ผู้ที่มีหน้าที่ในระบบจัดการอุบัติการณ์ ประกอบไปด้วย ผู้จัดการอุบัติการณ์ (Incident Manager) ทำหน้าที่หัวหน้าทีมจัดการอุบัติการณ์ รับผิดชอบให้ระบบดำเนินไปอย่างมีประสิทธิภาพ โดยมีเจ้าหน้าที่จุดบริการ (Service Desk) ทำหน้าที่รับแจ้งอุบัติการณ์และบันทึกรายละเอียด แก้ปัญหาเฉพาะหน้าให้กับผู้ใช้ และติดต่อกับผู้ใช้หลังอุบัติการณ์ยุติ สำหรับอุบัติการณ์ที่เกินกำลังของเจ้าหน้าที่จุดบริการ ผู้เชี่ยวชาญเฉพาะด้านต้องมารับไปสืบสวน วินิจฉัย แก้ไขและจัดการให้ระบบกลับมาเป็นปกติโดยด่วน

ตัวชี้วัดคุณภาพ ระบบจัดการอุบัติการณ์ มีหลายตัว ที่สำคัญได้แก่ จำนวนอุบัติการณ์ที่เกิดขึ้น อัตราส่วนอุบัติการณ์ที่ถูกจัดการได้ทันเวลาตามที่กำหนดไว้ใน Service Level Agreement ค่าใช้จ่ายเฉลี่ยที่เกิดขึ้นในอุบัติการณ์ อัตราส่วนอุบัติการณ์ที่ Service Desk จัดการได้โดยไม่ต้องปรึกษาผู้เชี่ยวชาญเฉพาะด้าน เป็นต้น

2.3 การจัดระบบจัดการปัญหา (Problem Management)

การจัดการปัญหา (Problem Management) เป็นขั้นตอนที่สำคัญหลังการจัดการอุบัติการณ์ โดยการจัดการอุบัติการณ์มีเป้าหมายให้ระบบกลับมาทำงานเป็นปกติในเวลารวดเร็วที่สุด แต่การจัดการปัญหาต้องการกำจัดสาเหตุที่ทำให้เกิดอุบัติการณ์ให้หมดไปอย่างถาวร นอกจากนั้น การจัดการปัญหายังมีเป้าหมายเพื่อป้องกันไม่ให้เกิดอุบัติการณ์ขึ้นซ้ำอีก และสร้างมาตรการลดความเสียหายที่อาจเกิดจากอุบัติการณ์ที่ไม่อาจป้องกันได้ให้น้อยที่สุดเท่าที่จะเป็นไปได้

การจัดการปัญหา แบ่งได้เป็น 2 แบบ คือการจัดการปัญหาเชิงรับ (Reactive Problem Management) และการจัดการปัญหาเชิงรุก (Proactive Problem Management)

การจัดการปัญหาเชิงรับจะดำเนินการเมื่อเกิดปัญหาขึ้นมาแล้ว ประกอบด้วยกระบวนการดังนี้

1. การรับแจ้งปัญหา และบันทึกรายละเอียด
2. การจัดหมวดหมู่ปัญหาและจัดลำดับความสำคัญ
3. การสืบสวนและวินิจฉัยสาเหตุของปัญหา
4. การสืบค้นวิธีแก้ไขปัญหาแบบต่างๆ
5. การลงมือแก้ปัญหาและปิดกรณีปัญหา
6. การติดตาม กำกับดูแล ควบคุมระบบจัดการปัญหา

การจัดการปัญหาเชิงรุก จะค้นหาความเสี่ยงที่จะเกิดปัญหาแล้วจัดการความเสี่ยงนั้น ประกอบด้วยกิจกรรมที่สำคัญ 2 กิจกรรม คือ การวิเคราะห์แนวโน้ม (Trend Analysis) และ การดำเนินการป้องกัน (Preventative Action)

การวิเคราะห์แนวโน้ม จะวิเคราะห์ข้อมูลรายงานอุบัติการณ์ที่เกิดขึ้น หาแนวโน้มกรณีอุบัติการณ์ที่เกิดเพิ่มขึ้น เพื่อนำมาจัดการต่อ โดยการดำเนินการป้องกันจะต้องดำเนินการร่วมกับ การจัดการศักยภาพ (ดูขั้นตอนที่ 5) และการจัดการความพร้อมให้บริการ (ดูขั้นตอนที่ 6)

ผู้ที่มีหน้าที่ในระบบจัดการปัญหา ประกอบไปด้วย ผู้จัดการปัญหา (Problem Manager) ทำหน้าที่หัวหน้าทีมจัดการปัญหา รับผิดชอบให้การจัดการปัญหาดำเนินไปอย่างมีประสิทธิภาพทั้งเชิงรับและเชิงรุก โดยมีทีมจัดการปัญหา (Problem Management Team) ทำหน้าที่รับแจ้งปัญหาและบันทึกรายละเอียด จัดหมวดหมู่ปัญหา เรียงลำดับความสำคัญ สืบสวนและวินิจฉัยสาเหตุของปัญหา สืบค้นวิธีแก้ไขปัญหาแบบต่างๆ ลงมือแก้ไขและปิดกรณีปัญหา

ระดับที่ 3 การสร้างความยั่งยืน การจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 3 ของการพัฒนา

การยกระดับการจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 3 เป็นการสร้างความแข็งแรงให้กับระบบที่พัฒนาจากระดับที่ 1 และ 2 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้อย่างมั่นคงและยั่งยืน ระดับที่ 3 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

3.1 ทบทวนผลการดำเนินงานในระดับที่ 2

เป็นการหมุนวงล้อ PDCA รอบต่อไปที่ทำให้ระดับคุณภาพสูงขึ้นอีก โดยทบทวนกระบวนการทั้งหมดอย่างเป็นระบบ ปรับปรุงกระบวนการที่สำคัญ ดังต่อไปนี้

- ข้อตกลงระดับบริการ
- ระบบจัดการอุบัติการณ์
- การวิเคราะห์การทำงานและกิจกรรมของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ
- ระบบจัดการปัญหา
- วิเคราะห์ความก้าวหน้าที่ผ่านมา ตั้งแต่ระดับที่ 1 มาระดับที่ 2 และระดับปัจจุบัน ควรแสดงให้การพัฒนาและยกระดับคุณภาพอย่างต่อเนื่อง

บทที่ 5

การควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล (Data Quality Control in Hospital Information System)

การควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้มั่นใจว่าข้อมูลที่สำคัญของระบบงานโรงพยาบาลจะเป็นข้อมูลที่ถูกต้อง ครบถ้วน มีรายละเอียดที่ดี และเป็นข้อมูลที่ทันสมัย สามารถนำมาใช้จัดทำสถิติและนำมาวิเคราะห์เพื่อวางแผนพัฒนาระบบงานของโรงพยาบาลให้มีคุณภาพ เพิ่มคุณภาพการรักษา เพิ่มความปลอดภัยของผู้ป่วย ลดต้นทุนและเพิ่มประสิทธิภาพการบริหารจัดการของโรงพยาบาลได้

ข้อมูลที่สำคัญที่สุดของโรงพยาบาล คือข้อมูลการดูแลรักษาโรคต่างๆ เพราะกิจกรรมหลักของโรงพยาบาลคือการดูแลรักษาโรคให้กับประชาชนผู้มารับบริการ ข้อมูลสำคัญคือข้อมูลการรักษาโรคแต่ละครั้ง ทั้งกรณีผู้ป่วยนอกและผู้ป่วยใน ประกอบไปด้วย วันเวลาที่ให้บริการผู้ป่วย อาการสำคัญ ประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การรักษา บันทึกการผ่าตัด/การคลอด บันทึกความก้าวหน้าระหว่างรักษาในโรงพยาบาล รวมถึงการให้รหัสกลุ่มโรคตามหลักการสากล (International Classification of Diseases – ICD) ข้อมูลเหล่านี้ เราสามารถนำมาใช้วิเคราะห์คุณภาพการรักษาได้ จึงต้องมีระบบควบคุมให้มั่นใจว่าข้อมูลมีคุณภาพดี

การควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล สามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระดับ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

ระดับที่ 1

กระบวนการทำงาน	ผลผลิต
1. การจัดมาตรฐานแบบฟอร์ม/หน้าจอบันทึกข้อมูล 2. การฝึกอบรมการบันทึกข้อมูลและการให้รหัส ICD ให้ได้มาตรฐาน 3. การจัดระบบตรวจสอบคุณภาพข้อมูล 4. การสร้างกลไกพัฒนาคุณภาพข้อมูล	1. แบบฟอร์ม/หน้าจอบันทึกข้อมูล 2. รายงานผลการตรวจสอบคุณภาพข้อมูล 3. แนวทางการพัฒนาคุณภาพข้อมูล

ระดับที่ 2

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. ปรับปรุงแบบฟอร์ม/หน้าจอที่ยังไม่เหมาะสม 3. การปรับปรุงระบบตรวจสอบคุณภาพข้อมูล 4. การปรับปรุงกลไกพัฒนาคุณภาพข้อมูล 5. การยกระดับคุณภาพข้อมูลให้สูงขึ้น	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. แบบฟอร์ม/หน้าจอที่ปรับปรุงใหม่ 3. รายงานผลการปรับปรุงระบบตรวจสอบคุณภาพข้อมูล 4. รายงานผลการปรับปรุงกลไกพัฒนาคุณภาพข้อมูล 5. รายงานคุณภาพข้อมูล

ระดับที่ 3

กระบวนกจรทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. ปรับปรุงระบบและกลไกที่ยังไม่เหมาะสม 3. การวิเคราะห์ข้อมูล 4. การสร้างคลังข้อมูล 5. การใช้ข้อมูลและสารสนเทศเพื่อเพิ่มคุณภาพการรักษาโรค เพิ่มความปลอดภัยผู้ป่วยและเพิ่มประสิทธิภาพของโรงพยาบาล	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. รายงานผลการปรับปรุงระบบและกลไกตรวจสอบและพัฒนาคุณภาพข้อมูล 3. ผลการวิเคราะห์ข้อมูล 4. คลังข้อมูลผู้ป่วยนอก 5. คลังข้อมูลผู้ป่วยใน 6. โครงการพัฒนาคุณภาพการรักษาโรคโดยการใช้ข้อมูลขับเคลื่อน

ระดับที่ 1 การเริ่มต้นควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล
ระดับที่ 1 ของการพัฒนา

ระดับแรก เป็นการวางพื้นฐานที่จำเป็นของการควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

1.1 การจัดมาตรฐานแบบฟอร์ม/หน้าจอบันทึกข้อมูล

แบบฟอร์มและหน้าจอที่มีรายละเอียดตามมาตรฐานจะช่วยให้การบันทึกข้อมูลเป็นไปได้โดยครบถ้วนมากขึ้น มาตรฐานที่ควรใช้ในการตรวจสอบว่าแบบฟอร์ม/หน้าจอของโรงพยาบาลมีช่องให้บันทึกข้อมูลครบถ้วนหรือไม่ คือ มาตรฐานการเก็บรวบรวมและบันทึกข้อมูลในสถานพยาบาล ปีพ.ศ. 2559 ของกระทรวงสาธารณสุข [1]

มาตรฐานการเก็บรวมรวมและบันทึกข้อมูลในสถานพยาบาลของกระทรวงสาธารณสุขกำหนดให้การบันทึกข้อมูลบริการผู้ป่วยนอกแต่ละครั้ง ควรประกอบไปด้วยหัวข้อที่สำคัญดังต่อไปนี้

a. วันที่และเวลาที่มารับบริการ
b. อาการสำคัญ
c. ประวัติปัจจุบัน ประวัติอดีต ประวัติส่วนตัว
d. ผลการตรวจร่างกาย
e. ผลการตรวจทางห้องปฏิบัติการหรือการตรวจพิเศษอื่นๆ
f. ผลการรักษาในกรณีที่นัดติดตามผล
g. คำวินิจฉัยโรค
h. การรักษา
i. การให้คำแนะนำ
j. วันที่นัดติดตามผล
k. ชื่อและการลงลายมือชื่อของผู้รักษา

เอกสารการดูแลรักษาผู้ป่วยในจะมีลักษณะบางส่วนคล้ายกับการดูแลรักษาผู้ป่วยนอก แต่จะมีรายละเอียด เพิ่มเติม มากกว่า ดังนี้

a. ประวัติการเจ็บป่วยของผู้ป่วยใน
b. ผลการตรวจร่างกายแรกรับ
c. ผลการตรวจทางห้องปฏิบัติการ
d. ผลการตรวจทางรังสีวิทยา
e. ผลการตรวจพิเศษอื่นๆ
f. รายการปัญหา

g. แผนการรักษา

h. บันทึกการสั่งการรักษาของแพทย์

i. บันทึกการให้คำปรึกษา

j. บันทึกการทำการผ่าตัดหรือหัตถการ

k. บันทึกความก้าวหน้า

l. บันทึกทางการพยาบาล

m. บันทึกการคลอด

n. บันทึกกิจกรรมเวชศาสตร์ฟื้นฟู

o. บันทึกการรักษาแบบแผนไทย แผนจีน หรือ การแพทย์ทางเลือก

p. สรุปการรักษา

q. แบบฟอร์มการให้ข้อมูลและการขอความยินยอมเพื่อรักษา

r. บันทึกอื่นๆ เช่น บันทึกการให้ยาระงับความรู้สึก

ควรดำเนินการตรวจสอบแบบฟอร์ม/หน้าจอบันทึกข้อมูลของโรงพยาบาลให้มั่นใจว่า มีหัวข้อต่างๆ ครบถ้วน ในปัจจุบันพบว่า หัวข้อที่มักจะหายไปจากหน้าจอบันทึกข้อมูลของโรงพยาบาล คือ คำวินิจฉัยโรคของผู้ป่วยนอก โดยโปรแกรมที่ออกแบบหน้าจอผิดพลาดจะไม่มีช่องให้แพทย์บันทึกคำวินิจฉัยโรคของผู้ป่วย มีแต่ช่องการให้รหัส ICD ถ้าใช้โปรแกรมลักษณะนี้บันทึกข้อมูลผู้ป่วยนอก จะทำให้ข้อมูลที่สำคัญที่สุดคือคำวินิจฉัยโรคของผู้ป่วยนอกหายไป

1.2 การฝึกอบรมการบันทึกข้อมูลให้ได้มาตรฐาน

เมื่อปรับปรุงแบบฟอร์ม/หน้าจอบันทึกข้อมูลจนมั่นใจว่ามีหัวข้อสำคัญครบถ้วนแล้ว ควรจัดฝึกอบรมการบันทึกข้อมูลให้ได้มาตรฐาน โดยบุคลากรที่ต้องฝึกอบรม คือ แพทย์ พยาบาล ทันตแพทย์ นักกายภาพบำบัด แพทย์แผนไทย ให้เข้าใจวิธีการบันทึกข้อมูลให้ครบถ้วน ตามมาตรฐาน [1]

การให้รหัส ICD ทั้งกรณีผู้ป่วยนอกและผู้ป่วยใน ควรเป็นการให้รหัสโดยใช้วิธีการมาตรฐานของกระทรวงสาธารณสุข [1] กล่าวคือ ผู้ให้รหัสควรเรียนรู้ขั้นตอนมาตรฐานของการให้รหัส และให้รหัสโดยใช้คู่มือมาตรฐานของศูนย์รหัสแห่งชาติที่อ้างอิงมาตรฐานขององค์การอนามัยโลก [2]

การให้รหัส ICD โดยค้นจากระบบห้องตรวจแพทย์ของโปรแกรมโรงพยาบาลที่ใช้งานอยู่ทั่วไปในประเทศไทย เป็นวิธีการที่ไม่ถูกต้องและทำให้รหัส ICD ผิดพลาดเป็นจำนวนมาก จึงไม่ควรให้รหัส ICD ด้วยวิธีการนี้ เพราะรหัสที่ได้จากโปรแกรมลักษณะนี้ จะเป็นรหัสที่ผิดมากกว่ารหัสที่ถูก

1.3 การจัดระบบตรวจสอบคุณภาพข้อมูล

โรงพยาบาลต้องมีระบบตรวจสอบคุณภาพข้อมูลที่ดี เพื่อให้รับทราบสถานการณ์ปัจจุบันของคุณภาพข้อมูลการรักษาผู้ป่วยที่เก็บไว้ในระบบของโรงพยาบาล การตรวจสอบคุณภาพข้อมูลต้องดำเนินการทั้งผู้ป่วยนอกและผู้ป่วยในรวมถึงการให้รหัส ICD ระบบตรวจสอบคุณภาพข้อมูลที่ดีประกอบไปด้วยองค์ประกอบที่สำคัญดังนี้

1. คณะผู้ตรวจสอบคุณภาพเวชระเบียน เป็น คณะทำงานที่ทำหน้าที่ประเมินคุณภาพข้อมูลใน OPD Cards และแฟ้มเวชระเบียนผู้ป่วยใน คณะทำงานควรประกอบไปด้วย แพทย์ พยาบาล เจ้าหน้าที่เวชสถิติ จำนวน 5-10 คน

2. เครื่องมือตรวจสอบคุณภาพเวชระเบียน เป็นหลักเกณฑ์การตรวจสอบและให้คะแนนคุณภาพเวชระเบียน ควรเลือกใช้เครื่องมือที่ประเมินได้ครบถ้วนทุกด้านที่จำเป็น เช่น คู่มือการตรวจสอบคุณภาพเวชระเบียนปี 2558 ของกระทรวงสาธารณสุข [3]

3. การตรวจสอบคุณภาพเวชระเบียนอย่างสม่ำเสมอ โดยควรมีกิจกรรมตรวจสอบคุณภาพเวชระเบียนอย่างน้อยทุกๆ 3 เดือน แต่หากพบว่าคุณภาพข้อมูลมีปัญหามากและต้องการปรับปรุงคุณภาพโดยด่วน ก็อาจจัดให้มีการตรวจสอบคุณภาพทุกๆเดือน เพื่อรับรู้ผลการดำเนินการพัฒนาคุณภาพและปรับปรุงแก้ไขได้ทุกเดือน

เมื่อตรวจสอบคุณภาพข้อมูลและคุณภาพรหัส ICD แล้ว ควรรายงานผลการตรวจสอบออกมาเพื่อนำผลมาพิจารณาแนวทางการแก้ปัญหาข้อมูลที่ด้อยคุณภาพต่อไปนี้ ดังตัวอย่างรายงานดังต่อไปนี้

รายงานผลการตรวจสอบคุณภาพข้อมูล และ คุณภาพการให้รหัส

สถานพยาบาล .....

วันที่ตรวจสอบ ...10 เมษายน 2558.... ช่วงระยะเวลาของข้อมูลที่ตรวจสอบ ม.ค.- มี.ค. 2558

สุ่มตัวอย่างข้อมูลผู้ป่วย จำนวน 40 คน มีรหัส ICD ทั้งหมด 68 รหัส

ผลการตรวจสอบการบันทึกข้อมูล

คะแนนคุณภาพข้อมูล

คุณภาพเฉลี่ยโดยรวม	65.27 %
คุณภาพการบันทึกวันเวลา	75 %
คุณภาพการบันทึกอาการสำคัญ	92.25 %
คุณภาพการบันทึกประวัติ	72.35 %

คุณภาพการบันทึกตรวจร่างกาย 37.5 %

คุณภาพการบันทึกคำวินิจฉัยโรค 52.5 %

คุณภาพการบันทึกการรักษา 85.17 %

ผลการตรวจสอบการให้รหัส ICD

ให้รหัสถูกต้อง 47.5 %

ให้รหัสผิด 52.5 %

ลักษณะความผิดพลาด

A	ให้รหัสผิดพลาด	12.5 %
B	มีรหัสโรคหลักทั้งๆที่ไม่มีคำวนิจฉัยโรคในบันทึก	20 %
C	รหัสด้อยคุณภาพ กำกวม	2.0 %
D	ให้รหัสไม่ครบทุกตำแหน่ง	4.5 %
E	ใช้รหัสสาเหตุการบาดเจ็บเป็นรหัสโรคหลัก	5.5 %
F	รหัสมีตัวเลขมากเกินไป	0 %
G	ให้รหัสไม่ครบ	3.5 %
H	ให้รหัสมากเกิน	4.5 %

สรุปปัญหา

ปัญหาที่พบบ่อยคือ การไม่บันทึกคำวินิจฉัยโรคแต่ใส่รหัสไปเลย การให้รหัสผิดพลาด และ การใช้รหัสสาเหตุภายนอกเป็นรหัสโรคหลัก

สาเหตุของปัญหา

สาเหตุหลัก มาจากการไม่บันทึกคำวินิจฉัย เพราะบางครั้งผู้ตรวจรักษาไม่วินิจฉัยโรค
วิธีการให้รหัสผิดพลาด ใช้โปรแกรมในการค้นหารหัส ICD ไม่ใช้คู่มือมาตรฐาน
การขาดความรู้และความชำนาญในการให้รหัส

แนวทางการแก้ปัญหา

1. ควรวางระบบควบคุมให้ผู้ตรวจรักษาโรคทุกคน ต้องบันทึกคำวินิจฉัยโรค
2. กำหนดมาตรฐาน ห้ามค้นหารหัส ICD จากโปรแกรม
3. อบรมเพิ่มความรู้ความชำนาญด้านการให้รหัส ICD

1.4 การสร้างกลไกพัฒนาคุณภาพข้อมูล

การตรวจสอบคุณภาพข้อมูลจะทำให้เห็นประเด็นที่ยังเป็นปัญหาของโรงพยาบาล ปัญหาที่พบนี้ควรได้รับการจัดการอย่างเป็นระบบ จึงควรสร้างกลไกพัฒนาคุณภาพข้อมูล เพื่อใช้กลไกนี้แก้ไขปัญหาข้อมูลด้อยคุณภาพ กลไกพัฒนาคุณภาพข้อมูลที่ดีควรมีองค์ประกอบดังนี้

1. การกำกับดูแลจากผู้บริหารโรงพยาบาล ผู้บริหารจะต้องให้ความสำคัญต่อประเด็นคุณภาพข้อมูล โดยต้องกำหนดเป็นตัวชี้วัดผลงานของแพทย์ พยาบาล ทันตแพทย์ และเจ้าหน้าที่อื่นๆที่เกี่ยวข้อง ผู้บริหารต้องรับทราบผลการประเมินคุณภาพข้อมูลทุกๆครั้ง และต้องมีกระบวนการจัดการให้เกิดการพัฒนาคุณภาพที่เป็นรูปธรรม เอาจริงเอาจัง และเห็นผลได้ชัดเจน

2. การปลูกฝังให้เกิดเป็นวัฒนธรรมใส่ใจคุณภาพข้อมูล โดยเบื้องต้นอาจกำหนดให้มีรางวัลเล็กๆน้อยสำหรับผู้ปฏิบัติงานที่บันทึกข้อมูลได้ดีมีคุณภาพ ยกย่องเป็นแบบอย่าง และให้ความใส่ใจต่อผู้ที่ยังปฏิบัติงานได้ไม่ดี ประคับประคองให้สามารถบันทึกข้อมูลได้ดีขึ้นจนได้มาตรฐาน

3. การนำข้อมูลมาวิเคราะห์เพื่อใช้ประโยชน์ในการวางแผนพัฒนาคุณภาพการรักษาโรค เพื่อให้ผู้ปฏิบัติงานเห็นว่าถ้าบันทึกข้อมูลไม่ดี ผลการวิเคราะห์จะผิดเพี้ยนไป ไม่สามารถนำมาใช้พัฒนาคุณภาพการรักษาโรคให้ดีขึ้นได้

เป้าหมายการพัฒนาคุณภาพข้อมูลในระดับที่ 1 ควรกำหนดระดับคุณภาพข้อมูล และคุณภาพการให้รหัส ICD ที่ระดับ 80%

ระดับที่ 2 การสร้างความแข็งแรง การควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 2 ของการพัฒนา

การยกระดับการควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 2 เป็นการสร้างความแข็งแรงให้กับระบบที่กำเนิดขึ้นมาในระดับที่ 1 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้จริงและทำให้งานดีขึ้น ระดับที่ 2 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

2.1 ทบทวนผลการดำเนินงานในระดับที่ 1

ก่อนที่จะมีการยกระดับการพัฒนา ควรทบทวนผลการดำเนินในระดับที่ 1 โดยใช้หลักการ Plan-Do-Check-Act กล่าวคือ การดำเนินงานในระดับที่ 1 เป็นขั้นตอนของ Plan และ Do เมื่อดำเนินการไป

สักระยะหนึ่ง ก็ควร ทบทวนประเมินผล (Check) ก่อนจะที่ยกระดับเป็นระดับที่ 2 (Act) ต่อไปนั่นเอง การประเมินการดำเนินงานที่ผ่านมา จะทำให้เราเห็นโอกาสที่จะปรับปรุงแบบฟอร์ม/หน้าจอที่ยังไม่เหมาะสมให้ดีขึ้นกว่าเดิม รวมถึงการปรับปรุงระบบตรวจสอบคุณภาพข้อมูลให้เป็นไปตามมาตรฐานมากขึ้น ดังนั้น การดำเนินการในระดับที่ 2 จึงเป็นการทำซ้ำการดำเนินการในระดับที่ 1 อีกรอบหนึ่งแต่เป็นการหมุนวงล้อ PDCA ที่ทำให้ระดับคุณภาพสูงขึ้น

เป้าหมายการพัฒนาคุณภาพข้อมูลในระดับที่ 2 ควรกำหนดระดับคุณภาพข้อมูล และคุณภาพการให้รหัส ICD ที่ระดับ 95%

ระดับที่ 3 การสร้างความยั่งยืน การควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 3 ของการพัฒนา

การยกระดับการควบคุมคุณภาพข้อมูลในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 3 เป็นการสร้างความแข็งแรงให้กับระบบที่พัฒนาจากระดับที่ 1 และ 2 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้อย่างมั่นคงและยั่งยืน ระดับที่ 3 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

3.1 ทบทวนผลการดำเนินงานในระดับที่ 2

เป็นการหมุนวงล้อ PDCA รอบต่อไปที่ทำให้ระดับคุณภาพสูงขึ้นอีก โดยทบทวนกระบวนการทั้งหมดอย่างเป็นระบบ ปรับปรุงกระบวนการที่สำคัญ ดังต่อไปนี้

- แบบฟอร์ม/หน้าจอบันทึกข้อมูล
- ระบบตรวจสอบคุณภาพข้อมูล
- กลไกพัฒนาคุณภาพข้อมูล
- วิเคราะห์ความก้าวหน้าที่ผ่านมา ตั้งแต่ระดับที่ 1 มาระดับที่ 2 และระดับปัจจุบัน ควรแสดงให้การพัฒนาและยกระดับคุณภาพอย่างต่อเนื่อง

นอกจากนั้น ในการพัฒนาระดับที่ 3 นี้ ควรมีกิจกรรมเพิ่มเติม ได้แก่ การวิเคราะห์ข้อมูล การสร้างคลังข้อมูล และการใช้ข้อมูลและสารสนเทศเพื่อเพิ่มคุณภาพการรักษาโรค เพิ่มความปลอดภัยผู้ป่วยและเพิ่มประสิทธิภาพของโรงพยาบาล

3.2 การวิเคราะห์ข้อมูล

เมื่อมั่นใจว่าข้อมูลในระบบมีคุณภาพที่ดีเพียงพอ แล้วควรวิเคราะห์ข้อมูลเพื่อนำมาค้นหาแนวทางมาพัฒนาโรงพยาบาลต่อไป โดยข้อมูลในระบบโรงพยาบาล จะมีลักษณะเฉพาะไม่เหมือนข้อมูลอื่นทั่วไป เพราะในโรงพยาบาลมีข้อมูลที่แตกต่าง 6 กลุ่ม ตามลักษณะกลุ่มโครงสร้างของระบบโรงพยาบาล ดังนี้

1. ข้อมูลผู้ป่วย เป็นข้อมูลระบุตัวผู้ป่วย ลักษณะทางประชากรศาสตร์ สถานภาพสมรส สิทธิการรักษา ที่อยู่ ฯลฯ ข้อมูลเหล่านี้จะเปลี่ยนแปลงเมื่อผู้ป่วยย้ายที่อยู่ เปลี่ยนที่ทำงาน แต่งงาน มีลูก ตามกิจกรรมของผู้ป่วย เจ้าหน้าที่เวชระเบียนควรหมั่นปรับปรุงข้อมูลผู้ป่วยให้ทันสมัยโดยขอข้อมูลเพิ่มเติมเป็นระยะ
2. ข้อมูลกิจกรรมการบริการผู้ป่วย เป็นข้อมูลที่มีมากที่สุดในทุกโรงพยาบาล เก็บรายละเอียดการบริการผู้ป่วยทุกครั้ง ได้แก่ ข้อมูลการมาตรวจ การจ่ายยา ค่ารักษา ผลการตรวจทางห้องปฏิบัติการ ฯลฯ ผู้บันทึกข้อมูลคือผู้ที่ดูแลผู้ป่วยทุกคน ตั้งแต่ แพทย์ พยาบาล เภสัชกร เจ้าหน้าที่ห้อง Lab เจ้าหน้าที่การเงิน ฯลฯ
3. ข้อมูลทรัพยากร เป็น ข้อมูลการจัดสรรทรัพยากรในการรักษาพยาบาลผู้ป่วย ได้แก่ ข้อมูลตารางนัด ตารางการผ่าตัด จำนวนเตียงว่าง รายการยาที่มีในโรงพยาบาล จำนวนแพทย์สาขาต่างๆ ฯลฯ ข้อมูลลักษณะนี้จะมีผู้บันทึกข้อมูลเพียงไม่กี่คน แต่มีผู้ใช้ข้อมูลจำนวนมากที่ต้องเรียกดูข้อมูลเหล่านี้อยู่บ่อยๆ
4. ข้อมูลทางคลินิก เป็นข้อมูลที่ช่วยให้แพทย์ พยาบาล และเจ้าหน้าที่ที่บำบัดรักษาผู้ป่วยโดยตรงต้องใช้เพื่อให้การดูแลรักษาอย่างต่อเนื่องมีคุณภาพที่ดี ได้แก่ ประวัติการเจ็บป่วย ผลการตรวจร่างกาย การวินิจฉัย รายงานการผ่าตัด การให้การพยาบาล บันทึกทางกายภาพบำบัด ฯลฯ ข้อมูลลักษณะนี้ ใช้เพื่อสื่อสารระหว่างแพทย์ พยาบาล และผู้มีหน้าที่บำบัดรักษาผู้ป่วย เพื่อให้รายละเอียดช่วยการตัดสินใจที่ดี
5. ข้อมูลการบริหาร เป็นข้อมูลเพื่อช่วยให้การบริหารโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพ ได้แก่ ข้อมูลต้นทุนค่ายา ค่ารักษาต่างๆ ข้อมูล username, password ข้อมูลการป่วย ลา ขาด สายของบุคลากร ฯลฯ ข้อมูลลักษณะนี้อาจได้มาจากการบันทึก หรือได้จากการคำนวณข้อมูลอื่นๆ ประกอบกัน
6. ข้อมูลอ้างอิง เป็นข้อมูลที่ใช้เรียกดูประกอบการตัดสินใจ ได้แก่ ตารางยาที่ออกฤทธิ์รบกวนกัน รายการยาที่เบิกค่ารักษาได้ รายการค่ารักษาที่เบิกได้ หรือ เบิกไม่ได้ ฯลฯ ข้อมูลนี้ส่วนใหญ่มา

จากองค์กรภายนอกของโรงพยาบาล ผู้ดูแลระบบจะเป็นผู้รับผิดชอบให้ข้อมูลกลุ่มนี้ทันสมัยอยู่เสมอ

ข้อมูลที่ควรนำมาใช้วิเคราะห์เป็นระยะได้แก่ ข้อมูลกลุ่มที่ 1 ผู้ป่วย 2 กิจกรรม 3 ทรัพยากร และ 5 บริหาร เพื่อให้รู้ว่าลักษณะผู้มารับบริการเป็นกลุ่มไหน กิจกรรมและการใช้ทรัพยากรเป็นอย่างไร ควรบริหารอย่างไรให้มีประสิทธิภาพ

การวิเคราะห์ข้อมูลผู้ป่วย

ข้อมูลผู้ป่วย เป็นข้อมูลที่สำคัญเพราะผู้ป่วยเป็นผู้มารับบริการรักษาพยาบาล หากเราเข้าใจลักษณะของผู้มารับบริการเป็นอย่างดี เราย่อมสามารถปรับบริการของโรงพยาบาลให้สอดคล้องกับผู้ป่วย เพิ่มความสะดวกสบายและความพึงพอใจของผู้ป่วยได้ ผู้ป่วยและญาติก็จะเกิดความรู้สึกที่ประทับใจ ลดโอกาสร้องเรียนได้ ตัวอย่างการวิเคราะห์ข้อมูลผู้ป่วยได้แก่

- สัดส่วน เพศ อายุ ภูมิลำเนา เชื้อชาติ สัญชาติ ของผู้ป่วย
- สัดส่วนสถานภาพสมรส อาชีพ สถานที่ทำงาน
- สัดส่วน สิทธิการรักษาของผู้ป่วย เรียงตามลำดับที่มีสัดส่วนมากไปน้อย
- กลุ่มโรคหลักที่ผู้ป่วยเป็นมากที่สุด 30 อันดับแรก
- โรคประจำตัวที่ผู้ป่วยเป็นมากที่สุด 10 อันดับแรก
- การผ่าตัดที่ผู้ป่วยได้รับกันมากที่สุด 20 อันดับแรก
- แนวโน้มการเปลี่ยนแปลงลักษณะผู้ป่วยในรอบ 6 เดือน 1 ปี 3 ปี 5 ปี

การวิเคราะห์ข้อมูลกิจกรรมการรักษาพยาบาล

ข้อมูลกิจกรรม เป็นข้อมูลที่มีมากที่สุดในระบบคอมพิวเตอร์โรงพยาบาล เพราะเราใช้คอมพิวเตอร์บันทึกข้อมูลกิจกรรมเหล่านี้ตลอดเวลา เริ่มจากจุดยื่นบัตร ไปจนพบพยาบาล พบแพทย์ ตรวจ Lab XRays จ่ายยา จ่ายเงิน จนผู้ป่วยกลับบ้าน จึงเป็นข้อมูลที่วิเคราะห์ได้มากที่สุด ตัวอย่างการวิเคราะห์ข้อมูลกิจกรรมได้แก่

- จำนวนผู้ป่วยที่มารับบริการตาม OPD หรือจุดบริการต่างๆ
- จำนวน และสัดส่วนการตรวจทางห้องปฏิบัติการ การตรวจพิเศษ การตรวจทางรังสีวิทยา
- ค่าใช้จ่ายเพื่อบริการต่างๆ เช่น ค่ายา ค่าตรวจทางห้องปฏิบัติการ ค่าตรวจพิเศษ
- ระยะเวลาที่รอคิว ระยะเวลาที่ให้บริการในจุดต่างๆ
- จำนวน และ สัดส่วนการให้บริการจำแนกตามแพทย์ พยาบาล บุคลากรอื่นๆ

- จำนวนและสัดส่วนผู้ป่วยที่มาตรวจตามนัด และไม่มาตามนัด
- แนวโน้มการเปลี่ยนแปลงจำนวน และสัดส่วนการให้บริการ ในรอบ 6 เดือน 1 ปี 3 ปี 5 ปี

การวิเคราะห์ข้อมูลทรัพยากร

เราควรวิเคราะห์จำนวน และการจัดสรรทรัพยากรด้านบุคคล สถานที่และวัสดุอุปกรณ์รวมทั้งยา ในกิจกรรมของโรงพยาบาลทุกๆกิจกรรม เพื่อให้สามารถบริหารทรัพยากรให้มีประสิทธิภาพมากที่สุด เพราะทรัพยากรทุกด้านมีจำกัด หากไม่วิเคราะห์ข้อมูลให้ดี ก็อาจไม่รู้ว่ากำลังใช้ทรัพยากรบางอย่างโดยสูญเปล่า ตัวอย่างการวิเคราะห์ข้อมูลทรัพยากร ได้แก่

- จำนวน และสัดส่วน แพทย์ พยาบาล เภสัชกร และบุคลากรอื่นๆ
- จำนวน และสัดส่วนยา เวชภัณฑ์ น้ำยา วัสดุต่างๆที่ใช้ รวมถึงการสั่งซื้อและจัดเก็บ
- จำนวนห้องตรวจ จำนวนเตียงผู้ป่วย จำนวนห้องผ่าตัด อัตราการครองเตียง
- เวลาที่ใช้ในการตรวจ การผ่าตัด การเจาะเลือด การตรวจเอ็กซเรย์
- เวลาที่ว่างในตารางนัดตรวจ คิวนัด การจัดสัดส่วนการนัด
- จำนวนและสัดส่วนการสูญเสียทรัพยากรด้านต่างๆ เช่น เวลาที่ผู้ป่วยไม่มาตามนัด
- แนวโน้มการเปลี่ยนแปลงจำนวน และสัดส่วนการใช้ทรัพยากรต่างๆ ในรอบ 6 เดือน 1 ปี 3 ปี 5 ปี

การวิเคราะห์ข้อมูลการบริหาร

ผู้บริหารโรงพยาบาล ต้องมีข้อมูลที่ดีเพื่อช่วยในการคิดและการตัดสินใจ โดยต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้ และทันสมัย ข้อมูลสนับสนุนการบริหารมักเป็นข้อมูลที่ต้องวิเคราะห์ไว้ล่วงหน้า จึงควรคิดวิธีการวิเคราะห์ไว้ก่อนที่ผู้บริหารจะเรียกใช้ เพื่อให้ได้ข้อมูลทันตามที่ผู้บริหารต้องการ ตัวอย่างการวิเคราะห์ข้อมูลการบริหารได้แก่

- ต้นทุนการรักษาผู้ป่วยนอก ผู้ป่วยใน ต้นทุนรายโรค
- ค่าใช้จ่ายในการซื้อยา วัสดุ อุปกรณ์ ค่าสาธารณูปโภค
- รายรับ และรายได้ต่างๆของโรงพยาบาล
- จำนวนและสัดส่วนคนทำงานตามจุดต่างๆ การจัดเวร
- อัตราการลาออกของแพทย์ พยาบาล บุคลากรต่างๆ
- ผลการดำเนินการตามตัวชี้วัดต่างๆ
- แนวโน้มการเปลี่ยนแปลงลักษณะข้อมูลบริหาร ในรอบ 6 เดือน 1 ปี 3 ปี 5 ปี

3.4 การสร้างคลังข้อมูล

คลังข้อมูล (Data Warehouse) เป็นแหล่งเก็บข้อมูล เพื่อใช้ค้นหาและสืบค้นรวมถึงการวิเคราะห์ข้อมูลเพื่อตอบคำถามต่างๆที่เกี่ยวข้องกับข้อมูลนั้นๆ ในปัจจุบัน เราสามารถใช้โปรแกรมสร้างคลังข้อมูลขึ้นมาเพื่อใช้ประโยชน์ในการวิเคราะห์ข้อมูลด้านต่างๆของโรงพยาบาล [4] โดยควรมีคลังข้อมูลที่สำคัญอย่างน้อย 2 คลังข้อมูล คือ คลังข้อมูลผู้ป่วยนอก และคลังข้อมูลผู้ป่วยใน นอกจากนั้น อาจพิจารณาสร้างคลังข้อมูลอื่นๆที่เห็นว่าเหมาะสม เช่น

- คลังข้อมูลยาและเวชภัณฑ์
- คลังข้อมูลห้องผ่าตัด
- คลังข้อมูลการเจ้าหน้าที่
- คลังข้อมูลบัญชีและการเงิน

3.5 การใช้ข้อมูลและสารสนเทศเพื่อเพิ่มคุณภาพการรักษาโรค เพิ่มความปลอดภัยผู้ป่วยและเพิ่มประสิทธิภาพของโรงพยาบาล

ข้อมูลการรักษาโรคของผู้ป่วยนอกและผู้ป่วยใน เป็นข้อมูลที่มีความสำคัญมาก เพราะสามารถนำมาวิเคราะห์ให้เห็นประเด็นที่จะนำมาพัฒนาคุณภาพการรักษาโรคของโรงพยาบาล เพิ่มความปลอดภัยของผู้ป่วยและเพิ่มประสิทธิภาพของโรงพยาบาลได้

การวิเคราะห์ข้อมูลการรักษาโรคในอดีตย้อนหลัง 3-5 ปี จะทำให้เห็นว่า ผู้ป่วยลักษณะใดเป็นกลุ่มเสี่ยงที่จะต้องรับไว้ในโรงพยาบาลก่อนเวลาอันควร (Unplanned Readmission) ผู้ป่วยลักษณะใดมีโอกาสเกิดโรคแทรกซ้อน ระหว่างนอนโรงพยาบาล ผู้ป่วยโรคใดมีอัตราตายสูง ค่าใช้จ่ายด้านใดสามารถลดลงได้มากกว่านี้ ผู้ป่วยกลุ่มใดเป็นผู้ที่สร้างรายได้ให้กับโรงพยาบาลสูง ฯลฯ ข้อมูลเหล่านี้ควรนำมาใช้วางแผนพัฒนาคุณภาพการรักษาโรค ลดการขาดทุน เพิ่มรายได้ เพิ่มความปลอดภัยของผู้ป่วยให้มากขึ้น

การใช้ข้อมูลและสารสนเทศเพื่อเพิ่มคุณภาพ ประกอบด้วยขั้นตอนหลักดังต่อไปนี้

1. การนำข้อมูลการรักษาเข้าสู่คลังข้อมูล
2. การสร้างคลังข้อมูล
3. การวิเคราะห์ข้อมูลด้านคุณภาพการรักษาโรค
4. การวิเคราะห์ข้อมูลเพื่อเพิ่มความปลอดภัยผู้ป่วย
5. การวิเคราะห์รายได้ ค่าใช้จ่ายของโรงพยาบาล
6. การพิจารณาผลการวิเคราะห์โดยคณะกรรมบริหารโรงพยาบาล
7. การตัดสินใจเชิงกลยุทธ์ของคณะกรรมการบริหาร

REFERENCES

1. สำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข. (2559). มาตรฐานการเก็บรวบรวมและบันทึกข้อมูลในสถานพยาบาล. นนทบุรี. กระทรวงสาธารณสุข.

2. World Health Organization. (2016). International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, volume 2. 5th ed. Geneva: World Health Organization.

3. สำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข. (2558). การตรวจสอบและควบคุมคุณภาพข้อมูลในระบบบริการสุขภาพด้านการบันทึกข้อมูลผู้มารับบริการและการให้รหัส ICD. นนทบุรี. กระทรวงสาธารณสุข.

4. สมาคมเวชสารสนเทศไทย. (2560). การวิเคราะห์ข้อมูลโรงพยาบาลขั้นพื้นฐาน. นนทบุรี. สมาคมเวชสารสนเทศไทย.

บทที่ 6

การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล (Quality Control of Hospital Software Development)

การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้มั่นใจได้ว่าโปรแกรมที่มีการพัฒนาขึ้นโดยฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลเป็นโปรแกรมที่ดีมีคุณภาพ มีการวิเคราะห์และออกแบบระบบไว้อย่างดี โดยหัวใจหลักคือการวิเคราะห์และออกแบบระบบ (System Analysis and Design) ที่ดี ให้มั่นใจว่า มีข้อมูลเอกสารสำคัญที่สามารถนำมาใช้ปรับปรุงโปรแกรมในอนาคตได้อย่างยั่งยืน รับประกันได้ว่า แม้ผู้เขียนโปรแกรมคนเดิมจะลาออกไป คนใหม่ที่มารับงานแทนก็สามารถปรับปรุงโปรแกรมต่อไปได้ทันที ไม่ต้องทิ้งของเก่าและสร้างขึ้นมาใหม่หมด

การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาลยังครอบคลุมไปถึงเรื่อง การทดสอบโปรแกรมให้มั่นใจว่าโปรแกรมทำงานได้อย่างถูกต้อง ตรงตามความต้องการของผู้ใช้โปรแกรม มีความมั่นคงปลอดภัย และมีคู่มือสอนการใช้งานโปรแกรมครบถ้วนทุกด้าน

การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล สามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระดับ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

ระดับที่ 1

กระบวนการสำคัญ	ผลผลิต
1. การระบุปัญหา ความต้องการให้เกิดการพัฒนาโปรแกรม 2. การวิเคราะห์ระบบงานปัจจุบัน 3. การออกแบบระบบงานใหม่ด้านขั้นตอนการทำงาน 4. การออกแบบหน้าจอและส่วนติดต่อกับผู้ใช้งาน 5. การออกแบบฐานข้อมูลสำหรับระบบงานใหม่ 6. การสร้างพจนานุกรมข้อมูล 7. การจัดทำคู่มือสำหรับผู้ใช้งานโปรแกรมและการอบรม 8. การประเมินความพึงพอใจของผู้ใช้โปรแกรม	1. รายงานผลการสำรวจปัญหาและความต้องการให้เกิดการพัฒนาโปรแกรม 2. รายงานผลการวิเคราะห์ระบบงานปัจจุบัน 3. เอกสารการออกแบบระบบงานใหม่ด้านขั้นตอนการทำงาน 4. เอกสารการออกแบบหน้าจอและส่วนติดต่อกับผู้ใช้งาน 5. เอกสารการออกแบบฐานข้อมูลสำหรับระบบงานใหม่ 6. พจนานุกรมข้อมูล

ระดับที่ 1 (ต่อ)

กระบวนการสำคัญ	ผลผลิต
	7. คู่มือการใช้โปรแกรม 8. รายงานผลการประเมินความพึงพอใจ

ระดับที่ 2

กระบวนการสำคัญ	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. ปรับปรุงเอกสารการวิเคราะห์ออกแบบระบบ รวมถึงคู่มือที่ยังไม่เหมาะสม 3. การจัดระบบควบคุมรุ่นของโปรแกรม (Software Version Control) 4. การเขียนหมายเหตุในรหัสต้นฉบับ (Source Code Comments) 5. การจัดระบบตรวจสอบคุณภาพโปรแกรม	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. เอกสารการวิเคราะห์ออกแบบระบบและคู่มือฉบับปรับปรุงใหม่ 3. เอกสารการควบคุมรุ่นของโปรแกรม 4. หมายเหตุในรหัสต้นฉบับ 5. แนวทางการตรวจสอบคุณภาพโปรแกรม

ระดับที่ 3

ระดับที่ 3	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. ปรับปรุงเอกสารการวิเคราะห์ออกแบบระบบ รวมถึงคู่มือ และหมายเหตุในรหัสต้นฉบับ ที่ยังไม่เหมาะสม 3. การตรวจสอบคุณภาพโปรแกรม 4. การประเมินความพึงพอใจของผู้ใช้ 5. การจัดการโครงการพัฒนาโปรแกรม	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. เอกสารการวิเคราะห์ออกแบบระบบและคู่มือฉบับปรับปรุงใหม่ หมายเหตุในรหัสต้นฉบับเพิ่มเติม 3. รายงานผลการตรวจสอบคุณภาพโปรแกรม 4. รายงานการประเมินความพึงพอใจ 5. เอกสารการจัดการโครงการพัฒนาโปรแกรม

ระดับที่ 1 การเริ่มต้นการควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล
ระดับที่ 1 ของการพัฒนา

ระยะแรก เป็นการวางพื้นฐานที่จำเป็นของการควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

1.1 การระบุปัญหา ความต้องการให้เกิดการพัฒนาโปรแกรม

การพัฒนาโปรแกรมขึ้นมาใช้เองภายในโรงพยาบาลส่วนใหญ่มักจะเกิดจากปัญหาของระบบงานเดิมที่ทำให้บุคลากรของโรงพยาบาลอยากจะใช้เทคโนโลยีสารสนเทศช่วยปรับปรุงระบบงานเดิม หรือบุคลากรเคยใช้โปรแกรมเดิมอยู่แล้วแต่อยากจะปรับปรุงให้โปรแกรมเดิมทำงานได้ครบถ้วนมีประสิทธิภาพมากขึ้น จึงร้องขอมายังฝ่ายเทคโนโลยีสารสนเทศให้ช่วยพัฒนาโปรแกรมใหม่ขึ้นมากเพื่อใช้แก้ปัญหาของระบบงานเดิม

เมื่อเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศรับคำร้องขอแล้ว ก็ควรจัดประชุมร่วมกับฝ่ายผู้ใช้งานระบบแล้วบันทึกปัญหาต่างๆตลอดจนความต้องการของฝ่ายผู้ใช้ เพื่อให้เข้าใจตรงกันว่า ปัญหาและความต้องการทั้งหมดมีกี่เรื่อง มีประเด็นสำคัญอะไรบ้าง ดังตัวอย่างรายงานผลการสำรวจปัญหาและความต้องการให้เกิดการพัฒนาโปรแกรมดังนี้

โปรแกรมรวบรวมข้อมูลและรายงานโรคระบาดและโรคที่ต้องเฝ้าระวัง [1]
รายงานผลการสำรวจปัญหาและความต้องการให้เกิดการพัฒนาโปรแกรม
วันที่รายงาน 15 พฤษภาคม 2561

ปัญหาในการแจ้งเตือนและรายงานโรคของระบบเดิม คือ

1. การแจ้งข่าวหรือรายงานโรคล่าช้า ทำให้การสอบสวน ควบคุมป้องกันโรคได้ไม่ทันการณ์
2. เกิดความสับสนในรหัสระบาดวิทยา (Code 506) ที่จะต้องแจ้งให้เฝ้าระวัง และสอบสวน
3. เพิ่มภาระงานให้กับพยาบาล ที่จะต้องรายงานอย่างรวดเร็ว ซึ่งบางครั้งมีภาระที่จะต้องให้การพยาบาลกับผู้ป่วยจำนวนมากทำให้ไม่สามารถแจ้งเตือนได้ทันเวลาหรือในภายหลังได้ เป็นเหตุให้เกิดการรายงานล่าช้า
4. การติดต่อหรือประสานงานกับเจ้าหน้าที่ที่รับผิดชอบ ไม่สามารถดำเนินการได้

ความต้องการในระบบใหม่จากผู้ใช้ระบบ

1. โปรแกรมสามารถแจ้งเตือนผู้ที่เกี่ยวข้องกับงานระบาด ในพื้นที่ที่ผู้ป่วยอยู่ได้อย่างรวดเร็ว และถูกต้อง
2. เจ้าหน้าที่งานระบาดระดับ อำเภอ สามารถรับทราบการเกิดโรคระบาดภายใน อำเภอของตัวเองได้

3. มีการจำกัดสิทธิ์ให้แต่ละผู้ใช้เป็น 3 ระดับ คือ

1. ระดับ Admin จังหวัด (รพท. , สสจ)

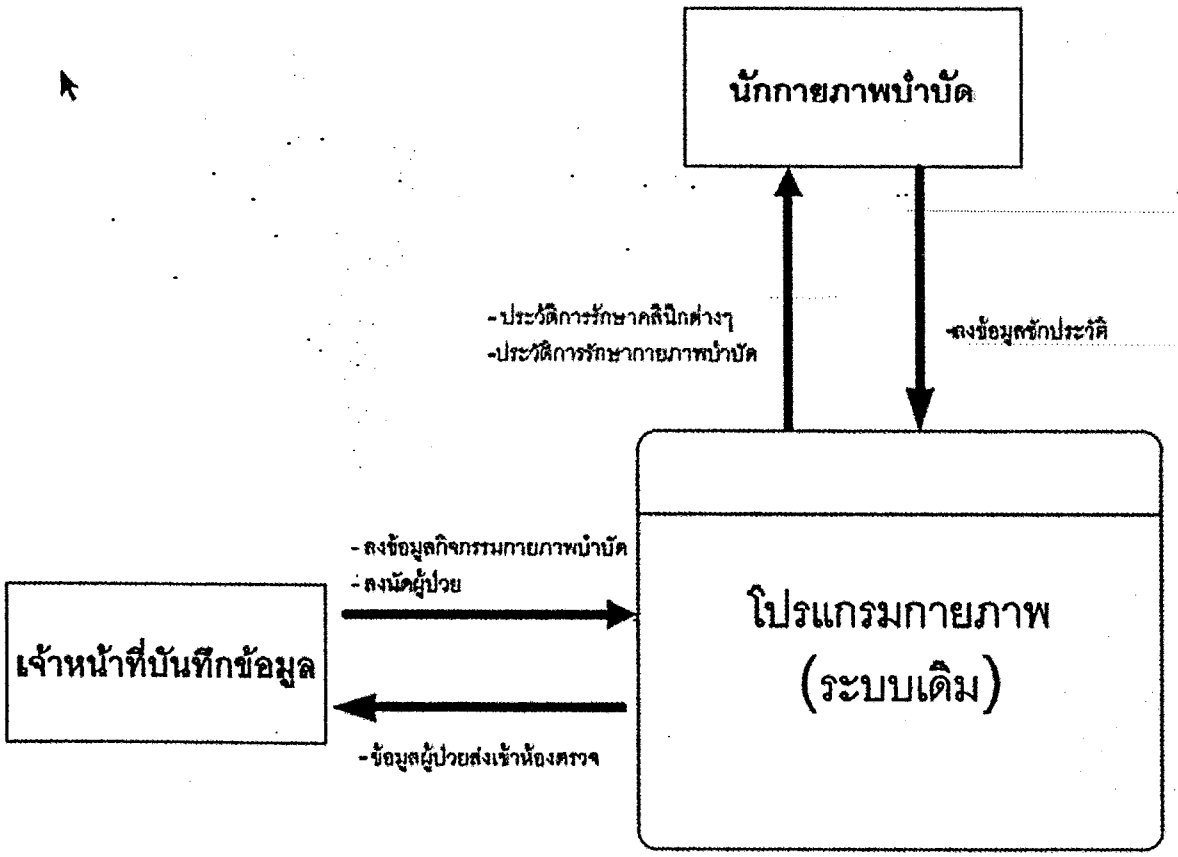
2. ระดับเจ้าหน้าที่ระบาดระดับอำเภอ โรงพยาบาลชุมชน

3. ระดับเจ้าหน้าที่ใน รพ.สต.

1.2 การวิเคราะห์ระบบงานปัจจุบัน

การวิเคราะห์ระบบงานปัจจุบัน เป็นการวิเคราะห์ที่ฝ่ายเทคโนโลยีสารสนเทศทำโดยการศึกษาและสังเกตการทำงานของระบบ เพื่อทำความเข้าใจระบบการทำงานปัจจุบัน โดยผลการวิเคราะห์ที่ได้จะนำมาเพื่อใช้ในการออกแบบระบบเทคโนโลยีสารสนเทศเพื่อปรับปรุงระบบงานทำงานได้มีประสิทธิภาพยิ่งขึ้น

เมื่อวิเคราะห์ระบบงานปัจจุบันแล้ว ควรจัดทำรายงานผลการวิเคราะห์ระบบงานปัจจุบัน โดยอาจรายงานในรูปแบบคำอธิบายขั้นตอนการทำงานของระบบงานปัจจุบัน หรือแสดงผลเป็น System Flow Chart หรือ Context Diagram ตามภาพที่ 6.1

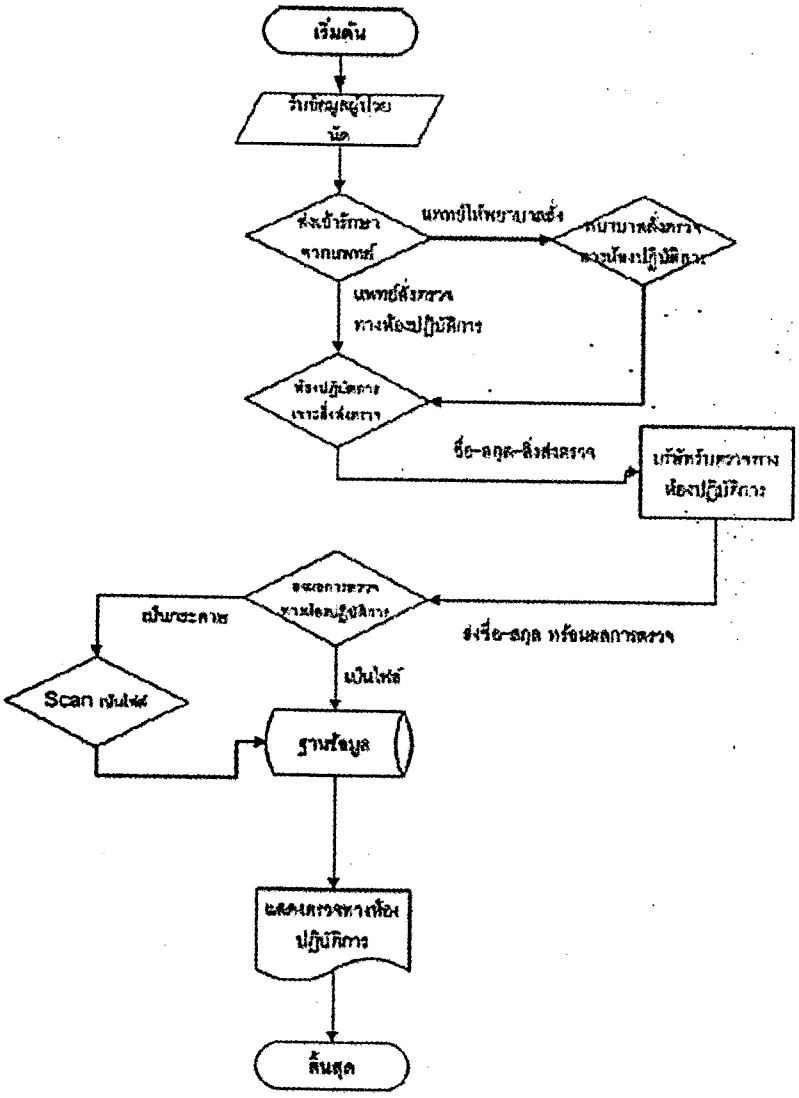


ภาพที่ 6.1 ตัวอย่างการนำเสนอระบบงานปัจจุบัน โดยใช้ Context Diagram [2]

1.3 การออกแบบระบบใหม่ด้านขั้นตอนการทำงาน

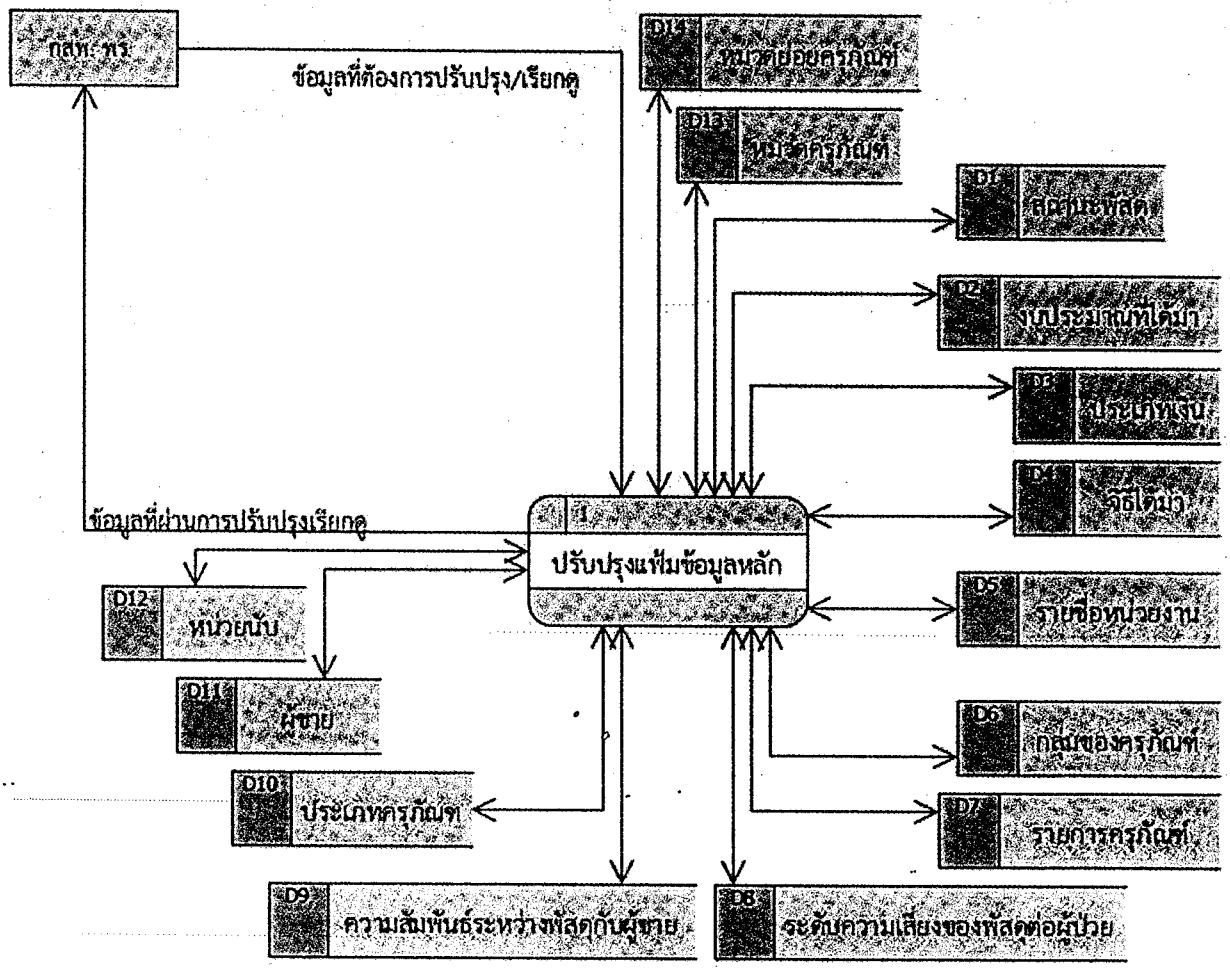
การออกแบบระบบใหม่ด้านขั้นตอนการทำงาน มีวัตถุประสงค์เพื่อทำให้มั่นใจว่า ระบบงานใหม่มีประสิทธิภาพที่ดีขึ้นกว่าระบบงานเดิม โดยทั่วไปการใช้เทคโนโลยีสารสนเทศจะทำให้ลดการบันทึกข้อมูลที่ซ้ำซ้อน และอาจช่วยลดขั้นตอนการทำงานในบางส่วนได้ ทำให้ระบบใหม่ช่วยให้ผู้ใช้ทำงานได้สะดวก รวดเร็วกว่าเดิม

เมื่อออกแบบระบบใหม่ด้านขั้นตอนการทำงานแล้ว ควรบันทึกรายละเอียดการออกแบบไว้ในเอกสารการออกแบบระบบ โดยอาจแสดงการออกแบบในรูปแบบคำอธิบายขั้นตอนการทำงานของระบบใหม่เปรียบเทียบกับระบบงานปัจจุบัน หรือแสดงผลเป็น Context Diagram หรือ System Flow Chart ตามภาพที่ 6.2

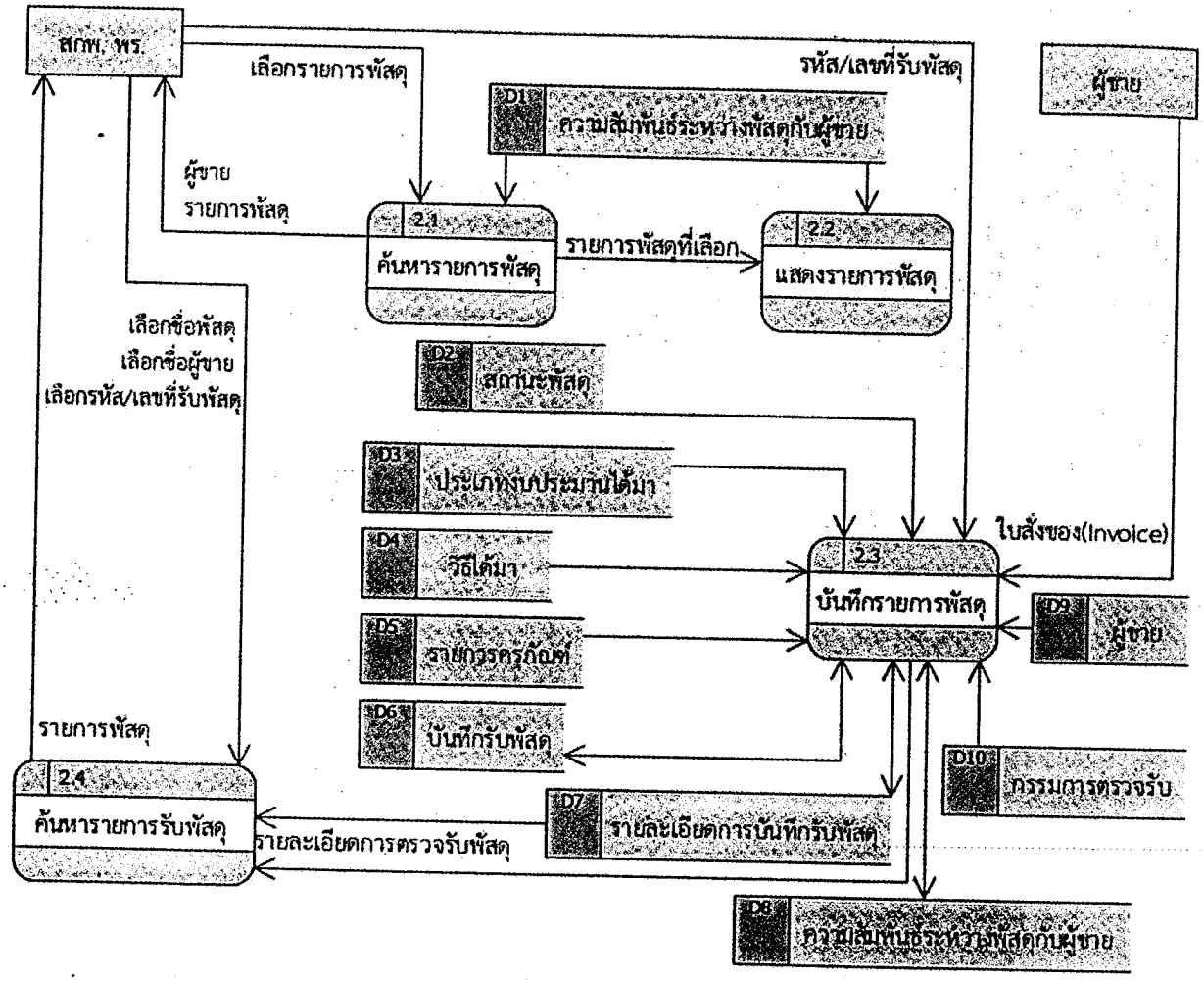


ภาพที่ 6.2 ตัวอย่างการออกแบบระบบงานใหม่ด้านขั้นตอนการทำงาน โดยใช้ Flow Chart [2]

การออกแบบขั้นตอนการทำงานยังจะได้ออกแบบรายละเอียดการรับส่งข้อมูล (Data Flow) ด้วย โดยต้องเขียนเป็นไดอะแกรมเรียกว่า Data Flow Diagram – DFD ดังตัวอย่างในภาพที่ 6.3 และ 6.4 ดังนี้



ภาพที่ 6.3 ตัวอย่าง Data Flow Diagram [3]

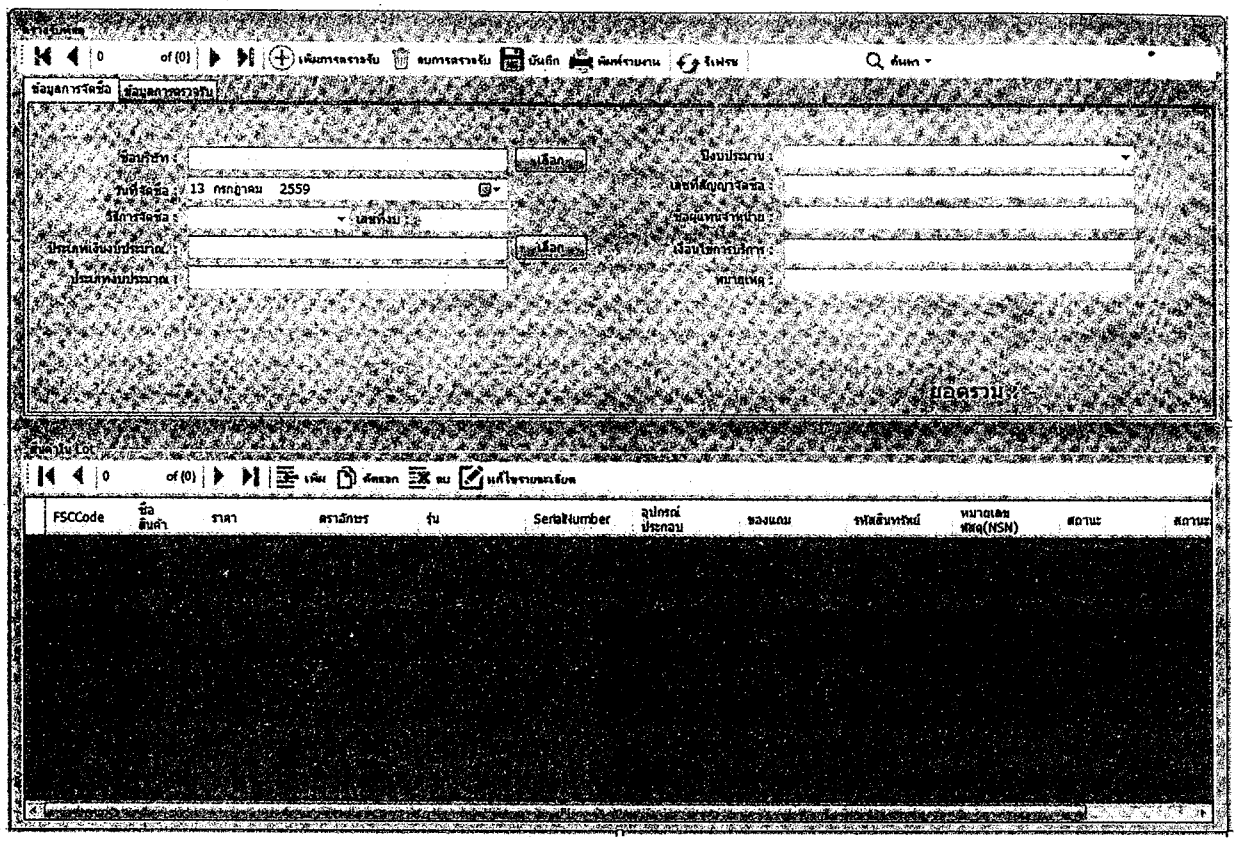


ภาพที่ 6.4 ตัวอย่าง Data Flow Diagram [3]

1.4 การออกแบบหน้าจอและส่วนติดต่อกับผู้ใช้งาน

การออกแบบหน้าจอและส่วนติดต่อกับผู้ใช้งาน เป็นการสร้างภาพหน้าจอให้ผู้ใช้เห็นก่อนลงมือเขียนโปรแกรม พร้อมทั้งการแสดงช่องรับข้อมูล กล่องแสดงทางเลือก ปุ่มกดต่างๆที่เป็นส่วนติดต่อกับผู้ใช้งาน โดยมีวัตถุประสงค์เพื่อให้ฝ่ายเทคโนโลยีสารสนเทศได้ติดต่อกับผู้ใช้อย่างมีประสิทธิภาพ เพราะหากผู้ใช้ได้เห็นหน้าจอโปรแกรมที่ตนเองจะต้องใช้งานก่อนการเริ่มเขียนโปรแกรม จะทำให้สามารถปรับปรุงหน้าจอให้ตรงกับความคาดหวังของผู้ใช้ให้ดีขึ้นก่อน โดยไม่ต้องเสียเวลาในการแก้โปรแกรม

การออกแบบหน้าจอในปัจจุบันสามารถทำได้อย่างง่ายดาย เนื่องจากมีโปรแกรมช่วยการออกแบบมากมายหลายโปรแกรม ภาพหน้าจอจะทำให้ผู้ใช้งานได้รับรู้ว่าโปรแกรมที่จะได้มา มีหน้าตาอย่างไร ดังตัวอย่างในภาพที่ 6.5

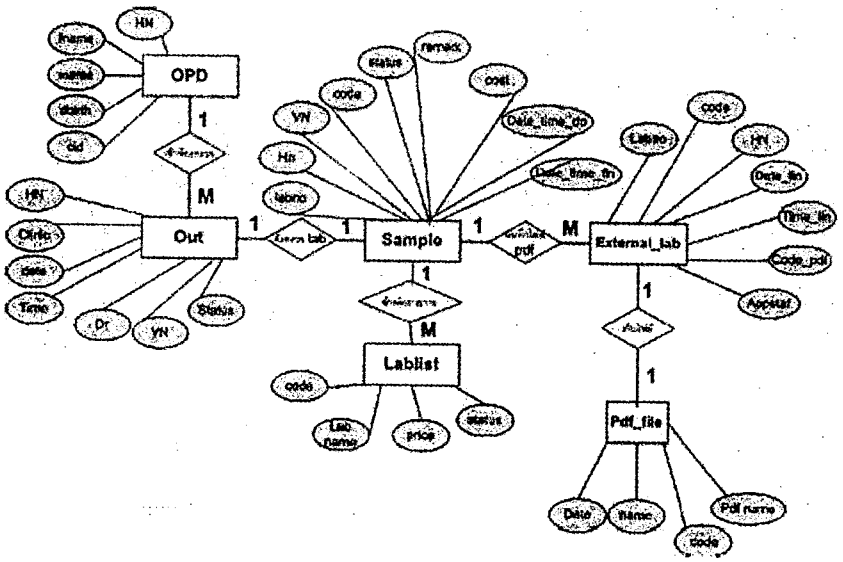


ภาพที่ 6.5 หน้าจอแสดงการจัดซื้อพัสดุของโรงพยาบาล [3]

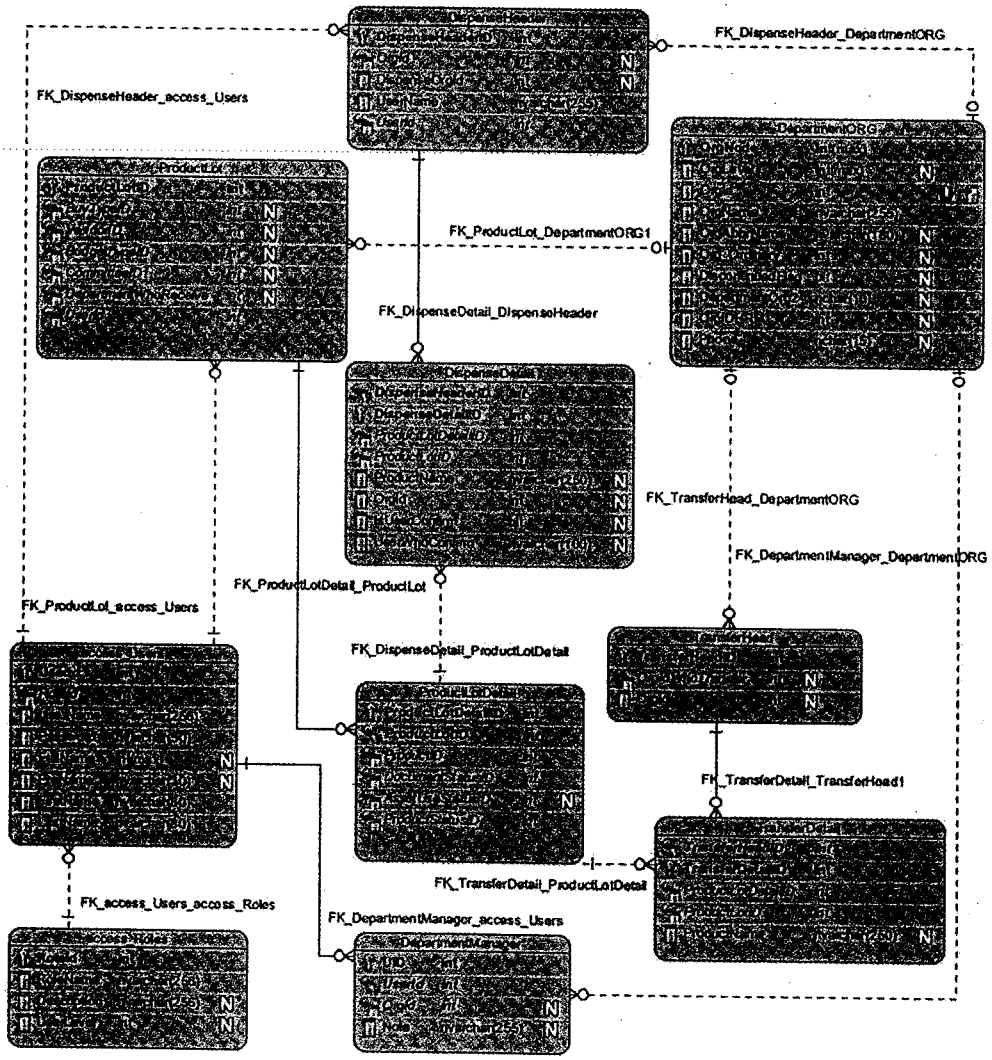
1.5 การออกแบบฐานข้อมูลสำหรับระบบฐานข้อมูลใหม่

โปรแกรมที่พัฒนาในโรงพยาบาลส่วนใหญ่เป็นโปรแกรมที่ต้องบันทึกและสืบค้นข้อมูลจากฐานข้อมูล การออกแบบระบบจึงต้องออกแบบฐานข้อมูลให้ดีด้วย เพื่อให้ได้ระบบฐานข้อมูลที่สามารถตอบสนองการจัดเก็บและสืบค้นข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ

การออกแบบฐานข้อมูลในปัจจุบันมี 2 แนวทาง โดยแนวทาง Object Oriented Design จะออกแบบโดยใช้ Class Diagram ส่วนแนวทาง Conventional Design จะออกแบบโดยใช้ Entity Relation –ER Diagram ดังตัวอย่างในภาพที่ 6.6 และ 6.7 ดังนี้



ภาพที่ 6.6 ตัวอย่าง ER Diagram [2]



ภาพที่ 6.7 ตัวอย่าง Class Diagram [3]

1.6 การสร้างพจนานุกรมข้อมูล

การสร้างพจนานุกรมข้อมูล (Data Dictionary) เป็นการบันทึกรายละเอียดของโครงสร้างและชนิดของข้อมูลที่อยู่ในฐานข้อมูลของโปรแกรม พจนานุกรมข้อมูลจะบอกว่าข้อมูลรายการใดเก็บไว้ที่ตารางไหน และมีลักษณะเป็นตัวอักษร หรือ ตัวเลข หรือเป็นรูปแบบอื่นๆ โดยหากไม่มีการจัดทำพจนานุกรมข้อมูล จะทำให้การปรับปรุงโปรแกรมในอนาคตเป็นได้โดยยากลำบาก นอกจากนั้น การเรียกดึงรายงานจากฐานข้อมูลให้ออกมาได้อย่างถูกต้องก็ต้องอาศัยพจนานุกรมที่ดี จึงสามารถเขียนคำสั่งที่ดึงรายงานได้อย่างมีประสิทธิภาพ

ตัวอย่างพจนานุกรมข้อมูล แสดงไว้ใน ตารางที่ 6.1 ดังนี้

Column	Data type	Nullability	Description
Remark	nvarchar(*50*)	null	*พัสดุนี้เป็นครุภัณฑ์เก่าหรือไม่*
DocRef	nchar(*10*)	null	*ที่หนังสือ แสดงเลขที่เอกการการตรวจรับ*
DocDate	datetime	Not null	*วันที่ทำรายการบันทึกรับพัสดุ*
DepartmentWhoReceive	int	null	*หน่วยงานที่รับสินค้าจากผู้ขาย (ส่งของไว้ที่)*
BudgetYear	int	null	*ปีงบประมาณที่ใช้จัดซื้อ*
ContractNo	nchar(*10*)	null	*เลขที่สัญญาจัดซื้อ*
SaleMan	nvarchar(*100*)	null	*ชื่อผู้ติดต่อ (ตัวแทนขาย)*
ConditionService	varchar(*255*)	null	*เงื่อนไขการบริการ*
UserName	nvarchar(*255*)	Not null	*ชื่อผู้ใช้ : สำหรับลงทะเบียนเข้าใช้งานระบบ*
UserId	int	Not null	*รหัสประจำตัวผู้ใช้งาน*

ตารางที่ 6.1 ตัวอย่างพจนานุกรมข้อมูล [3]

1.7 การจัดทำคู่มือสำหรับผู้ใช้งานโปรแกรมและการอบรม

คู่มือสำหรับผู้ใช้งานโปรแกรม (User Manual) เป็นเอกสารที่มีเนื้อหาแนะนำการใช้โปรแกรมให้กับผู้ใช้ หากเขียนคู่มือได้ดี ผู้ใช้จะสามารถใช้คู่มือศึกษาเรียนรู้วิธีการใช้โปรแกรมได้ด้วยตนเอง โดยเฉพาะเมื่อผู้ใช้ลืมวิธีการที่ได้รับการอบรมการใช้โปรแกรม

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดการฝึกอบรมให้กับผู้ใช้งานโปรแกรมก่อนเริ่มใช้งาน เพื่อให้ผู้ใช้เข้าใจขั้นตอนการทำงานของโปรแกรมและสามารถใช้โปรแกรมได้อย่างถูกต้องตามขั้นตอนที่ได้ออกแบบไว้ โดยผู้ใช้ควรได้รับการฝึกฝนการใช้โปรแกรมอย่างน้อย 2-3 ครั้ง ก่อนการเริ่มใช้งานโปรแกรมจริง โดยควรมีการประเมินด้วยว่าผู้ใช้สามารถใช้โปรแกรมได้อย่างถูกต้องแล้ว

1.8 การประเมินความพึงพอใจของผู้ใช้โปรแกรม

เมื่อเริ่มใช้โปรแกรมทำงานจริงสักระยะหนึ่ง ควรจัดให้มีการประเมินความพึงพอใจของผู้ใช้บริการ เพื่อให้ได้ข้อมูลว่าผู้ใช้บริการมีความรู้สึกอย่างไรต่อโปรแกรม และควรสำรวจประเด็นอื่นๆที่เกี่ยวข้องด้วย เช่น อยากให้โปรแกรมมีด้านในเพิ่มเติมหรือไม่ หรือส่วนติดต่อกับผู้ใช้ควรได้รับการปรับปรุงอย่างไร ฯลฯ

ผลการประเมินความพึงพอใจและทำให้ฝ่ายเทคโนโลยีสารสนเทศได้เข้าใจความรู้สึกของผู้ใช้โปรแกรม และยังสามารถนำผลการประเมินนี้มาใช้เป็นตัวชี้วัดความสำเร็จและติดตามการพัฒนาในอนาคตต่อไปได้ด้วย

ระดับที่ 2 การสร้างความแข็งแรง ของการควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล

ระดับที่ 2 ของการพัฒนา

การยกระดับการจัดระบบบริการในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 2 เป็นการสร้างความแข็งแรงให้กับระบบที่กำเนิดขึ้นมาในระดับที่ 1 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้จริงและทำให้งานดีขึ้น ระดับที่ 2 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

2.1 ทบทวนผลการดำเนินงานในระดับที่ 1

ก่อนที่จะมีการยกระดับการพัฒนา ควรทบทวนผลการดำเนินในระดับที่ 1 โดยใช้หลักการ Plan-Do-Check-Act กล่าวคือ การดำเนินงานในระดับที่ 1 เป็นขั้นตอนของ Plan และ Do เมื่อดำเนินการไปสักระยะหนึ่ง ก็ควร ทบทวนประเมินผล (Check) ก่อนจะที่ยกระดับเป็นระดับที่ 2 (Act) ต่อไปนั่นเอง การประเมินการดำเนินงานที่ผ่านมา จะทำให้เราเห็นโอกาสที่จะปรับปรุงโปรแกรมที่ยังไม่ครอบคลุมบริการสำคัญ

หรือไม่ชัดเจน ให้ครอบคลุมบริการสำคัญและชัดเจนมากขึ้น เพื่อทำให้ได้โปรแกรมที่ทำงานได้ดีขึ้น รวมถึงการปรับปรุงโปรแกรมให้เป็นไปตามมาตรฐานมากขึ้น ดังนั้น การดำเนินการในระดับที่ 2 จึงเป็นการทำซ้ำการดำเนินการในระดับที่ 1 อีกรอบหนึ่งแต่เป็นการหมุนวงล้อ PDCA ที่ทำให้ระดับคุณภาพสูงขึ้น

อย่างไรก็ตาม การดำเนินการในระดับที่ 2 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการจัดระบบควบคุมรุ่นของโปรแกรม เพื่อบันทึกรายละเอียดและวันเวลาการปรับปรุงแก้ไขโปรแกรม และความแตกต่างของการปรับปรุงโปรแกรมในแต่ละครั้ง การเขียนหมายเหตุในรหัสต้นฉบับ และการจัดระบบตรวจสอบคุณภาพโปรแกรม

2.2 การจัดระบบควบคุมรุ่นของโปรแกรม (Software Version Control)

การจัดระบบควบคุมรุ่นของโปรแกรม คือการดำเนินการให้มั่นใจ ทุกครั้งที่มีการแก้ไขโปรแกรม ผู้ที่แก้ไขต้องบันทึกรายละเอียดการแก้ไข วันเวลาที่แก้ไข ไว้ในตารางที่เก็บรายละเอียดการควบคุมรุ่นของโปรแกรม (ตารางที่ 6.2) เพื่อไว้อ้างอิงและเรียกดูในอนาคต นอกจากนั้น การบันทึกรหัสต้นฉบับ (Source Code) ของโปรแกรมก็ต้องบันทึกรหัสต้นฉบับแต่ละรุ่นและจัดเก็บแยกไว้อย่างเป็นระบบ เพื่อป้องกันไม่ให้เกิดเหตุการณ์รหัสต้นฉบับสูญหายไป ค้นหาไม่พบ

โปรแกรมรุ่น	วันที่แก้ไข	รายละเอียดการแก้ไข
0.7	12/01/2018	เพิ่มเติมปุ่มแก้ไขข้อมูล เพิ่มหน้าจอตัวช่วยค้นหารหัสสินค้า

ตารางที่ 6.2 ตารางการควบคุมรุ่นของโปรแกรม

2.3 การเขียนหมายเหตุในรหัสต้นฉบับ

การเขียนหมายเหตุในรหัสต้นฉบับ (Source Code Comments) เป็นขั้นตอนที่สำคัญส่วนหนึ่งในการเขียนโปรแกรม เพราะหมายเหตุในรหัสต้นฉบับเป็นคำอธิบายให้คนอื่นที่ไม่ได้เป็นคนเขียนโปรแกรมได้อ่านแล้วทำความเข้าใจการทำงานในส่วนต่างๆของรหัสต้นฉบับได้โดยง่าย อย่างไรก็ตาม ถ้าโปรแกรมเมอร์ย่อหย่อนในการทำงาน ก็อาจไม่เขียนหมายเหตุเลย หรือเขียนหมายเหตุสั้นเกินไปจนคนอื่นมาอ่านก็ไม่เข้าใจอยู่ดี

การเขียนหมายเหตุในรหัสต้นฉบับ จึงควรเขียนอธิบายรายละเอียดมากพอสมควร โดยส่วนสำคัญที่ต้องมีหมายเหตุ ได้แก่ ฟังก์ชั่นการทำงานต่างๆ ลักษณะของ Class (ในกรณีการเขียนโปรแกรมแบบ Object Oriented) และ หน้าที่ของตัวแปรต่างๆ

2.4 การจัดระบบตรวจสอบคุณภาพโปรแกรม

เพื่อพัฒนาโปรแกรมไปสักระยะหนึ่ง หรือเมื่อพัฒนาโปรแกรมเสร็จแล้ว ฝ่ายเทคโนโลยีสารสนเทศควรวางระบบเพื่อตรวจสอบคุณภาพโปรแกรมที่พัฒนาเสร็จ โดยการทดสอบเพื่อตรวจสอบคุณภาพโปรแกรมสามารถแบ่งได้เป็น 2 ชนิด คือ การทดสอบโดยบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศ และการทดสอบโดยบุคลากรภายนอกฝ่ายเทคโนโลยีสารสนเทศ

การทดสอบโดยบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศ เป็นการทดสอบว่าโปรแกรมทำงานได้ถูกต้องตามเทคนิคที่กำหนดไว้หรือไม่ เช่น บันทึกข้อมูลได้ครบถ้วน ส่งต่อไปยังส่วนต่างๆได้ตามที่ออกแบบ ไม่เกิดความผิดพลาดหรือการหยุดทำงาน การทดสอบนี้ควรเกิดขึ้นก่อนส่งมอบให้กับผู้ใช้

การทดสอบโดยบุคลากรภายนอก ส่วนหนึ่งเป็นการให้ผู้ใช้ทดสอบโปรแกรม โดยเป็นการทดสอบโปรแกรมทำงานได้ตามความต้องการที่กำหนดไว้ตั้งแต่แรกหรือไม่ ขั้นตอนต่างๆเป็นไปอย่างเหมาะสมถูกต้องหรือไม่ เพื่อให้ผู้ใช้มั่นใจว่าได้โปรแกรมที่นำไปใช้ประโยชน์ได้จริง อีกส่วนหนึ่งเป็นการทดสอบโดยผู้เชี่ยวชาญ ซึ่งทำเพื่อให้มั่นใจว่าโปรแกรมมีความมั่นคงปลอดภัย ไม่เกิดช่องโหว่ให้ใครเจาะเข้ามาในระบบได้

ระดับที่ 3 การสร้างความยั่งยืน การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล

ระดับที่ 3 ของการพัฒนา

การยกระดับการควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาลขึ้นสู่ระดับที่ 3 เป็นการสร้างความแข็งแรงให้กับระบบที่พัฒนาจากระดับที่ 1 และ 2 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้อย่างมั่นคงและยั่งยืน ระดับที่ 3 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

3.1 ทบทวนผลการดำเนินงานในระดับที่ 2

เป็นการหมุนวงล้อ PDCA รอบต่อไปที่ทำให้ระดับคุณภาพสูงขึ้นอีก โดยทบทวนกระบวนการทั้งหมดอย่างเป็นระบบ ปรับปรุงกระบวนการที่สำคัญ ดังต่อไปนี้

- การวิเคราะห์ระบบ
- การออกแบบระบบและหน้าจอผู้ใช้
- การออกแบบฐานข้อมูล
- ระบบรักษาความปลอดภัยของโปรแกรม
- วิเคราะห์ความก้าวหน้าที่ผ่านมา ตั้งแต่ระดับที่ 1 มาระดับที่ 2 และระดับปัจจุบัน ควรแสดงให้การพัฒนาและยกระดับคุณภาพอย่างต่อเนื่อง

อย่างไรก็ตาม การดำเนินการในระดับที่ 3 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการตรวจสอบคุณภาพโปรแกรม การประเมินความพึงพอใจของผู้ใช้ และการจัดการโครงการพัฒนาโปรแกรม

3.1 การตรวจสอบคุณภาพโปรแกรม

การตรวจสอบคุณภาพโปรแกรมในการพัฒนาระดับที่ 3 นี้ เป็นการตรวจสอบโดยเข้มข้นเพื่อให้มั่นใจว่าโปรแกรมมีคุณภาพและมั่นคงปลอดภัยแน่นอน โดยการทดสอบโดยบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการอย่างน้อยดังต่อไปนี้

- Unit Testing
- Validating Test
- Security Test

การทดสอบโดยบุคลากรภายนอก ต้องดำเนินการอย่างน้อยดังต่อไปนี้

- Requirements fulfillment Testing
- User Acceptance Test
- Security Test

3.2 การประเมินความพึงพอใจของผู้ใช้โปรแกรม

เมื่อเริ่มใช้โปรแกรมทำงานจริงสักระยะหนึ่ง ควรจัดให้มีการประเมินความพึงพอใจของผู้ใช้บริการ เพื่อให้ได้ข้อมูลว่าผู้ใช้บริการมีความรู้สึกอย่างไรต่อโปรแกรม และควรสำรวจประเด็นอื่นๆที่เกี่ยวข้องด้วย เช่น อยากให้โปรแกรมมีด้านในเพิ่มเติมหรือไม่ หรือส่วนติดต่อกับผู้ใช้ควรได้รับการปรับปรุงอย่างไร ฯลฯ

ผลการประเมินความพึงพอใจและทำให้ฝ่ายเทคโนโลยีสารสนเทศได้เข้าใจความรู้สึกของผู้ใช้โปรแกรม และยังสามารถนำผลการประเมินนี้มาใช้เป็นตัวชี้วัดความสำเร็จและติดตามการพัฒนาในอนาคตต่อไปได้ด้วย

3.3 การจัดการโครงการพัฒนาโปรแกรม

ทุกครั้งที่มีการพัฒนาโปรแกรมขึ้นมาใหม่ ควรมีการจัดการโครงการพัฒนาโปรแกรม (Software Development Project Management) ที่ดี โดยมีวัตถุประสงค์เพื่อให้ได้ระบบใหม่ที่มีคุณภาพ ตรงตามความต้องการ สำเร็จใช้งานได้ทันเวลา ภายในงบประมาณที่กำหนด

ทุกๆโครงการควรมีผู้ทำหน้าที่ ผู้จัดการโครงการ (Project Manager) รับผิดชอบบริหารโครงการตั้งแต่ต้นจนจบ ด้วยทำงานร่วมกับ ผู้สนับสนุนโครงการ (Project Sponsor) ซึ่งมาจากทีมผู้บริหารโรงพยาบาลคนใดคนหนึ่งขึ้นอยู่กับลักษณะของโครงการ ผู้สนับสนุนโครงการทำหน้าที่กำกับดูแลการใช้งบประมาณและให้การสนับสนุนทรัพยากรที่จำเป็นในการผลักดันโครงการไปสู่ความสำเร็จ

การจัดการโครงการที่ดี ประกอบไปด้วย กระบวนการที่สำคัญดังนี้

1. การริเริ่มโครงการ (Project Initiating) ประกอบด้วย การกำหนดวัตถุประสงค์ ขอบเขต ข้อจำกัด ความเสี่ยง หารือผู้ที่เกี่ยวข้อง เขียนข้อเสนอโครงการ และ ขออนุมัติโครงการ
2. การวางแผนโครงการ (Project Planning) ประกอบด้วย การเขียนความต้องการ ความคาดหวัง ข้อจำกัด โดยละเอียดทั้งหมด จัดตั้งทีมงาน กำหนดบทบาทหน้าที่ของแต่ละคน แตกโครงการย่อย ค้นหาเส้นทางความเสี่ยง (Critical Path Method – CPM) พัฒนาแผนจัดการความเปลี่ยนแปลง จัดการกระบวนการเริ่มโครงการ (Kick-off)
3. การดำเนินโครงการ (Project Executing) ประกอบด้วย การดำเนินการไปตามแผนที่วางไว้ การประสานงาน การติดตามความก้าวหน้า การจัดการปัญหา การรายงานผลการดำเนินโครงการให้กับฝ่ายบริหาร จนถึงการติดตั้งและเริ่มใช้งานระบบใหม่
4. การติดตามและควบคุมโครงการ (Project Monitoring and Control) ประกอบด้วย การตรวจสอบว่าโครงการดำเนินไปตามแผนหรือไม่ ผลงานตรงตามมาตรฐานและความต้องการของผู้ใช้หรือไม่ ควบคุมไม่ให้เกิดความต้องการเพิ่มเติมจากขอบเขตที่กำหนดไว้เดิม ควบคุมปัจจัยเสี่ยงต่างๆ
5. การปิดโครงการ (Project Closing) ประกอบด้วย การสรุปผลการใช้งบประมาณและทรัพยากรต่างๆ การตรวจรับระบบ ส่งคืนบุคลากรที่มาจากฝ่ายต่างๆ เขียนรายงาน สรุปบทเรียน วัดความพึงพอใจของผู้ใช้งานในระยะแรก

เมื่อระบบใหม่ทำงานได้ตามที่ต้องการแล้ว ควรมีกระบวนการตอบสนองคำร้องจากผู้ใช้ (Request Fulfillment) ที่ดีด้วย เนื่องจากผู้ใช้อาจต้องการเพิ่มสิทธิการใช้ เพิ่มจุดใช้ระบบ ต้องการให้พัฒนาระบบเพิ่มเติม ฯลฯ กระบวนการตอบสนองคำร้องจากผู้ใช้ ประกอบด้วย การเปิดช่องทางให้ส่งคำร้อง การจัดการคำร้องให้โดยระบบอัตโนมัติ (ในกรณีที่คำร้องเป็นเรื่องง่ายๆ เช่น Reset Password) การส่งคำร้องไปขอคำอนุมัติจากผู้บริหาร การจัดสรรทรัพยากร (เงิน สิ่งของ แรงงาน) เพื่อดำเนินการตามคำร้อง การสรุปผลการดำเนินการตามคำร้อง (ดูเรื่องการจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล)

REFERENCES

1. ฝ่ายเทคโนโลยีสารสนเทศ โรงพยาบาลน่าน. (2560). การวิเคราะห์และออกแบบระบบ Smart EPI NH. โรงพยาบาลน่าน.

2. ฝ่ายเทคโนโลยีสารสนเทศ โรงพยาบาลมหาสารคาม. (2559). การวิเคราะห์และออกแบบระบบนำเข้าผลการตรวจทางห้องปฏิบัติการจากภายนอก. โรงพยาบาลมหาสารคาม.

3. กลุ่มงานสารสนเทศและเวชระเบียน โรงพยาบาลสมเด็จพระนางเจ้าสิริกิติ์. (2559). การวิเคราะห์และออกแบบระบบจัดการครุภัณฑ์โรงพยาบาล. โรงพยาบาลสมเด็จพระนางเจ้าสิริกิติ์.

บทที่ 7

การจัดการศักยภาพและการจัดการการเปลี่ยนแปลง ในระบบเทคโนโลยีสารสนเทศโรงพยาบาล (Capacity and Change Management in Hospital Information System)

การจัดการศักยภาพ (Capacity Management) ในระบบเทคโนโลยีสารสนเทศโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมีศักยภาพที่จะทำงานได้อย่างราบรื่น ไม่หยุดชะงัก หรือสะดุดติดขัด โดยหัวใจหลักคือการประเมินศักยภาพปัจจุบัน ทั้งด้าน Hardware, software, network และบุคลากรว่าจะศักยภาพเพียงพอหรือไม่ ถ้าพบว่าศักยภาพด้านใดยังไม่เพียงพอก็ต้องคิดวางแผนหาทางเพิ่มศักยภาพให้เพียงพอ รวมทั้งวางแผนการจัดการศักยภาพในระยะยาวด้วย

การจัดการการเปลี่ยนแปลง (Change Management) ในระบบเทคโนโลยีสารสนเทศโรงพยาบาลมีวัตถุประสงค์เพื่อทำให้มั่นใจว่า การนำเทคโนโลยีสารสนเทศมาใช้ในรูปแบบใหม่ที่เปลี่ยนวิธีการทำงานเดิม จะเกิดขึ้นได้โดยไม่มีปัญหาอุปสรรคที่ทำให้การเปลี่ยนแปลงล้มเหลว และยังรวมถึงกระบวนการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศตามความต้องการใหม่ๆที่เกิดขึ้นอีกด้วย

การจัดการศักยภาพและการจัดการการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาลสามารถแบ่งได้เป็น 3 ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลของสมาคมเวชสารสนเทศไทย ดังนี้

ระดับที่ 1 การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ 2 ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ 3 ระบบขับเคลื่อนแล้ว เสริมระบบให้แข็งแกร่งและมั่นคงยั่งยืน

ในแต่ละระดับ ควรมีกิจกรรมที่สำคัญแสดงในรูปแบบตารางดังต่อไปนี้

ระดับที่ 1

กระบวนการทำงาน	ผลผลิต
1. การสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศ 2. การวิเคราะห์ช่องว่าง (Gap Analysis) 3. การจัดทำแผนเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศ 4. การจัดทำแบบประเมินสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ 5. การประเมินสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ	1. รายงานผลการสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศ 2. รายงานผลการวิเคราะห์ช่องว่าง 3. แผนเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศ 4. แบบประเมินสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ 5. ผลการประเมินสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

ระดับที่ 1 (ต่อ)

กระบวนการทำงาน	ผลผลิต
6. การวางแผนพัฒนาสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ	6. แผนพัฒนาสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

ระดับที่ 2

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 1 2. ปรับปรุงแผนการจัดการศักยภาพและแผนพัฒนาสมรรถนะที่ยังไม่เหมาะสม 3. การวางแผนจัดการการเปลี่ยนแปลงระบบการทำงาน	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 1 2. แผนการจัดการศักยภาพและแผนพัฒนาสมรรถนะฉบับปรับปรุงใหม่ 3. แผนจัดการการเปลี่ยนแปลงระบบการทำงาน

ระดับที่ 3

กระบวนการทำงาน	ผลผลิต
1. ทบทวนผลการดำเนินงานในระดับที่ 2 2. ปรับปรุงแผนการจัดการศักยภาพและแผนพัฒนาสมรรถนะที่ยังไม่เหมาะสม 3. สร้างระบบจัดการการเปลี่ยนแปลง	1. รายงานผลการทบทวนการดำเนินงานในระดับที่ 2 2. แผนการจัดการศักยภาพและแผนพัฒนาสมรรถนะฉบับปรับปรุงใหม่ 3. ระบบจัดการการเปลี่ยนแปลง

ระดับที่ 1 การเริ่มต้นจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล
ระดับที่ 1 ของการพัฒนา

ระดับแรก เป็นการวางพื้นฐานที่จำเป็นของการจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

1.1 การสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศ

การสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศ เป็นกระบวนการตรวจสอบและทำบัญชีทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดของโรงพยาบาล เพื่อให้ทราบสถานะปัจจุบัน ก่อนที่จะเพิ่มเติมในส่วนที่ขาดหรือปรับปรุงแก้ไขในส่วนที่ล้าสมัย เพื่อให้ทรัพยากรทั้งหมดตอบสนองต่อการดำเนินการตามแผนยุทธศาสตร์ที่กำหนดไว้อย่างมีประสิทธิภาพ

ทรัพยากรเทคโนโลยีสารสนเทศในองค์การ แบ่งได้เป็น 5 กลุ่มดังนี้

1. Hardware ทรัพยากรกลุ่มนี้ ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องสถานีทำงาน เครื่องพิมพ์ อุปกรณ์นำเข้าข้อมูล อุปกรณ์แสดงภาพหรือเสียง เป็นต้น
2. Software ทรัพยากรกลุ่มนี้ ได้แก่ โปรแกรมที่องค์การนำมาใช้งานในหน่วยงานต่างๆ โดยอาจเป็นโปรแกรมสำเร็จรูป หรือ โปรแกรมที่พัฒนาขึ้นมาสำหรับโรงพยาบาลโดยเฉพาะ
3. Network ทรัพยากรกลุ่มนี้ ได้แก่ ระบบเครือข่ายภายในองค์การ และระบบเครือข่ายที่เชื่อมโยงกับระบบภายใน คืออินเทอร์เน็ตและระบบโทรศัพท์ไร้สาย
4. People ทรัพยากรกลุ่มนี้ ได้แก่ นักบริหารเทคโนโลยีสารสนเทศ มีความรู้ด้านการจัดการเทคโนโลยีสารสนเทศ แต่จะไม่รู้ลึกลงไปในเนื้อหาเทคโนโลยีสารสนเทศมากนัก ทำหน้าที่ จัดการการใช้เทคโนโลยีสารสนเทศในองค์การให้มีประสิทธิภาพ และ นักวิชาการเทคโนโลยีสารสนเทศ มีความรู้ลึกด้านเทคโนโลยีสารสนเทศด้านต่างๆ เช่น ผู้บริหารเครือข่าย ผู้บริหารฐานข้อมูล นักวิเคราะห์ระบบ โปรแกรมเมอร์ ช่างซ่อมบำรุงคอมพิวเตอร์ เป็นต้น
5. Data and Information ทรัพยากรกลุ่มนี้ ได้แก่ ข้อมูล สารสนเทศ ที่สำคัญของโรงพยาบาล คือ ข้อมูลในเวชระเบียน และข้อมูลการดำเนินการด้านต่างๆของแต่ละแผนก

การทำบัญชีทรัพยากรด้านเทคโนโลยีสารสนเทศ จะทำให้ทราบสถานภาพของทรัพยากรด้านต่างๆ โดยต้องมีการปรับปรุงบัญชีทรัพยากรนี้เป็นระยะ อย่างน้อยทุกๆ 3-6 เดือน เพื่อติดตาม เฝ้าระวัง ไม่ให้เกิดการขาดแคลนทรัพยากร หรือ ทรัพยากรเสื่อมและลดคุณภาพโดยไม่รู้ตัว โดยเฉพาะคุณภาพข้อมูล

ตัวอย่างบัญชีทรัพยากรเทคโนโลยีสารสนเทศ แสดงไว้ในตารางที่ 7.1

ตารางที่ 7.1 ตัวอย่างบัญชีทรัพยากรเทคโนโลยีสารสนเทศ ประเภท Hardware และ Software

รายการ	ราคา	วันที่นำเข้ามาใช้	ใช้งานมาแล้ว (ปี)	ตำแหน่ง	สถานภาพปัจจุบัน
1. HP Server	250,000	2 มค. 50	5	IT Center	ใช้งานได้ Hard Disk เต็ม 70%
2. Brother Laser Printer	50,000	2 มค. 50	5	ห้องผอ.	สภาพ 80%
3. โปรแกรม Oracle Finance	1,000,000	1 ต.ค. 52	3	งานการเงินและบัญชี	ใช้งานได้ 85 %

1.2 การวิเคราะห์ช่องว่าง (Gap Analysis)

เมื่อสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาลเสร็จสิ้นแล้ว ควรดำเนินการวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อประเมินความแตกต่างระหว่างสถานะปัจจุบันกับเป้าหมายหรือมาตรฐานที่ควรจะเป็น ทั้งนี้ผลของการวิเคราะห์ช่องว่าง จะนำมาจัดทำแผนปฏิบัติการเพื่อเติมเต็มช่องว่างนั่นเอง

ลักษณะการวิเคราะห์ช่องว่าง จะวิเคราะห์ 4 ด้านดังนี้

1. รายการที่วิเคราะห์
2. สถานะในปัจจุบัน
3. สถานะที่ควรจะเป็น
4. แนวทางดำเนินการแก้ไข

ตัวอย่างการวิเคราะห์ช่องว่างเป็นดังตารางที่ 7.2 ดังนี้

ตารางที่ 7.2 Gap Analysis ทรัพยากรเทคโนโลยีสารสนเทศ

รายการ	สถานการณ์ปัจจุบัน	เป้าหมายที่ต้องการ	การดำเนินการ
1. Database Server	RAM 4 GB (80% Utilization) Harddisk 500 GB (80% use)	RAM 8 GB Add new harddisk	จัดซื้อเพิ่มเติม
2. Software ระบบบัญชี	License 5 users	License 10 user	จัดซื้อเพิ่มเติม
3. นักวิเคราะห์ระบบ	1 คน	3 คน	ขออนุมัติจ้างเพิ่มเติม

1.3 การจัดทำแผนเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศ

การวางแผนศักยภาพเทคโนโลยีสารสนเทศ (Capacity Planning) เป็นการสำรวจและวิเคราะห์ศักยภาพของทรัพยากรด้าน Hardware และ Network เพื่อวางแผนจัดการให้ทรัพยากรเหล่านี้ไม่ขาดแคลน ป้องกันปัญหาที่จะเกิดขึ้น และให้มั่นใจว่าใช้ทรัพยากรอย่างมีประสิทธิภาพ การวางแผนศักยภาพเทคโนโลยีสารสนเทศ ประกอบไปด้วยขั้นตอน 9 ขั้นตอนดังนี้

1. กำหนดบุคลลที่รับผิดชอบในการวางแผนศักยภาพเทคโนโลยีสารสนเทศ
2. กำหนดทรัพยากรที่ต้องการวัดศักยภาพ เช่น CPU Capacity, Memory, Storage, Bandwidth ฯลฯ
3. ลงมือวัดการใช้งานหรือผลการทำงานของทรัพยากรที่กำหนดไว้
4. เปรียบเทียบผลที่ได้จากการวัดกับมาตรฐานหรือความสามารถสูงสุด
5. รวบรวมข้อมูลการใช้งานทรัพยากรจากผู้พัฒนาระบบหรือผู้ใช้ระบบ
6. วิเคราะห์ข้อมูลจากผู้ใช้และคำนวณความต้องการใช้ทรัพยากร
7. เปรียบเทียบผลการวิเคราะห์กับการใช้งานทรัพยากรในปัจจุบัน
8. พยากรณ์เวลาที่ทรัพยากรจะเต็มหรือหมดไป
9. เสนอแนวทางจัดการ และติดตามผลอย่างต่อเนื่อง

เมื่อวางแผนศักยภาพเทคโนโลยีสารสนเทศเสร็จแล้วก็จะเป็นการจัดการศักยภาพ (Capacity Management) คือการจัดการให้เทคโนโลยีสารสนเทศของโรงพยาบาลมีศักยภาพตามที่วางแผนไว้นั่นเอง

1.4 การจัดทำแบบประเมินสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

ศักยภาพด้านความสามารถของบุคลากร หรือ สมรรถนะ (Competency) เป็นองค์ประกอบที่สำคัญอันจะทำให้ภารกิจของฝ่ายเทคโนโลยีสารสนเทศสำเร็จลุล่วงตามแผนที่วางไว้ ถ้าบุคลากรมีสมรรถนะไม่เพียงพอ ก็จะต้องส่งบุคลากรไปฝึกฝนหรืออบรมเพิ่มเติมให้มีสมรรถนะเพียงพอที่จะทำงานให้สัมฤทธิ์ผล

ก่อนการประเมินสมรรถนะ ต้องกำหนดรายการสมรรถนะทั้งหมดที่ต้องการให้มีในฝ่ายเทคโนโลยีสารสนเทศเสียก่อน เพื่อให้เกิดความมั่นใจว่าฝ่ายเทคโนโลยีสารสนเทศน่าจะมีสมรรถนะที่ครอบคลุมพันธกิจตามแผนแม่บทเทคโนโลยีสารสนเทศ ดังตัวอย่างต่อไปนี้

สมรรถนะเชิงเทคนิคของฝ่ายเทคโนโลยีสารสนเทศ - Functionally Competency

ฝ่ายเทคโนโลยีสารสนเทศคอมพิวเตอร์ได้กำหนดสมรรถนะเฉพาะตามลักษณะงานที่ปฏิบัติ ดังนี้

- การบริหารจัดการด้านระบบสารสนเทศและชี้นำทิศทางองค์กร
- กำหนดนโยบายและยุทธศาสตร์ระบบสารสนเทศของโรงพยาบาล
- การบริหารแผนงาน/โครงการด้านระบบสารสนเทศ
- การพัฒนาระบบงานสารสนเทศ
- การพัฒนาโปรแกรมประยุกต์
- การใช้เครื่องมือและโปรแกรมระบบงานสารสนเทศ
- การดูแลและบำรุงรักษาระบบข้อมูลสารสนเทศ
- การจัดการระบบความปลอดภัยในระบบเครือข่าย
- ความรู้ด้านสถาปัตยกรรมคอมพิวเตอร์และระบบเครือข่าย
- การบริหารจัดการด้านระบบคอมพิวเตอร์และเครือข่าย
- การใช้เครื่องมือและโปรแกรมระบบงานสารสนเทศ
- การประยุกต์ใช้ข้อมูลสารสนเทศ
- การใช้เทคโนโลยีสารสนเทศ
- การแก้ไขปัญหาและการตัดสินใจ
- ความปลอดภัยในการปฏิบัติงาน
- การให้คำปรึกษา สนับสนุน และการฝึกอบรมการใช้ข้อมูลสารสนเทศ
- การสื่อสารและประสานงาน
- มีจิตบริการและทำงานเป็นทีม
- การแก้ไขปัญหาและการตัดสินใจ

เมื่อกำหนดสมรรถนะรวมในฝ่ายแล้ว ก็ควรกำหนดระดับของสมรรถนะแต่ละเรื่องว่าระดับต้น กลาง สูงของแต่ละสมรรถนะ ควรมีรายลเอียดเป็นอย่างไร ดังตัวอย่างการกำหนดระดับสมรรถนะต่อไปนี้

ชื่อสมรรถนะ : **การให้คำปรึกษา สนับสนุน และการฝึกอบรมการใช้ข้อมูลสารสนเทศ**	
คำจำกัดความ : การให้คำปรึกษา สนับสนุน และการฝึกอบรม ให้แก่ผู้ใช้งานและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ให้มีความรู้ ความสามารถ ความเข้าใจ และสามารถนำไปใช้งานและแก้ไขปัญหาได้	
ความหมายของระดับ	คำอธิบายพฤติกรรม
ระดับ 0	ไม่แสดงสมรรถนะด้านนี้อย่างชัดเจน
ระดับ 1	- สามารถสอบถาม และทบทวนความต้องการ หรือประเด็นปัญหาที่แน่ชัดของผู้ร้องขอ ก่อนการให้คำแนะนำ ปรึกษา - สามารถใช้เอกสารอ้างอิง หรือตัวอย่างประกอบการอธิบาย หรือให้คำแนะนำ - สามารถสอบถามผู้ที่มีประสบการณ ก่อนการตอบคำถามให้กับผู้ร้องขอ - สามารถจัดทำสรุปคำถาม และคำตอบ หรือข้อแนะนำ ที่ใช้บ่อยๆ
ระดับ 2 แสดงสมรรถนะในระดับที่ 1	- สามารถสื่อสารถึงข้อผิดพลาดที่พบบ่อยๆ หรือข้อพึงระวังในการใช้งาน เพื่อป้องกันการเกิดปัญหากับผู้ใช้งาน - สามารถบันทึกพฤติกรรมการใช้งานของผู้ใช้งานที่ทำให้เกิดปัญหา - สามารถเลือกใช้สื่อการสอน หรือสื่อการให้คำปรึกษาที่หลากหลาย ในการถ่ายทอดความรู้
ระดับ 3 แสดงสมรรถนะในระดับที่ 2	- สามารถเน้นย้ำความสำคัญของการดำเนินการของระบบรักษาความมั่นคงและปลอดภัยของการใช้งาน แก่ผู้ปฏิบัติงานและผู้ใช้งาน - สามารถนำเสนอถึงวิธีการแก้ปัญหาที่ช่วยให้ผู้ใช้งาน สามารถทำความเข้าใจและแก้ไขปัญหาเบื้องต้นได้ - สามารถถ่ายทอดเทคนิคใหม่ๆ ให้กับผู้ใช้งาน เพื่อนำไปใช้ประโยชน์มากยิ่งขึ้น
ระดับ 4 แสดงสมรรถนะในระดับที่ 3	- สามารถให้คำปรึกษาและนำเสนอทางเลือกในการพัฒนาระบบงาน แก่หน่วยงานในโรงพยาบาล แก่โครงการที่ได้รับการร้องขอจากหน่วยงานอื่น - สามารถจัดทำคู่มือ หรือเอกสารประกอบการให้คำแนะนำปรึกษาแก่ผู้ปฏิบัติงาน เพื่อใช้ประกอบการถ่ายทอด - จัสามารถดให้เกิดการปรับปรุงหลักสูตร หรือสื่อการ ให้มีความเป็นปัจจุบัน
ระดับ 5 แสดงสมรรถนะในระดับที่ 4	- สามารถจัดกระบวนการในการพัฒนา และสรรหาบุคลากรที่มีความรู้ความสามารถ เพื่อถ่ายทอดความรู้ ให้ตรงกับความต้องการของหน่วยงาน - สามารถจัดให้เกิดการปรับปรุงวิธีการหรือกระบวนการในการถ่ายทอดความรู้ให้สอดคล้องกับสภาพปัญหา ความต้องการของบุคลากร

เมื่อกำหนดระดับสมรรถนะแต่ละเรื่องเสร็จแล้ว ก็ควรวางแผนว่า สมรรถนะต่างๆเหล่านี้ ควรจะอยู่ในบุคลากรคนใด และระดับใดและจัดทำเป็นแบบประเมินสมรรถนะต่อไป ดังตัวอย่างต่อไปนี้

สมรรถนะประจำตำแหน่งงานในฝ่ายเทคโนโลยีสารสนเทศ

1. CIO งานสารสนเทศทางการแพทย์
    a. นายแพทย์
        i. การบริหารจัดการด้านระบบสารสนเทศและชี้นำทิศทางองค์กร
        ii. กำหนดนโยบายและยุทธศาสตร์ระบบสารสนเทศของโรงพยาบาล
        iii. การบริหารแผนงาน/โครงการด้านระบบสารสนเทศ
        iv. การพัฒนาระบบงานสารสนเทศ
2. งานเทคโนโลยีสารสนเทศ
    a. หัวหน้าฝ่าย
        i. การบริหารจัดการด้านระบบสารสนเทศและชี้นำทิศทางองค์กร
        ii. กำหนดนโยบายและยุทธศาสตร์ระบบสารสนเทศของโรงพยาบาล
        iii. การบริหารแผนงาน/โครงการด้านระบบสารสนเทศ
        iv. การพัฒนาระบบงานสารสนเทศ
    b. นักวิชาการคอมพิวเตอร์
        i. การพัฒนาโปรแกรมประยุกต์
        ii. การใช้เครื่องมือและโปรแกรมระบบงานสารสนเทศ
        iii. การดูแลและบำรุงรักษาระบบข้อมูลสารสนเทศ
        iv. การจัดการระบบความปลอดภัยในระบบเครือข่าย
        v. ความรู้ด้านสถาปัตยกรรมคอมพิวเตอร์และระบบเครือข่าย
        vi. การบริหารจัดการด้านระบบคอมพิวเตอร์และเครือข่าย
        vii. มีจิตบริการและทำงานเป็นทีม
    c. เจ้าพนักงานเครื่องคอมพิวเตอร์
        i. การใช้เครื่องมือและโปรแกรมระบบงานสารสนเทศ
        ii. การประยุกต์ใช้ข้อมูลสารสนเทศ
        iii. การให้คำปรึกษา สนับสนุน และการฝึกอบรมการใช้ข้อมูลสารสนเทศ
        iv. มีจิตบริการและทำงานเป็นทีม
        v. การดูแลและซ่อมบำรุงเครื่องคอมพิวเตอร์

vi. บริหารจัดการฐานข้อมูล

vii. การบริหารจัดการเครือข่ายคอมพิวเตอร์

d. พนักงานบริการ

i. การใช้เทคโนโลยีสารสนเทศ

ii. การดูแลและซ่อมบำรุงเครื่องคอมพิวเตอร์

iii. ความปลอดภัยในการปฏิบัติงาน

iv. มีจิตบริการและทำงานเป็นทีม

v. บริหารจัดการฐานข้อมูล

vi. การบริหารจัดการเครือข่ายคอมพิวเตอร์

vii. การพัฒนาโปรแกรมประยุกต์

1.5 การประเมินสมรรถนะรายบุคคล

เมื่อกำหนดรายละเอียดสมรถนะ และกำหนดสมรรถนะที่แต่ละคนต้องมีแล้ว ขั้นตอนสุดท้าย เป็นการจัดทำแบบประเมินสมรรถนะรายบุคคล และนำมาใช้ประเมินสมรรถนะ และสรุปผลดังตัวอย่างต่อไปนี้

การประเมินสมรรถนะรายบุคคล

ชื่อผู้รับการประเมิน : นาย ก. **ตำแหน่ง นักวิชาการคอมพิวเตอร์**

สมรรถนะ	กำหนด	ผลประเมิน
1. การพัฒนาโปรแกรมประยุกต์	5	3
2. ความรู้ด้านสถาปัตยกรรมคอมพิวเตอร์และระบบเครือข่าย	5	2
3. การบริหารจัดการด้านระบบคอมพิวเตอร์และเครือข่าย	5	2
4. การแก้ไขปัญหาและการตัดสินใจ	5	4

1.6 การวางแผนพัฒนาสมรรถนะบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

ผลการประเมินสมรรถนะมักจะชี้ให้เห็นว่า บุคลากรบางคนยังขาดสมรรถนะที่จำเป็นในการทำงานให้สำเร็จ จึงควรวางแผนเพิ่มสมรรถนะรายบุคคล โดยในแผนควรกำหนดรายการสมรรถนะที่ต้องพัฒนา วิธีการ ระยะเวลาและงบประมาณที่ใช้ในการเพิ่มพูนสมรรถนะ ดังตัวอย่างต่อไปนี้

แผนพัฒนาสมรรถนะรายบุคคล

ชื่อ นามสกุล	สมรรถนะที่ต้องพัฒนา	วิธีการ	ระยะเวลา	งบประมาณ
นาย ก	การจัดการระบบเครือข่าย	ฝึกอบรม	3-5 มีนาคม 2561	10,000 บาท
นาย ข	การจัดการ Data Center	ศึกษาดูงาน	4 เมษายน 2561	5,000 บาท0

ระดับที่ 2 การสร้างความแข็งแรงการจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 2 ของการพัฒนา

การยกระดับการจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 2 เป็นการสร้างความแข็งแรงให้กับระบบที่กำเนิดขึ้นมาในระดับที่ 1 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้จริงและทำให้งานดีขึ้น ระดับที่ 2 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

2.1 ทบทวนผลการดำเนินงานในระดับที่ 1

ก่อนที่จะมีการยกระดับการพัฒนา ควรทบทวนผลการดำเนินในระดับที่ 1 โดยใช้หลักการ Plan-Do-Check-Act กล่าวคือ การดำเนินงานในระดับที่ 1 เป็นขั้นตอนของ Plan และ Do เมื่อดำเนินการไปสักระยะหนึ่ง ก็ควร ทบทวนประเมินผล (Check) ก่อนจะที่ยกระดับเป็นระดับที่ 2 (Act) ต่อไปนั่นเอง การประเมินการดำเนินงานที่ผ่านมา จะทำให้เราเห็นโอกาสที่จะปรับปรุงแผนการจัดการศักยภาพและแผนพัฒนาสมรรถนะที่ยังไม่ครอบคลุมรายกาสำคัญ ให้ครอบคลุมและชัดเจนมากขึ้น เพื่อทำให้การดำเนินการตามการจัดการศักยภาพและพัฒนาสมรรถนะมีผลลัพธ์ที่ดีขึ้น ดังนั้น การดำเนินการในระดับที่ 2 จึงเป็นการทำซ้ำการดำเนินการในระดับที่ 1 อีกรอบหนึ่งแต่เป็นการหมุนวงล้อ PDCA ที่ทำให้ระดับคุณภาพสูงขึ้น

อย่างไรก็ตาม การดำเนินการในระดับที่ 2 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการวางแผนจัดการการเปลี่ยนแปลงระบบการทำงาน

2.2 การวางแผนการจัดการการเปลี่ยนแปลงระบบการทำงาน

การวางแผนการจัดการการเปลี่ยนแปลงระบบการทำงาน (Work Process Change Management) เป็นสิ่งที่ต้องทำทุกครั้งที่จะเปลี่ยนวิธีการทำงาน โดยเฉพาะการพัฒนาคุณภาพงานในระบบเทคโนโลยีสารสนเทศ ต้องการการเปลี่ยนแปลงระบบการทำงานเสมอ ตัวอย่างเช่น

- เปลี่ยนระบบการสั่งยาโดยการเขียนใบสั่งยาให้กลายเป็นการสั่งยาในระบบคอมพิวเตอร์
- เปลี่ยนขั้นตอนการชำระเงิน โดยให้ผู้ป่วยไปชำระเงินก่อนตรวจเลือด
- เปลี่ยนวิธีการให้รหัส ICD โดยไม่ให้แพทย์บันทึกรหัส ICD ในห้องตรวจผู้ป่วยนอก แต่ให้แพทย์บันทึกคำวินิจฉัยโรคแทน

การเปลี่ยนแปลงระบบการทำงานเหล่านี้ เป็นการเปลี่ยนวิธีการทำงานของบุคลากรที่เคยชินกับการทำงานแบบเดิมให้ทำแบบใหม่ ย่อมเกิดการต่อต้านของผู้ที่ไม่อยากเปลี่ยนแปลง ดังนั้น จึงควรมีกระบวนการจัดการให้เกิดการเปลี่ยนแปลง โดยมีขั้นตอนที่สำคัญดังต่อไปนี้

1. ประชาสัมพันธ์ให้เข้าใจหลักการ เหตุผล และความสำคัญที่ต้องเกิดการเปลี่ยนแปลง
2. ฝึกอบรมวิธีการใหม่ให้มั่นใจว่าบุคลากรสามารถดำเนินการตามขั้นตอนใหม่ได้
3. สร้างปัจจัยและสิ่งแวดล้อมที่สนับสนุนให้เกิดการเปลี่ยนแปลง เช่น เครื่องมือเพิ่มความสะดวก
4. มีกลไกตรวจสอบว่าเกิดการเปลี่ยนแปลงแล้วอย่างถูกต้อง
5. มีระบบ feedback ทั้งในเชิงบวกและลบเพื่อกระตุ้นให้เกิดการเปลี่ยนแปลงสำเร็จ

ระดับที่ 3 การสร้างความยั่งยืน การจัดการศักยภาพและการเปลี่ยนแปลงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ระดับที่ 3 ของการพัฒนา

การยกระดับการจัดการศักยภาพและการเปลี่ยนเปลงในในระบบเทคโนโลยีสารสนเทศโรงพยาบาลขึ้นสู่ระดับที่ 3 เป็นการสร้างความแข็งแรงให้กับระบบที่พัฒนาจากระดับที่ 1 และ 2 ให้มั่นใจว่าระบบนี้สามารถดำเนินการได้อย่างมั่นคงและยั่งยืน ระดับที่ 3 ประกอบด้วยขั้นตอนที่ควรดำเนินการดังต่อไปนี้

3.1 ทบทวนผลการดำเนินงานในระดับที่ 2

เป็นการหมุนวงล้อ PDCA รอบต่อไปที่ทำให้ระดับคุณภาพสูงขึ้นอีก โดยทบทวนกระบวนการทั้งหมดอย่างเป็นระบบ ปรับปรุงกระบวนการที่สำคัญ ดังต่อไปนี้

- การวิเคราะห์ช่องว่าง
- การจัดการศักยภาพ
- การพัฒนาสมรรถนะบุคลากร
- การจัดการการเปลี่ยนแปลงระบบการทำงาน
- วิเคราะห์ความก้าวหน้าที่ผ่านมา ตั้งแต่ระดับที่ 1 มาระดับที่ 2 และระดับปัจจุบัน ควรแสดงให้การพัฒนาและยกระดับคุณภาพอย่างต่อเนื่อง

นอกจากนั้น การดำเนินการในระดับที่ 3 นี้ ยังมีเรื่องที่ต้องดำเนินการเพิ่มเติม คือการสร้างระบบจัดการการเปลี่ยนแปลง

3.1 การสร้างระบบจัดการการเปลี่ยนแปลง

เมื่อโรงพยาบาลใช้ระบบเทคโนโลยีสารสนเทศไปได้สักระยะหนึ่ง ผู้ใช้งานระบบจะค้นพบว่าระบบเทคโนโลยีสารสนเทศช่วยให้การทำงานสะดวกขึ้น และจะเกิดความต้องการใช้งานเพิ่มเติม นำมาถึงข้อเสนอให้ปรับปรุงและเปลี่ยนแปลงระบบ โรงพยาบาลควรมีระบบจัดการการเปลี่ยนแปลง (IT Project Management) ที่ดี โดยมีวัตถุประสงค์เพื่อให้ได้การเปลี่ยนแปลงที่ดีขึ้น ตรงตามความต้องการ สำเร็จใช้งานได้ทันเวลา ภายในงบประมาณที่กำหนด และไม่ส่งผลกระทบอันไม่พึงปรารถนา

กระบวนการจัดการการเปลี่ยนแปลง ประกอบด้วย กระบวนการต่างๆดังนี้

1. การรับคำร้องขอเปลี่ยนแปลง (Request for Change) โดยผู้ร้องขอการเปลี่ยนแปลงต้องระบุรายละเอียด 7 Rs ดังนี้
   - Who RAISED the change? ใครเสนอการเปลี่ยนแปลง
   - What is the REASON for the change? เหตุผลเป็นอย่างไร
   - What is the RETURN required from the change? จะได้ผลลัพธ์อย่างไร
   - What are the RISKS involved in the change? มีความเสี่ยงอะไรบ้าง
   - What RESOURCES are required to deliver the change? ต้องใช้ทรัพยากรอะไรบ้าง
   - Who is RESPONSIBLE for the build, test and implementation of the change? ใครเป็นผู้พัฒนา ทดสอบ และติดตั้งการเปลี่ยนแปลง
   - What is the RELATIONSHIP between this change and other changes? การเปลี่ยนแปลงครั้งนี้สัมพันธ์อย่างไรกับการเปลี่ยนแปลงอื่น
2. การทบทวนคำร้อง ว่า ซ้ำซ้อนหรือไม่ ขัดแย้งกับคำร้องอื่นหรือไม่
3. ประเมินระดับความสำคัญและความเร่งด่วนของคำร้อง
4. ขออนุมัติการดำเนินการตามคำร้อง

5. ดำเนินการเปลี่ยนแปลง
6. ติดตั้งส่วนที่เปลี่ยนแปลง
7. ประเมินผลการเปลี่ยนแปลง
8. สรุปและบันทึกบทเรียนการเปลี่ยนแปลง

ผู้ที่มีบทบาทหน้าที่ในการจัดการการเปลี่ยนแปลง ประกอบด้วย ผู้จัดการการเปลี่ยนแปลง (Change Manager) รับผิดชอบ บริหารการเปลี่ยนแปลงทั้งหมด โดยทำงานร่วมกับ คณะกรรมการกำกับการเปลี่ยนแปลง (Change Advisory Board – CAB) มีตัวชี้วัดที่สำคัญในการประเมินการจัดการการเปลี่ยนแปลง เช่น

- จำนวนคำร้องขอการเปลี่ยนแปลง แบบธรรมดา และ เร่งด่วน
- จำนวนการเปลี่ยนแปลงที่เกิดขึ้น
- ผลกระทบต่อคุณภาพการบริการ
- จำนวนคำร้องที่ค้างอยู่ในระบบ ระยะเวลาที่รอดำเนินการ
- ฯ ล ฯ