รายงานการศึกษา ฝึกอบรม ประชุม ดูงาน สัมมนา ปฏิบัติการวิจัย ในประเทศ และต่างประเทศ
(ระยะสั้นไม่เกิน ๙๐ วัน และ ระยะยาวตั้งแต่ ๙๐ วันขึ้นไป)

ส่วนที่ ๑ ข้อมูลทั่วไป

๑.๑ ชื่อ – นามสกุล นายณัฐภาส สาตรจำเริญ
อายุ ๒๘ ปี การศึกษา ปริญญาตรี
สาขา วิศวกรรมกรรมศาสตร์อิเล็กทรอนิกส์และระบบคอมพิวเตอร์
ความเชี่ยวชาญเฉพาะด้าน คอมพิวเตอร์
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หน้าที่ความรับผิดชอบ ดูแล ติดตั้ง ระบบคอมพิวเตอร์ให้พร้อมใช้งานทั้งด้าน Hardware Software รวมทั้งการจัดทำแผนระบบงานไอทีให้เป็นไปตามมาตรฐาน

๑.๒ ชื่อ - นามสกุล นายพีรวัฒน์ มะนาวหวาน
อายุ ๒๙ ปี การศึกษา ปริญญาตรี
สาขาวิชาวิทยาศาสตร์บัณฑิต (เทคนิคการแพทย์)
ความเชี่ยวชาญเฉพาะด้าน -
ตำแหน่ง นักเทคนิคการแพทย์ปฏิบัติการ
หน้าที่ความรับผิดชอบ รายงานผลตรวจทางห้องปฏิบัติการ ผ่านระบบสารสนเทศ ตรวจสอบผลการควบคุมคุณภาพในห้องปฏิบัติการผ่านระบบสารสนเทศ

๑.๓ ชื่อเรื่อง / หลักสูตร HA ๖๐๙ การบริหารระบบสารสนเทศในโรงพยาบาล (Hospital Information Management) รุ่นที่ ๒
สาขา.....
เพื่อ ☐ ศึกษา ☑ ฝึกอบรม ☐ ประชุม ☐ ดูงาน ☐ สัมมนา ☐ ปฏิบัติการวิจัย
งบประมาณ ☐ เงินงบประมาณกรุงเทพมหานคร ☑ เงินบำรุงโรงพยาบาล
☐ ทุนส่วนตัว ☐ ไม่มีค่าใช้จ่าย
จำนวนเงินคนละ ๔,๕๐๐ บาท รวมทั้งสิ้น ๙,๐๐๐ บาท
ระหว่างวันที่ ๒๔ – ๒๖ พฤษภาคม ๒๕๖๖
สถานที่ โรงแรมอัศวิน แกรนด์ คอนเวนชั่น กรุงเทพ
คุณวุฒิ/วุฒิบัตรที่ได้รับ ใบประกาศนียบัตร

ส่วนที่ ๒ ข้อมูลที่ได้รับจากการศึกษา ฝึกอบรม ประชุม ดูงาน สัมมนา ปฏิบัติการวิจัย
(โปรดให้ข้อมูลในเชิงวิชาการ)

๒.๑ วัตถุประสงค์ เพื่อเตรียมความพร้อมในการประเมินด้านเทคโนโลยีสารสนเทศให้นำไปใช้ในโรงพยาบาลผู้สูงอายุบางขุนเทียนรวมทั้งกำหนดมาตรฐานสารสนเทศให้ตรงตามมาตรฐานที่กำหนด

๒.๒ เนื้อหา

ผลการฝึกอบรมหลักสูตรการบริหารระบบสารสนเทศในโรงพยาบาล (HA๖๐๙) วันแรกในช่วงเช้าในหัวข้อแรกแนวคิดการพัฒนาและมาตรฐานที่เกี่ยวข้องกับระบบสารสนเทศในโรงพยาบาล อธิบายเกี่ยวกับ HA เบื้องต้นเช่น ๓ P: Basic Building Block of Quality , แนวคิด ๓C-PDSA/DAL , ๒P Safety

Goals ,มาตรฐานสำคัญจำเป็นต่อความปลอดภัย,แนวทางการกำหนดระดับคะแนน Scoring Guideline โดยนำมาประยุกต์ใช้เกี่ยวกับระบบสารสนเทศและเทคโนโลยีสารสนเทศ

ซึ่งความสำคัญของการพัฒนาระบบสารสนเทศในโรงพยาบาลเป็นการนำระบบสารสนเทศและเทคโนโลยีสารสนเทศ มาประยุกต์ใช้ในกิจการต่างๆ ของโรงพยาบาล โดยมีวัตถุประสงค์เพื่อให้สามารถดำเนินการต่างๆ ได้อย่างรวดเร็ว ถูกต้องตรงตามเป้าหมายหลักของโรงพยาบาล ลดความซ้ำซ้อนในการทำงาน พร้อมทั้งสนับสนุนการตัดสินใจได้อย่างถูกต้องในทุกขั้นตอน ก่อให้เกิดการใช้ทรัพยากรอย่างเกิดประโยชน์สูงสุด

ซึ่งนิยามศัพท์ในหัวข้อแนวคิดการพัฒนาและมาตรฐานที่เกี่ยวข้องกับระบบสารสนเทศในโรงพยาบาลมีดังนี้

๒.๒.๑. นิยามศัพท์ของความหมายระบบสารสนเทศและเทคโนโลยีแบ่งออกเป็นดังนี้

๑. ข้อมูล (Data) คือ ข้อเท็จจริงที่ได้จากการรวบรวมข้อมูล ซึ่งมีทั้งที่อยู่ในรูปแบบตัวอักษร, ข้อความตัวเลข, เสียง รูปภาพ และ ภาพเคลื่อนไหว

๒. สารสนเทศ (Information) คือ ข้อมูลที่ผ่านการประมวลผล เพื่อนำไปใช้ในการตัดสินใจ เช่น อัตราป่วยของโรคไข้เลือดออก, ระยะเวลารอคอยเฉลี่ย, อัตราการเสียชีวิต เป็นต้น

๓. ระบบสารสนเทศ (Information System) คือ การจัดการข้อมูลตั้งแต่การรวบรวมและตรวจสอบข้อมูล การประมวลผลข้อมูล รวมถึงการดูแลรักษาข้อมูลเพื่อให้ได้สารสนเทศที่ถูกต้องและทันต่อความต้องการของผู้ใช้และผู้ใช้สามารถนำสารสนเทศที่ได้ไปประกอบการตัดสินใจได้อย่างมีประสิทธิภาพ

๔. ระบบเทคโนโลยีสารสนเทศ (Information Technology) การนำความรู้ทางด้านวิทยาศาสตร์มาประยุกต์ใช้เพื่อสร้างหรือจัดการสารสนเทศอย่างเป็นระบบและรวดเร็ว โดยอาศัยเทคโนโลยีทางด้านคอมพิวเตอร์

๒.๒.๒. นิยามศัพท์ประเภทของระบบสารสนเทศแบ่งออกเป็นดังนี้

๑. ระบบประมวลผลรายการ (Transaction Processing Systems – TPS)

คือ ระบบที่ใช้สนับสนุนการปฏิบัติงาน/การให้บริการเพื่อความสะดวกรวดเร็ว ลดขั้นตอน

๒. ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems- MIS)

คือ ระบบสารสนเทศที่จะช่วยในการบริหารจัดการ มีการรวมสารสนเทศภายในและภายนอกที่เกี่ยวข้องกับองค์กรทั้งในอดีตและปัจจุบัน เพื่อให้ผู้บริหารสามารถตัดสินใจในการวางแผนการควบคุม และการปฏิบัติการขององค์กรได้อย่าง ถูกต้อง

๓. ระบบสนับสนุนการตัดสินใจ (Decision Support Systems – DSS)

คือ เป็นระบบที่สนับสนุนความต้องการเฉพาะของผู้บริหารแต่ละคน (made by order) ในหลาย ๆ สถานะการณ์ ระบบนี้มีหน้าที่ช่วยให้การตัดสินใจเป็นไปได้อย่างสะดวก

๔. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information System – EIS)

คือ เพื่อสนับสนุนสารสนเทศและการตัดสินใจสำหรับผู้บริหารระดับสูงโดยเฉพาะรวมทั้งการทำมาตรฐานเทคโนโลยีสารสนเทศในโรงพยาบาล (Hospital Accreditation Information Technology: HAIT) ซึ่งประกอบไปด้วย การจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ การจัดการความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ การจัดระบบบริการในระบบเทคโนโลยีสารสนเทศ การควบคุมคุณภาพ ข้อมูลในระบบเทคโนโลยีสารสนเทศ การควบคุมคุณภาพการพัฒนาโปรแกรมที่ใช้ในโรงพยาบาล การจัดการศักยภาพและการจัดการเปลี่ยนแปลงใน ระบบเทคโนโลยีสารสนเทศโรงพยาบาล เป็นต้น

"ประเด็นที่พบจากการเยี่ยมสำรวจระบบสารสนเทศในโรงพยาบาล" โดยแบ่งออกเป็นหัวข้อดังนี้

๑. บทบาทของคณะกรรมการสารสนเทศซึ่งได้อธิบายปัญหาส่วนใหญ่ที่เกิดขึ้นในโรงพยาบาลดังนี้

- โครงสร้างคณะกรรมการไม่ชัดเจน/เป็นคณะกรรมการเฉพาะกิจ
- การกำหนดบทบาทคณะกรรมไม่ชัดเจน
- ขาดการกำหนดนโยบาย เป้าหมายของคณะกรรมการ หรือกำหนดไม่ชัดเจน
- การกำหนดตัวชี้วัดเพื่อประเมินประสิทธิภาพ/ผลการดำเนินงานไม่ชัดเจน
- การควบคุม กำกับ ติดตามการปฏิบัติตามนโยบาย เป้าหมาย ตัวชี้วัดยังไม่ชัดเจน
- ขาดการวางแผนการพัฒนาระบบเทคโนโลยีสารสนเทศที่ชัดเจน (IT Master plan)
- เน้นการพัฒนาด้าน IT แต่ยังไม่เน้น IM

๒. ปัญหาส่วนใหญ่ที่เกิดขึ้นเกี่ยวกับการจัดการเทคโนโลยีสารสนเทศในโรงพยาบาลดังนี้

- ระบบ Network infrastructure ไม่เหมาะสม เช่น สาย Lan การจัดการสายไม่เรียบร้อย
- Hardware ไม่ทันสมัย และ ไม่เพียงพอ
- มีการใช้ Software ที่หลากหลาย ขาดการติดตามประเมินผล
- ห้องจัดเก็บ Server หรือ Data Center ไม่ได้มาตรฐาน
- ระบบการสำรองข้อมูลแบบ Real Time ขาดการ Backup แบบ Offline
- แผนการปฏิบัติเมื่อระบบล่ม (BCP) และแผนกู้คืนระบบ (DRP) ไม่ชัดเจน ขาดการฝึกซ้อม
- ขาดแผนและรายงานผลการตรวจติดตามความมั่นคงของระบบ

๓. ปัญหาของผู้ใช้ระบบเทคโนโลยีสารสนเทศมีดังนี้

- ใช้งานระบบ HIS ใช้ได้ไม่สะดวก
- มีการทำงานซ้ำซ้อน มีการบันทึกทั้งในรูปแบบของกระดาษ และในระบบ HIS
- มีการร้องขอให้ Admin เข้าไปแก้ไขโปรแกรมให้บ่อยๆ (แต่ Admin ไม่สามารถแก้ไขได้)
- ไม่รู้ว่าระบบ HIS มี Function นี้ไว้ใช้งาน
- ไม่เชื่อถือข้อมูลที่บันทึกเข้าไปในระบบ HIS

๔. ปัญหาของผู้ดูแลระบบเทคโนโลยีสารสนเทศส่วนใหญ่มีดังนี้

- ผู้ดูแลระบบส่วนใหญ่พูดภาษา Digital ทำให้ User ฟังไม่รู้เรื่อง
- ต้องทำหน้าที่หลายหลากมากจนเกินไปเช่น (พิมพ์งาน, ถ่ายรูป, ทำ PowerPoint)
- การปรับปรุง แก้ไข ปัญหาที่เจอจาก HIS ของ Admin ต้องใช้ระยะเวลานาน
- การติดตามนโยบายต่างๆ ที่วางไว้ไม่สม่ำเสมอ
- การสื่อสารระหว่าง Admin กับ User น้อย
- การค้นหาความต้องการใช้ระบบสารสนเทศแบบเชิงรุกน้อย
- การดึงศักยภาพของระบบ HIS ออกมาใช้งานยังไม่มากพอ
- มีปัญหาทุกครั้งที่การตรวจประเมินจากเจ้าหน้าที่ภายนอก

๕. ปัญหาเกี่ยวกับการรักษาความลับและความปลอดภัยในโรงพยาบาลดังนี้

- นโยบายด้านความมั่นคงความปลอดภัยของสารสนเทศที่ขาดความชัดเจน และขาดการติดตามประเมินผล
- การป้องกันการโจมตีจากภายนอก, การป้องกันไวรัส
- ขาดการตั้งค่าระบบงานสำคัญให้บันทึกเหตุการณ์ (LOG) การเข้าใช้งานไม่น้อยกว่า ๙๐ วัน

- การกำหนดเข้าถึงตามสิทธิ (ทั้งการเข้าถึงทางกายภาพและการเข้าถึงทางอิเล็กทรอนิกส์)
- การกำหนดและการปรับเปลี่ยนรหัสเข้าใช้งาน (Password)
- การรักษาความลับข้อมูลผู้ป่วยในกลุ่มอ่อนไหว เช่น HIV, OSCC, ยาเสพติด เป็นต้น

"ความรู้ ความเข้าใจ PDPA และบทบัญญัติในการคุ้มครองข้อมูลกับสถานการณ์ที่เผชิญในภาคการดูแลสุขภาพ"

ความสำคัญของข้อมูลส่วนบุคคล ถือเป็นสิ่งที่สำคัญอย่างยิ่ง เนื่องจากข้อมูลส่วนนี้สามารถนำไปประมวลผลได้หลากหลายรูปแบบ ไม่ว่าจะเป็นการนำข้อมูลไปวิเคราะห์เพื่อปรับปรุงเว็บไซต์ ให้เข้ากับความต้องการของผู้ใช้งาน หรือเพิ่มความน่าสนใจให้กับการใช้งานนั้นๆ นอกจากนี้แล้ว ข้อมูลส่วนบุคคลยังสามารถนำไปใช้ในทางที่ก่อให้เกิดความเสียหายกับตัวบุคคล

ทั้งนี้ ความสำคัญของ PDPA คือการทำให้เจ้าของข้อมูลมีสิทธิในข้อมูลส่วนตัวที่ถูกจัดเก็บไปแล้วหรือกำลังจะถูกจัดเก็บมากขึ้น เพื่อสร้างความปลอดภัยและเป็นส่วนตัวให้แก่เจ้าของข้อมูล โดยมีสิทธิที่สำคัญ คือ สิทธิการรับทราบและยินยอมการเก็บข้อมูลส่วนตัว และสิทธิในการขอเข้าถึงข้อมูลส่วนตัว คัดค้านและเพิกถอนการเก็บและนำข้อมูลไปใช้ และสิทธิขอให้ลบหรือทำลายข้อมูลส่วนตัว

วัตถุประสงค์การคุ้มครองข้อมูลส่วนบุคคล

๑. เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพโดยกำหนดและความรับผิดชอบที่เหมาะสม
๒. เพื่อให้มีมาตรการเยียวยาจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ
๓. เพื่อส่งเสริมการใช้ข้อมูลในการพัฒนานวัตกรรมอย่างมั่งคงปลอดภัย
๔. เพื่อสร้างความโปร่งใสและเป็นธรรมในการใช้ข้อมูลส่วนบุคคล

เหตุผลในการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น

เพื่อกำหนดหลักเกณฑ์ > กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้ สำหรับหมวดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ แบ่งออกเป็น ๗ หมวด ดังนี้

- การบังคับถัดจากวันประกาศในราชกิจจานุเบกสา (๒๕ พ.ค. ๒๕๖๒) ประกอบไปด้วย
- หมวดที่ ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวดที่ ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การบังคับเมื่อครบ ๑ ปีนับจากวันประกาศในราชกิจจานุเบกษา (ตั้งแต่ ๒๕ พ.ค. ๒๕๖๓ แต่เลื่อนเป็นวันที่ ๑ มิ.ย. ๒๕๖๕)

- หมวดที่ ๒ การคุ้มครองข้อมูลส่วนบุคคล
- หมวดที่ ๒ สิทธิของเจ้าของข้อมูลส่วนบุคคล
- หมวดที่ ๕ การร้องเรียน
- หมวดที่ ๖ ความรับผิดทางเพ่ง
- หมวดที่ ๗ บทกำหนดโทษ

ขอบเขตการบังคับใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

- ใช้บังคับแก่การเก็บรบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร

- มีผลใช้บังคับถึง กรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมีกิจกรรม ดังนี้

๑) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่

๒) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักรประเภทของข้อมูลส่วนบุคคล

๑. ข้อมูลส่วนบุคคลทั่วไป (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งข้อมูลในรูปแบบออนไลน์หรือออฟไลน์ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล เลขบัตรประชาชน เลขที่บัญชีธนาคาร เป็นต้น

๒.ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เป็นข้อมูลที่เฉพาะเจาะจงของบุคคล มีความละเอียดอ่อนสูง เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติ อาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นในทำนองเดียวกัน

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลประกอบด้วยดังนี้

เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้ ซึ่งสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ประกอบไปด้วย สิทธิที่ได้รับแจ้งให้ทราบ สิทธิในการแก้ไขข้อมูล สิทธิในการเพิกถอนความยินยอม สิทธิในการขอระงับการใช้ข้อมูล สิทธิในการขอเข้าถึงข้อมูล สิทธิในการขอรับ และให้โอนย้ายข้อมูล

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งมีหน้าหน้าที่ดังนี้

๑. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
๒. ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
๓. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
๔. แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
๕. การแต่งตั้งตัวแทนภายในราชอาณาจักร
๖. การจัดทำบันทึกรายการ

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคล หรือ นิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมีหน้าหน้าที่ ดังนี้

๑. ดำเนินการตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย หรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๒. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมรวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึง เหตุการณ์ ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๓. จัดทำและจัดเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

๔. แต่งตั้งตัวแทนภายในราชอาณาจักร

๕. ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล

ความยินยอม(Consent) เหตุผลความยินยอมจะต้องมีกรณีดังนี้

๑. ต้องได้รับความยินยอมก่อน จึงจะสามารถใช้เก็บข้อมูลรวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลโดยจะขอความยินยอมทีหลัง หรือขอย้อนหลังไม่ได้

๒. ต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์

๓. ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

๔. ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง

๕. มีความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (freely given)

๖. ถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในส่วนกรณีความยินยอมของผู้เยาว์ คนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ ประกอบด้วยดังนี้

๑. ผู้เยาว์ที่มีอายุไม่เกิน ๑๐ ปี ให้ขอความยินยอมจากผู้ปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

๒. ผู้เยาว์ที่ยังไม่บรรลุนิติภาวะสามารถให้ความยินยอมโดยลำพังได้ หากเข้าข่ายตามมาตราที่ ๒๒, ๒๓ และ ๒๔ ของประมวลกฎหมายแพ่งและพาณิชย์ (อันว่าด้วยเรื่องการใด ๆ ที่ ผู้เยาว์สามารถกระทำเองโดยลำพัง) นอกเหนือจากนั้น ให้ขอความยินยอมจากผู้ปกครองที่ มีอำนาจกระทำการแทนผู้เยาว์ประกอบด้วย

๓. คนไร้ความสามารถให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

๔. คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ประกอบไปด้วย

๑. Explicit consent การได้รับการยินยอมโดยชัดแจ้ง

๒. Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓. Social Protection& Non-Profit การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร

๔. Manifestly Made Public เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๕. Legal Claims เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๖. Legal Obligations เป็นเรื่องที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

- เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์

- ประโยชน์ด้านสาธารณะสุข, การคุ้มครองแรงงาน, การประกันสังคม, หลักประกันสุขภาพแห่งชาติ
- การศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์, สถิติ, หรือประโยชน์สาธารณะอื่น
- ประโยชน์สาธารณะที่สำคัญ

การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นจะต้องห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจาก แหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

- ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ คือประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่

- เป็นการปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- จำเป็นเพื่อการปฏิบัติตามสัญญา
- กระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น
- ป้องกันหรือระงับอันตรายต่อ ชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น
- จำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ

บทลงโทษตาม PDPA ประกอบไปด้วย

๑) โทษทางแพ่งคือค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

๒) โทษทางอาญา

๒.๑ ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย

- ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุก ไม่เกิน ๖ เดือน หรือ ปรับไม่เกิน ๕๐๐,๐๐๐ บาท
- เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุกไม่เกิน ๑ ปี หรือ ปรับไม่เกิน ๕๐๐,๐๐๐ บาท

๒.๒ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตามพระราชบัญญัตินี้ห้ามนำไปเปิดเผยแก่ผู้อื่น เว้นแต่เปิดเผยตามหน้าที่ หรือเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี หรือได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือเปิดเผยให้หน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือข้อมูลคดีต่างๆ ที่เปิดเผยต่อสาธารณะจำคุกไม่เกิน ๖ เดือน หรือ ปรับไม่เกิน ๕๐๐,๐๐๐ บาท

๒.๓ ผู้กระทำความผิดที่เป็นนิติบุคคล หากกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่ง รับผิดชอบในการดำเนินงานของนิติบุคคลนั้น สั่งการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคล นั้นกระทำความผิด ต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย

๓. โทษทางปกครอง

๓.๑ ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของ DPO โทษปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท

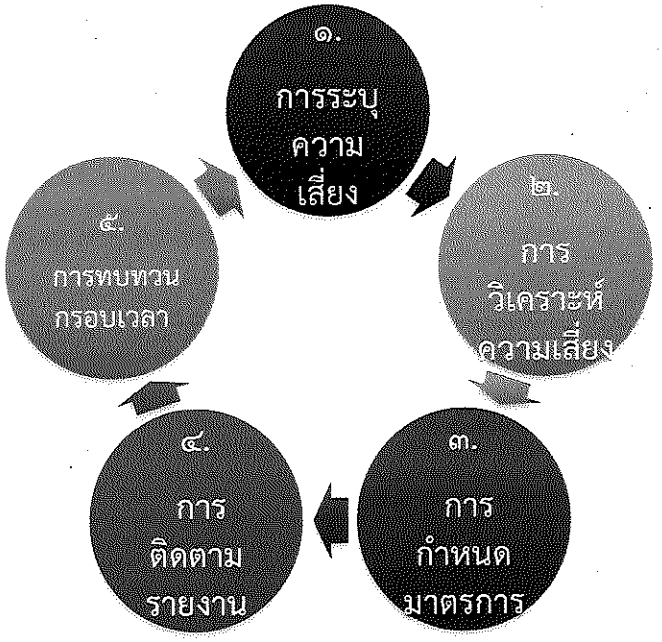
๓.๒ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจำเป็นขอความยินยอมที่เป็นการหลอกลวงให้เข้าใจผิด ไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่แจ้งเหตุเมื่อมีการละเมิดข้อมูล โอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย ไม่ตั้งตัวแทนในราชอาณาจักร โทษปรับไม่เกิน ๓,๐๐๐,๐๐๐ บาท

๓.๓ เก็บรวบรวม ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย โทษปรับไม่เกิน ๕,๐๐๐,๐๐๐ บาท

๒.๒.๓ "การวิเคราะห์และจัดการความเสี่ยงในระบบสารสนเทศ"

ความเสี่ยงของระบบฐานข้อมูลสารสนเทศ หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าหรือเหตุการณ์ซึ่งไม่พึงประสงค์ ที่ทำให้งานไม่ประสบความสำเร็จตาม วัตถุประสงค์และเป้าหมายที่กำหนด

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



รูปที่ ๒.๒.๓.๑ แสดงกระบวนการบริหารความเสี่ยง

๒.๒.๓.๑. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ กับ กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒. การใช้ Checklist

๓. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๔. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๕. การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

๒.๒.๓.๒. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๑. การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง

๓. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง

๔. การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดย พิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๒.๒.๓.๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๑. ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๒. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓. การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔. การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่

๒.๒.๓.๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้ว ให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก

๒.๒.๓.๕. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๒.๓ ประโยชน์ที่ได้รับ

๒.๓.๑ ☐ ต่อตนเอง ได้ความรู้เรื่องการใช้ระบบงานเทคโนโลยีสารสนเทศ รวมทั้งมาตรฐานที่เกี่ยวข้องของเทคโนโลยีสารสนเทศ กฎหมายที่เกี่ยวข้อง รวมทั้งได้ความรู้วิธีป้องกันจัดความเสี่ยงเบื้องต้น

๒.๓.๒ ☐ ต่อหน่วยงาน ยกระดับความเชื่อมั่นขององค์กรทั้งมาตรฐานการจัดเก็บข้อมูลส่วนบุคคล มาตรฐานการเข้าถึงระบบสารสนเทศ มาตรฐานการจัดทำแผนแม่บทสารสนเทศ ทำให้ไปทิศทางเดียวกัน และเป็นหน่วยงานที่โปร่งใสตรวจสอบได้

๒.๓.๓ ☐ อื่น ๆ

ส่วนที่ ๓ ปัญหาและอุปสรรค

๓.๑ ☐ การปรับปรุง เนื่องจากสถานที่อบรมค่อนข้างไกล

๓.๒ ☐ การพัฒนา

๓.๒.๑ นำไปพัฒนาด้านมาตรฐาน HAIT เพื่อให้รองรับความเชื่อมั่นการให้บริการด้านสารสนเทศ พร้อมกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓.๒.๒ จัดทำแผนแม่บทด้านสารสนเทศ และแผนความเสี่ยงเพื่อประเมินและป้องกันเหตุที่เกิดรวมทั้งตรวจพร้อมกับเหตุการณ์ที่เกิดขึ้น

๓.๒.๓ ทำระบบรักษาความปลอดภัยทั้งด้านกายภาพและด้านอิเล็กทรอนิกส์เกี่ยวกับข้อมูลของคนไข้เพื่อรองรับเตรียมพร้อมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

ส่วนที่ ๔ ข้อคิดเห็นและข้อเสนอแนะ -

ลงชื่อ..ผู้รายงาน
(นายณัฐภาส สาตรจำเริญ)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ลงชื่อ..ผู้รายงาน
(นายพีรวัฒน์ มะนาวหวาน)
นักเทคนิคการแพทย์ปฏิบัติการ

ส่วนที่ ๕ ความคิดเห็นของผู้บังคับบัญชา

- เป็นองค์ความรู้ที่ดี และมีประโยชน์
- เห็นควรให้เผยแพร่องค์ความรู้ [illegible] ไป [illegible] และเผยแพร่ [illegible] [illegible] [illegible] และ [illegible]

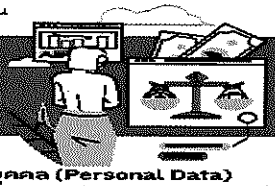
ลงชื่อ..หัวหน้าส่วนราชการ
(นายสุรินทร์ นัมคณิสรณ์)
ผู้อำนวยการโรงพยาบาลผู้สูงอายุบางขุนเทียน

PDPA

พระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562

ความสำคัญของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลถือเป็นสิ่งที่สำคัญอย่างยิ่ง เนื่องจากข้อมูลส่วนนี้สามารถนำประมวลผลได้หลากหลายรูปแบบไม่ว่าจะเป็นการนำข้อมูลไปวิเคราะห์เพื่อปรับปรุงให้เข้ากับความต้องการของผู้ใช้งานนอกจากนี้แล้ว ข้อมูลส่วนบุคคลยังสามารถนำไปใช้ในทางที่ก่อให้เกิดความเสียหายกับตัวเจ้าของ ดังนั้นโรงพยาบาลถือเป็นศูนย์กลางของข้อมูลขนาดใหญ่ที่เก็บข้อมูลส่วนบุคคลของคนไข้ที่เข้ารับบริการและยังจัดเก็บข้อมูลอ่อนไหว (Sensitive Personal Data) ไว้จำนวนมาก อาทิ การทำประวัติคนไข้หรือเวชระเบียน การใช้ประวัติการรักษาพยาบาล การเก็บข้อมูลกรุ๊ปเลือด ประวัติการใช้ยา ประวัติการผ่าตัด ข้อมูลเกี่ยวกับประกันสุขภาพ เป็นต้น



ข้อมูลส่วนบุคคล (Personal Data)

คือข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่รวมข้อมูลนิติบุคคลและข้อมูลของผู้ที่เสียชีวิตไปแล้ว เช่น เลขประจำตัวประชาชน ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ E-mail ข้อมูลทางการเงิน ข้อมูลอุปกรณ์หรือเครื่องมือ

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

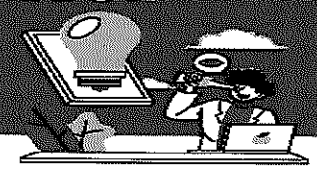
คือข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในศักดิ์ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลทางชีวมิติ (Biometric)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

1. สิทธิที่ได้รับแจ้งให้ทราบ
2. สิทธิในการแก้ไขข้อมูล
3. สิทธิในการเพิกถอนความยินยอม
4. สิทธิในการขอระงับการใช้ข้อมูล
5. สิทธิในการขอเข้าถึงข้อมูล
6. สิทธิในการขอรับและให้โอนย้ายข้อมูล
7. สิทธิคัดค้านการประมวลผลข้อมูล
8. สิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล
9. สิทธิในการร้องเรียน

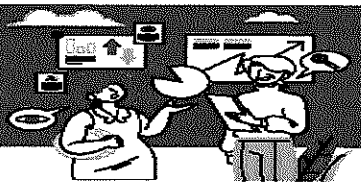
การนำประโยชน์ไปใช้ในหน่วยงานและโรงพยาบาล

- ยกระดับการป้องกันข้อมูลส่วนบุคคลอย่างมีมาตรฐาน ไม่ให้รั่วไหลออกนอกโรงพยาบาลทั้งด้านเอกสารและด้านดิจิตอล
- เจ้าหน้าที่และผู้ป่วยมีสิทธิรับทราบวัตถุประสงค์ของการให้ข้อมูลก่อนตัดสินใจให้ข้อมูล



พระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562 ประกอบด้วย

- หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล
- หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล
- หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด 5 การร้องเรียน
- หมวด 6 ความรับผิดทางแพ่ง
- หมวด 7 บทกำหนดโทษ



บุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

บทลงโทษ PDPA

โทษทางแพ่ง

ค่าสินไหมทดแทนจากความเสียหายที่ได้รับแจ้ง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

โทษทางอาญา

ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดวัตถุประสงค์ หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบกฎหมาย

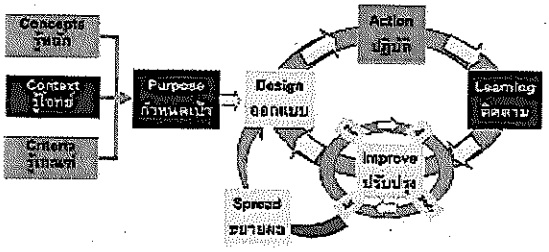
- ทำให้ผู้อื่นเกิดได้รับความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอายจำคุก <= 6 เดือน ปรับ <= 500,000 บาท
- เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุก <= 1 ปีหรือ ปรับ <= 500,000 บาท

โทษทางปกครอง

- ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้ข้อมูลทราบโทษปรับไม่เกิน 1,000,000 บาท
- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจำเป็นไม่มีมีการแจ้งเหตุเมื่อเกิดการละเมิดข้อมูล โอนไปต่างประเทศโดยมิชอบกฎหมาย โทษปรับไม่เกิน 3,000,000 บาท
- เก็บรวบใช้เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบกฎหมาย โทษปรับไม่เกิน 5,000,000 บาท

จัดทำโดย นายณัฐกาส สาตรจำเริญ
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
โรงพยาบาลผู้สูงอายุบางบุนเทียน

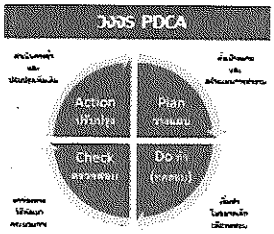
การบริหารระบบสารสนเทศในโรงพยาบาล



มาตรฐานที่เกี่ยวข้องกับการจัดการระบบสารสนเทศ

มาตรฐาน ISO 27001: 2013 ระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

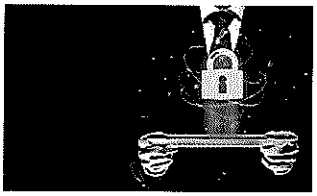
ประยุกต์ใช้หลักการ PDCA : วงจรบริหารงานคุณภาพ (วางแผน-ปฏิบัติ-ตรวจสอบ-ปรับปรุง)



กฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่ 2) พ.ศ.2560

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562



การวิเคราะห์และจัดการความเสี่ยงในระบบสารสนเทศ

เพื่อให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ

เพื่อป้องกันหรือลดผลที่ไม่พึงปรารถนา

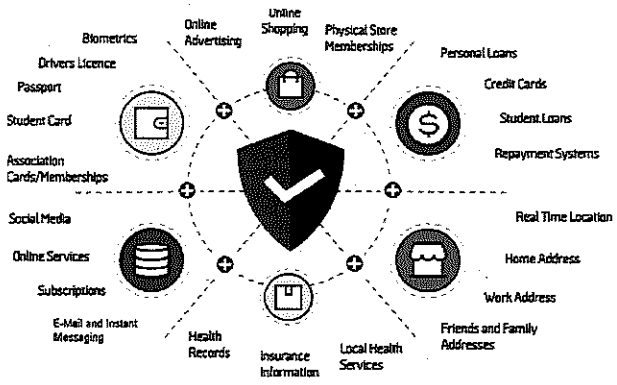
สามารถบรรลุการปรับปรุงอย่างต่อเนื่อง

การจัดการข้อมูลส่วนบุคคลสำหรับสถานพยาบาล

การเก็บรวบรวมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้

วัตถุประสงค์ของการเก็บรวบรวม
ระยะเวลาในการเก็บรวบรวม
การเปิดเผยข้อมูลส่วนบุคคล
ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
สิทธิของเจ้าของข้อมูลส่วนบุคคล



การนำไปประยุกต์ใช้กับหน่วยงาน

ได้รับความรู้เกี่ยวกับมาตรฐานของการจัดการระบบสารสนเทศ และสามารถนำมาวางแผน ออกแบบและตรวจติดตาม ระบบบริหารคุณภาพของหน่วยงานได้ครอบคลุมมากยิ่งขึ้น

นายพีรวัฒน์ มะนาวหวาน นักเทคนิคการแพทย์ปฏิบัติการ
โรงพยาบาลผู้สูงอายุบางขุนเทียน