ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่
เรื่อง นโยบายธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่
(Data Governance Policy Faculty of Medicine Chiang Mai University)

****

หลักการ

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้ตระหนักถึงความสำคัญในเรื่องการดูแลและการบริหารจัดการข้อมูล อีกทั้งจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act: PDPA) และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ที่ประกาศในราชกิจจานุเบกษาเมื่อวันที่ ๒๒ พฤษภาคม พ.ศ. ๒๕๖๒ ได้กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลให้มีความสอดคล้องเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่มีหลายส่วนงานที่มีการใช้ข้อมูลทั้งทางด้านการบริการด้านการแพทย์ ด้านการเรียนการสอนของนักศึกษา และด้านงานวิจัย จึงจำเป็นต้องกำหนดให้มีธรรมาภิบาลข้อมูล เพื่อเป็นหลักการและแนวทางในการดำเนินการให้เป็นไปตามพระราชบัญญัติดังกล่าว อันจะนำไปสู่การพัฒนาระบบข้อมูลที่สำคัญ เพื่อประโยชน์ในการกำหนดหลักเกณฑ์ ระบุวัตถุประสงค์และวิธีการเชื่อมโยง แลกเปลี่ยน ฐานการประมวลผลข้อมูล และบูรณาการข้อมูลของหน่วยงานอย่างเป็นระบบ ประกาศเป็นแนวปฏิบัติให้สอดคล้องกับนโยบายของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

เพื่อให้การดำเนินการยกระดับและพัฒนามาตรฐานการบริหารจัดการและการบูรณาการข้อมูลเป็นไปตามนโยบายและกฎหมายที่เป็นปัจจุบันในระดับประเทศ และในระดับสากลที่เกี่ยวข้องจึงประกาศนโยบายธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ (Data Governance Policy for Faculty of Medicine Chiang Mai University) ตามเอกสารแนบท้ายประกาศ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศนโยบายธรรมาภิบาลข้อมูล”

ข้อ ๒ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ มีนโยบายกำหนดให้ผู้ปฏิบัติงานในคณะแพทยศาสตร์ที่มีการดำเนินการเกี่ยวข้องกับการเก็บ ใช้ และเผยแพร่หรือเปิดเผยข้อมูลให้ถูกต้องตามกฎหมาย กฎระเบียบหลักวิชาการและมาตรฐานสากล

ข้อ ๓ ในประกาศนี้

“ธรรมาภิบาลข้อมูล” (Data Governance) หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลไปใช้เป็นไปอย่างถูกต้อง มีความครบถ้วนเป็นปัจจุบันมีการรักษาความเป็นส่วนบุคคล สามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

“ข้อมูล” (Data) หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง

แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“หมวดหมู่ของข้อมูล” (Data Category) หมายความว่า แบ่งออกได้เป็น ๕ หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง

“ระดับชั้นข้อมูล” (Data Classification Level) หมายความว่า ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหว แบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และชั้นลับที่สุด (Top Secret)

“ข้อมูลหลัก” (Master Data) หมายความว่า ข้อมูลที่ถูกสร้างขึ้นเป็นข้อมูลพื้นฐานที่มีความสำคัญต่อการดำเนินงานเพื่อใช้งานร่วมกันภายในองค์กรและขับเคลื่อนองค์กรให้บรรลุเป้าหมาย เช่น ข้อมูลพนักงาน ข้อมูลโครงสร้างองค์กร ข้อมูลครุภัณฑ์ ข้อมูลสถานที่ เป็นต้น

“ข้อมูลอ้างอิง” (Reference Data) หมายความว่า ข้อมูลที่ถูกสร้างขึ้น หรืออ้างอิงมาจากข้อมูลหลัก เพื่อกำหนดให้เป็นมาตรฐาน เป็นสากล และใช้งานร่วมกันในวงกว้าง โดยมีการระบุแหล่งที่มาที่ใช้อ้างอิงได้ชัดเจน หรือมีหน่วยงานรับผิดชอบเป็นทางการ เช่น ข้อมูลรหัสไปรษณีย์ ข้อมูลรหัสประเทศ ข้อมูลชื่อจังหวัด

“ชุดข้อมูล” (Data Set) หมายความว่า การนำข้อมูลมารวบรวมเพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูลหรือลักษณะการนำไปใช้งานและมีการสร้างคำอธิบายชุดข้อมูลประกอบอย่างเป็นระบบ เช่น ตาราง หรือฐานข้อมูล เป็นต้น

“บัญชีข้อมูล” (Data Catalog) หมายความว่า เอกสารแสดงรายการของชุดข้อมูลที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของคณะแพทยศาสตร์และส่วนงาน

“คำอธิบายชุดข้อมูล” (Metadata) หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูล โดยระบุรายละเอียดแหล่งข้อมูล และคำอธิบายรายละเอียดเกี่ยวกับข้อมูล ซึ่งจะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล

“ข้อมูลเปิด” (Open Data) หมายความว่า ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะ สามารถเข้าถึงและนำไปใช้ได้อย่างเสรี ไม่จำกัดแพลตฟอร์ม สามารถนำกลับมาใช้ใหม่ (Reuse) หรือนำไปแจกจ่าย (Redistribute) ได้ภายใต้ข้อตกลงที่กำหนดไว้

“ทรัพยสิทธิ” (Real Rights) หมายความว่า สิทธิที่มีอยู่เหนือตัวทรัพย์สิน ซึ่งได้มาโดยนิติกรรมหรือโดยผลของกฎหมาย โดยทรัพยสิทธิจะเกาะเกี่ยวอยู่กับทรัพย์สินเสมอ

“เจ้าของกรรมสิทธิ์ข้อมูล” (Data Proprietorship) หมายความว่า ทรัพยสิทธิแสดงความเป็นเจ้าของในทรัพย์สินข้อมูล (Information Assets) เป็นสิทธิอันสมบูรณ์ที่สุดที่บุคคลจะพึงมีในทรัพย์สินข้อมูล กรรมสิทธิ์ได้รวมเอาสิทธิทั้งหลายเกี่ยวกับทรัพย์สินข้อมูลเข้าไว้ด้วย ได้แก่ สิทธิในการใช้สอยทรัพยสิทธิ สิทธิในการจำหน่ายทรัพย์สินข้อมูล สิทธิที่จะได้ดอกผลแห่งทรัพย์สินข้อมูลนั้น สิทธิติดตามเอาทรัพย์สินข้อมูลคืนจากผู้ไม่มีสิทธิ และสิทธิขัดขวางมิให้ผู้อื่นสอดเข้าไปเกี่ยวข้องกับทรัพย์สินข้อมูลนั้นโดยไม่ชอบด้วยกฎหมาย

“ผู้ถือสิทธิครอบครองข้อมูล” (Data Holder) หมายความว่า บุคคล หรือคณะบุคคล หรือส่วนงานที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย และมีการทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล และทำหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล มีสิทธิครอบครองการใช้ทรัพย์สินข้อมูลเพื่อประโยชน์ต่อคณะแพทยศาสตร์

“เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายความว่า บุคคลธรรมดาที่มีข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึงได้ไม่ว่าทางตรงหรือทางอ้อม

“คุณภาพข้อมูล” (Data Quality) หมายความว่า ข้อมูลที่เหมาะสมและได้มาตรฐานตามวัตถุประสงค์ กล่าวคือผลรวมของคุณลักษณะและคุณสมบัติของผลิตผลข้อมูล ที่พึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้ มีความแม่นยำ สมบูรณ์แบบ สอดคล้องถูกต้อง มีความเป็นปัจจุบัน และตรงตามความต้องการที่กำหนดและตรงตามวัตถุประสงค์

“ความถูกต้องและสมบูรณ์แบบ” (Accuracy and Completeness) หมายความว่า ข้อมูลถูกต้องแม่นยำ หรือข้อมูลที่ปราศจากข้อผิดพลาดคลาดเคลื่อน หมายถึงขอบเขตที่ข้อมูลถูกต้องเชื่อถือได้ และความสมบูรณ์ของข้อมูล หรือข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน ข้อมูลครบ ทั้งหมดตามที่ผู้ใช้ต้องการ

“ความสอดคล้องกัน” (Consistency) หมายความว่า ข้อมูลถูกนำเสนอในรูปแบบเดียวกัน ข้อมูลต่าง ๆ ที่มีความสัมพันธ์กันล้วนมีความสอดคล้องหรือไม่ขัดแย้งกัน มีแนวคิด คำนิยาม วิธีการและรหัสที่ทำให้ข้อมูลจากต่าง ๆ แหล่งกันสามารถเปรียบเทียบข้ามช่วงเวลา และบูรณาการข้อมูลจากหลายแหล่งได้

“ความเป็นปัจจุบัน” (Timeliness) หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการใช้งาน และพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ผู้ใช้ต้องการ

“ตรงตามความต้องการของผู้ใช้” (Relevancy) หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับงานที่ทำอยู่ เป็นข้อมูลที่ผู้ใช้งานต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมองและความละเอียดเพียงพอต่อการนำไปใช้งาน

“ความพร้อมใช้” (Availability) หมายความว่า ข้อมูลเข้าถึงได้ง่าย หรือมีข้อมูลนั้นอยู่ สามารถใช้งานได้จริงและสามารถใช้งานได้ตลอดเวลา

ข้อ ๔ มีการจัดตั้งคณะกรรมการธรรมาภิบาล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ (Data Governance Committee หรือ DGC) วางนโยบายกำกับดูแลข้อมูล ให้คำแนะนำหรือตัดสินประเด็นสำคัญด้านข้อมูล ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบ ทบทวน ความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสียอย่างน้อยปีละ ๑ ครั้ง และดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

ข้อ ๕ สนับสนุนให้มีระบบการกำหนดกรอบการกำกับดูแลข้อมูลดังนี้

ข้อ ๕.๑ กำหนดบทบาทหน้าที่ ขอบเขตความรับผิดชอบของผู้มีส่วนเกี่ยวข้องกับข้อมูล ที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ที่ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน ผู้บริหารจากส่วนงานต่างๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้ากลุ่มบริกรข้อมูล (Lead Data Steward) คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในการดำเนินการที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล ซึ่งทำหน้าที่ดังนี้

๑. พิจารณากำหนดนโยบาย แนวทางธรรมาภิบาลข้อมูล และหลักเกณฑ์การกำหนดสิทธิหน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ในการบริหารจัดการข้อมูลตามนโยบาย แนวทางธรรมาภิบาลข้อมูล และแนวปฏิบัติธรรมาภิบาลข้อมูล

๒. พิจารณากำหนดแผนธรรมาภิบาลข้อมูล ซึ่งประกอบด้วยมาตรการควบคุมคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคลของข้อมูล โดยสร้างกระบวนการทางสารสนเทศให้มีความปลอดภัยเพียงพอ

๓. พิจารณากำหนดกรอบและหลักเกณฑ์การเปิดเผยข้อมูลและการขอใช้ข้อมูลทั้งภายในและภายนอก คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ส่งเสริมให้ทุกส่วนงานในคณะแพทยศาสตร์ใช้ข้อมูลได้อย่างถูกต้อง และมีประสิทธิภาพ

๔. ให้คำแนะนำหรือตัดสินประเด็นสำคัญด้านข้อมูล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

๕. ตรวจสอบ ทบทวน ความสอดคล้องระหว่าง นโยบาย กับ การดำเนินการใดๆ ของผู้มีส่วนได้ส่วนเสีย และดำเนินการปรับปรุงอย่างต่อเนื่อง

กลุ่มบริกรข้อมูล (Data Stewards Team) ประกอบไปด้วย หัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Steward) บริกรข้อมูลด้านเทคนิค (Technical Data Steward) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Steward) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย กลุ่มบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล ทั้งนี้ กลุ่มบริกรข้อมูล มีบทบาทหน้าที่ดังนี้

๑. จัดทำนโยบายแนวทางธรรมาภิบาลข้อมูลและหลักเกณฑ์การกำหนดสิทธิหน้าที่และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ในการบริหารจัดการข้อมูล ตามแนวทางธรรมาภิบาลข้อมูลและแนวปฏิบัติธรรมาภิบาลข้อมูล รวมทั้งการจัดส่งหรือ เชื่อมโยงชุดข้อมูลของข้อมูลเปิด เสนอคณะกรรมการธรรมาภิบาลข้อมูลเพื่อพิจารณา

๒. จัดทำแผนธรรมาภิบาลข้อมูล ซึ่งประกอบด้วย มาตรการควบคุมคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และความเป็น ส่วนบุคคลของข้อมูล และเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูล เพื่อพิจารณา

๓. จัดทำหลักเกณฑ์การเปิดเผยข้อมูล รวมถึงการขอใช้ข้อมูล ทั้งภายในและภายนอกคณะแพทยศาสตร์ และเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูล เพื่อพิจารณาต่อไป

๔. กำหนดแนวปฏิบัติธรรมาภิบาลข้อมูล ตามหมวดที่ ๑ ถึง ๑๒ ตามประกาศฉบับนี้

๕. กำหนดแนวทางในการวัดระดับ ติดตาม และรวบรวมผลการประเมินธรรมาภิบาลข้อมูล

๖. ดำเนินการกำกับดูแลการดำเนินงาน ตลอดจนรวบรวมข้อมูลและเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูล

๗. ดำเนินการติดต่อและประสานงานกับหน่วยงานภายนอกในการดำเนินการที่เกี่ยวข้องกับการบริหารจัดการข้อมูลตามนโยบายธรรมาภิบาลข้อมูล ให้เป็นไปตามกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

๘. ดำเนินการอื่นๆ ตามที่ได้รับมอบหมายจากคณะกรรมการธรรมาภิบาลข้อมูล

ข้อ ๕.๒ วางแผนการดำเนินงาน กำหนดแนวปฏิบัติเกี่ยวกับการบริหารจัดการข้อมูลที่ได้มาตรฐาน ทันสมัย สอดคล้องกับกฎระเบียบ ข้อตกลง และกฎหมายในประเทศและระหว่างประเทศ โดยสนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและระบบบริหารและ กระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล) จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงานมีการตรวจสอบรายงานผลการดำเนินงานและปรับปรุงแผนการดำเนินงานอย่างต่อเนื่อง มีการวัดผลการบริหารจัดการข้อมูล โดยอย่างน้อยประกอบด้วย การประเมินความพร้อมของธรรมาภิบาลข้อมูลในระดับส่วนงาน การประเมินคุณภาพข้อมูล

และการประเมิน ความมั่นคงปลอดภัยของข้อมูล เพื่อให้ระบบบริหารและกระบวนการจัดการข้อมูลมีประสิทธิภาพ ให้ข้อมูลมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ

ข้อ ๕.๓ จำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายหรือกฎเกณฑ์เกี่ยวกับสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในคณะแพทยศาสตร์ กำหนดการปกป้องรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) จากความเสี่ยงหรือภัยคุกคามทางข้อมูลในทุกรูปแบบ ด้วยมาตรการที่เหมาะสมและมีประสิทธิภาพ เช่น การป้องกันการเข้าถึง การสูญหาย การจัดเก็บข้อมูลและทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต รวมถึงดูแลความลับหรือความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ได้อย่างถูกต้อง โดยกำหนดชั้นความลับของข้อมูล (Data Classification) เช่น ข้อมูลลับ ข้อมูลลับมาก และข้อมูลเปิดเผยได้ เป็นต้น และจัดเก็บให้สอดคล้องกับกฎหมาย เงื่อนไข แนวทาง ข้อกำหนดต่าง ๆ หรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล ต้องคำนึงถึงมูลค่า ความสำคัญ และความ อ่อนไหวของข้อมูล มีการกำหนดมาตรการควบคุม สิทธิ์การเข้าถึงข้อมูล การป้องกันการเข้าถึงข้อมูล (Data Protection) และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล โดยคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ การประมวลผลข้อมูลที่เป็นความลับให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้นและสามารถตรวจสอบย้อนกลับได้ การเปิดเผยข้อมูลต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลส่วนบุคคลก่อนการเปิดเผยข้อมูล และสามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้

ข้อ ๕.๔ มีการดูแลรักษามาตรฐานและคุณภาพข้อมูล (Data Quality) ให้เป็นที่หน้าเชื่อถือและเป็นที่ยอมรับ การประมวลผลข้อมูลและการใช้ข้อมูลให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยไม่ขัดต่อกฎหมาย พร้อมทั้งส่งเสริมให้มีการนำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา มีการประเมินคุณภาพของข้อมูล ด้านความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และมีความพร้อมใช้ (Availability) รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินหรือเหตุละเมิดใด ๆ ที่อาจมีผลต่อการเก็บและใช้ข้อมูล

ข้อ ๕.๕ สนับสนุน สื่อสารและเผยแพร่ นโยบายการนำข้อมูลข้อมูลไปใช้ภายในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ให้เกิดประโยชน์สูงสุดรวมถึงขยายประโยชน์ของข้อมูลสู่ภายนอกได้อย่างเหมาะสม กำหนดและทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้ให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ และต้องสามารถตรวจสอบย้อนกลับได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยนและมาตรฐานตามที่กำหนด

ข้อ ๖ คณะแพทยศาสตร์และส่วนงานต้องมีความรับผิดชอบให้เป็นไปตามธรรมาภิบาลข้อมูลและมีการปฏิบัติเป็นแบบอย่างที่ดีตามประกาศ ระเบียบ ข้อบังคับและแนวทางปฏิบัติด้านการบริหารจัดการข้อมูล

ข้อ ๗ คณะแพทยศาสตร์และส่วนงานต้องมีความรับผิดชอบและปฏิบัติให้เป็นไปตามประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

ข้อ ๘ ส่วนงานในคณะแพทยศาสตร์ต้องจัดทำธรรมาภิบาลข้อมูลในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ โดยให้มีการประเมินผลการปฏิบัติงานตามกฎ ระเบียบมาตรการ แนวปฏิบัติด้านการบริหารจัดการข้อมูลตามแนวทางของคณะแพทยศาสตร์

แนวทางการดำเนินงานและแผนธรรมาภิบาลข้อมูล

การกำหนดวิธีการบริหารจัดการธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ ที่ระบุอย่างชัดเจน สอดคล้องกับ กฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือ ข้อกำหนดอื่นๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหารมีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมทั้งการดำเนินการทบทวนอย่างสม่ำเสมอ เพื่อให้แนวทางและแผนธรรมาภิบาลข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง และมีการจัดทำคำอธิบายชุดข้อมูล (Data Set) ในระดับองค์กรให้มีความชัดเจนและสอดคล้องกับกรอบการดำเนินการที่กำหนดในพระราชบัญญัติและตามกรอบธรรมาภิบาลข้อมูล (Data Governance Framework) เพื่อเป็นพื้นฐานสำคัญในการกำกับดูแลการพัฒนาระบบดิจิทัลที่จะสามารถบูรณาการข้อมูลและการทำงานทั้งด้านการบริหารจัดการภายใน และเครือข่ายให้มีประสิทธิภาพต่อไป

ปัจจุบันประเทศไทยมีกฎหมายหลายฉบับที่กำหนดให้หน่วยงานภาครัฐต้องบริหารจัดการและดำเนินงานที่เกี่ยวข้องกับข้อมูลในหลายมุม เพื่อแสดงความโปร่งใสในการดำเนินงานและสามารถตรวจสอบได้จากทุกภาคส่วน ประชาชนทั่วไป ภาคธุรกิจ หรือประชาชนจะสามารถนำข้อมูลไปเผยแพร่ต่อ ใช้ประโยชน์หรือพัฒนาบริการและนวัตกรรมในรูปแบบต่าง ๆ ได้ โดยกฎหมายและข้อกำหนดต่าง ๆ เกี่ยวข้องกับข้อมูลที่หน่วยงานของรัฐควรจะต้องปฏิบัติตามให้สอดคล้องและเหมาะสม โดยเฉพาะประเด็นเกี่ยวกับธรรมาภิบาลข้อมูล มีดังนี้

กฎหมายและแนวทางที่เกี่ยวข้อง

๑) รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ ในมาตราที่ ๕๙ ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

๒) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๓) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

๕) พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒

๖) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๗) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)

๘) มรด. ๓-๑: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (Government Data Catalog Guideline)

๙) มรด. ๓-๒: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ (Government Data Catalog Registration Guideline)

๑๐) มรด. ๔-๑: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Policy)

๑๑) มรด. ๔-๒: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline)

๑๒) มรด. ๕: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (Data Quality Assessment Framework for Government Agency)

๑๓) มสพร. ๘-๒๕๖๕ มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework)

รัฐธรรมนูญแห่งราชอาณาจักรไทย

มาตรา ๒๕๘ ให้ดำเนินการปฏิรูปประเทศอย่างน้อยในด้านต่างๆ ให้เกิดผล

ให้มีการนำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้ในการบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะ เพื่อประโยชน์ในการบริหารราชการแผ่นดิน และเพื่ออำนวยความสะดวกให้แก่ประชาชน

ให้มีการบูรณาการฐานข้อมูลของหน่วยงานของรัฐทุกหน่วยงานเข้าด้วยกันเพื่อให้เป็นระบบข้อมูลเพื่อการบริหารราชการแผ่นดินและการบริการประชาชน

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒

หน่วยงานรัฐต้องจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล การบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ทั้งนี้เพื่อเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึงประชาชน และเพื่อให้มีการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

หน่วยงานของรัฐพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็นให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนา กระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ มีการบูรณาการ และสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้ง ให้ประชาชนเข้าถึงโดยสะดวก

กำหนดให้หน่วยงานของรัฐมีการเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐ จัดทำ และครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประขาชนเข้าถึงโดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐและสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

หน่วยงานของรัฐต้องควบคุมและกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยทางไซเบอร์และทางกายภาพ รวมทั้งรักษาสถานะของข้อมูลและระบบ คอมพิวเตอร์ให้มีความพร้อมใช้งาน และข้อมูลไม่รั่วไหลโดยมิชอบ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

หน่วยงานต้องมีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

หน่วยงานรัฐต้องกำหนดหลักการหรือแนวปฏิบัติที่เกี่ยวกับการเปิดเผยข้อมูล ๓ ประเด็น ได้แก่

๑) ข้อมูลภาครัฐต้อง "เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น" ๒) มีการกำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล ๓) มีการกำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้

ประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครอง อย่างมีหลักเกณฑ์

ระเบียบว่าด้วยการรักษาความลับของทางราชการพ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม

ได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

มติคณะรัฐมนตรีเมื่อวันที่ ๗ พฤษภาคม พ.ศ. ๒๕๖๒ เรื่อง แนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data)

ให้หน่วยงานภาครัฐร่วมมือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานสถิติแห่งชาติในการจัดทำรายการข้อมูลภาครัฐ (Government Data Catalog) และ ระบบนามานุกรม (Directory Services) ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอ

มติคณะรัฐมนตรีวันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๖๒ เรื่อง ข้อเสนอมาตรฐานสถิติ

คณะรัฐมนตรีมีมติเห็นชอบตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอ ให้ส่วนราชการ รัฐวิสาหกิจ องค์กรปกครองส่วนท้องถิ่น และหน่วยงานของรัฐจัดส่งข้อมูลการใช้มาตรฐานสถิติรวมถึงรายละเอียดของข้อมูล (Metadata) ตามมาตรฐานที่สำนักงานสถิติแห่งชาติ กำหนดทั้งข้อมูลระดับย่อย (Microdata) และข้อมูลสถิติ เพื่อให้สำนักงานสถิติแห่งชาติรวบรวมเป็นข้อมูลในการจัดทำศูนย์กลางรายการข้อมูลภาครัฐ (National Data Catalogue and Directory Services) และเพื่อให้สามารถติดตามและประเมินสถานการณ์ การพัฒนาสถิติของประเทศให้มีคุณภาพตามหลักการพื้นฐานสถิติทางการและสอดคล้องตามมาตรฐานสากล สามารถนำมาใช้สนับสนุนการตัดสินใจของผู้บริหารและการใช้ประโยชน์จากข้อมูลร่วมกันได้อย่างคุ้มค่า

วัตถุประสงค์

การจัดทำแนวทางและแผนธรรมาภิบาลข้อมูลคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เพื่อให้ส่วนงานต่าง ๆ ในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ สามารถนำไปผลักดัน และดำเนินการตามธรรมาภิบาลข้อมูล รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อ คุณภาพ ความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน มีรายละเอียดดังนี้

๑) เพื่อจัดทำวิธีการบริหารจัดการและกำกับดูแลข้อมูล ให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๒) เพื่อให้มีการกำหนดมาตรการในการควบคุม ตรวจสอบ และพัฒนาคุณภาพข้อมูล เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ

๓) เพื่อให้มีการกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงข้อมูลและใช้ประโยชน์จากข้อมูลที่ชัดเจน รวมทั้งมีการกำหนดมาตรการและหลักประกันในการคุ้มครองป้องกันข้อมูลที่อยู่ในความครอบครองของคณะแพทยศาสตร์ โดยใช้กระบวนการธรรมาภิบาลข้อมูลและความปลอดภัยของข้อมูล ให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด

๔) เพื่อดำเนินการกำหนดบทบาทหน้าที่ กรอบการทำงานของผู้ถือสิทธิครอบครองข้อมูล และผู้ที่เกี่ยวข้องกับข้อมูลในทุกขั้นตอน เช่นการกำหนดวิธีการที่ผู้ดูแลข้อมูลหรือผู้ถือสิทธิครอบครองข้อมูลสามารถจัดการ เปลี่ยนแปลง หรือส่งผ่านข้อมูลให้ชัดเจน เพื่อไม่ให้เกิดปัญหาในกรณีที่ชุดข้อมูลหรือ

ฐานข้อมูลบางแหล่งอาจจะมีผู้ดูแล ผู้ใช้งาน หรือผู้ถือสิทธิครอบครองข้อมูลหลายคนหรือหลายหน่วยงาน

๕) เพื่อกำหนดเมทาดาตาของข้อมูล โดยใช้การจำแนกข้อมูลช่วยให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไรสามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไร โดยมีมาตรฐานของเมทาดาตาที่เหมาะสมกับการใช้งาน

๖) เพื่อจัดทำชุดข้อมูล (Data Set) สำหรับนำมาใช้งานรวมถึงแลกเปลี่ยนข้อมูล หรือประมวลผลข้อมูลให้บริการข้อมูลกับหน่วยงานภายในและภายนอกคณะแพทยศาสตร์ และยังสามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้ อย่างมีประสิทธิภาพ

ส่วนงานที่จะนำไปใช้

ธรรมาภิบาลข้อมูลคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่นี้ครอบคลุมถึงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลภายในส่วนงานต่างๆ ทั้ง ภาควิชา หน่วยงานสังกัดคณะแพทยศาสตร์ ศูนย์ต่างๆ และหน่วยงานสังกัดโรงพยาบาล ดังนี้

๑. ภาควิชา ได้แก่ ภาควิชากายวิภาคศาสตร์ ภาควิชากุมารเวชศาสตร์ ภาควิชาจักษุวิทยา ภาควิชาจิตเวชศาสตร์ ภาควิชาจุลชีววิทยา ภาควิชาชีวเคมี ภาควิชานิติเวชศาสตร์ ภาควิชาปรสิตวิทยา ภาควิชาพยาธิวิทยา ภาควิชาเภสัชวิทยา ภาควิชารังสีวิทยา ภาควิชาวิสัญญีวิทยา ภาควิชาเวชศาสตร์ครอบครัว ภาควิชาเวชศาสตร์ฉุกเฉิน ภาควิชาเวชศาสตร์ชุมชน ภาควิชาเวชศาสตร์ฟื้นฟู ภาควิชาศัลยศาสตร์ ภาควิชาสรีรวิทยา ภาควิชาสูติศาสตร์และนรีเวชวิทยา ภาควิชาโสต ศอ นาสิกวิทยา ภาควิชาอายุรศาสตร์ และภาควิชาออร์โทปิดิกส์
๒. หน่วยงานสังกัดคณะฯ ได้แก่ งานคลัง งานซ่อมบำรุง งานเทคโนโลยีสารสนเทศ งานนโยบายและแผน งานบริการการศึกษา งานบริการวิชาการและวิเทศสัมพันธ์ งานบริหารงานบุคคล งานบริหารงานวิจัย งานบริหารทั่วไป งานประกันคุณภาพการศึกษา งานประชาสัมพันธ์ งานพัสดุและยานพาหนะ งานโสตทัศนศึกษา งานอาคารสถานที่และงานห้องสมุด [สังกัดสำนักหอสมุด มช.]
๓. ศูนย์ต่าง ๆ ได้แก่ ศูนย์ศรีพัฒน์ ศูนย์ความเป็นเลิศทางการแพทย์ ศูนย์ฝึกทักษะผ่าตัด ศูนย์โรคสมองภาคเหนือ ศูนย์วิจัยและฝึกอบรมสาขาโรคทางไฟฟ้าหัวใจ ศูนย์เลสิคฯ ศูนย์เพทซีที ศูนย์ผ่าตัดต้อกระจกด้วยเลเซอร์ ศูนย์สุขภาพสตรี ศูนย์การแพทย์ผสมผสาน ศูนย์บริหารจัดการข้อมูล (OC) ศูนย์พัฒนาเทคโนโลยีแพทยศาสตรศึกษา (MTEC) และศูนย์บูรณาการเทคโนโลยีการแพทย์ทันสมัย (CMUTEAM)
๔. หน่วยงานสังกัดโรงพยาบาล ได้แก่ ฝ่ายการพยาบาล ฝ่ายเภสัชกรรม งานทันตกรรม งานธนาคารเลือด งานบริการกลางโรงพยาบาล งานบริหารโรงพยาบาล งานปฏิบัติการชันสูตร งานประกันสังคม งานพัฒนาคุณภาพโรงพยาบาล งานโภชนาการ งานเวชภัณฑ์ปลอดเชื้อ งานเวชระเบียนและสถิติ งานสังคมสงเคราะห์ หน่วยทะเบียนมะเร็งและหน่วยสร้างเสริมสุขภาพ

กระบวนการธรรมาภิบาลข้อมูล เริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่องดังนี้

๑. การวางแผน (Plan)

การวางแผน เริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนดกฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่างๆ เพื่อใช้ในธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล ขั้นตอนถัดไปคือ การกำหนดขอบเขต

การดำเนินการ ระยะเวลาดำเนินการ บุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

๒. ขั้นตอนการปฏิบัติ (Operating Procedure)
การดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูล และผู้ที่เกี่ยวข้องอื่นๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูล วิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล เจ้าของข้อมูลส่วนบุคคล ผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล ผู้ถือสิทธิครอบครองข้อมูล ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้อง สามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้รายงานความก้าวหน้า ผลการปฏิบัติงาน และประเด็นปัญหาที่พบระหว่างปฏิบัติงาน จะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูล

๓. การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report)
ในการตรวจสอบบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนดกับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่นๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูล ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงาน และประเด็นปัญหาที่พบ

๔. การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)
ธรรมาภิบาลข้อมูลเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่อง ตลอดระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการความต้องการ จากผู้บริหารและผู้มีส่วนได้ส่วนเสีย รวมไปถึงผลการตรวจสอบ เช่น รายงานผลการตรวจสอบความสอดคล้อง ของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูล นโยบาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูล

แนวทางและแผนธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ แบ่งเนื้อหาตามหมวดดังนี้

หมวดที่ ๑ บททั่วไป
หมวดที่ ๒ การสร้างและการรวบรวมข้อมูล
หมวดที่ ๓ การจัดเก็บและการสำรองข้อมูล
หมวดที่ ๔ การจัดหมวดและการทำบัญชีข้อมูล
หมวดที่ ๕ การประมวลผลและการใช้ข้อมูล
หมวดที่ ๖ การเข้ารหัสและการปกป้องข้อมูล
หมวดที่ ๗ การจัดทำข้อมูลนิรนาม
หมวดที่ ๘ การควบคุมการเข้าถึงข้อมูล
หมวดที่ ๙ การควบคุมคุณภาพและมาตรฐานข้อมูล
หมวดที่ ๑๐ การแลกเปลี่ยน เชื่อมโยงข้อมูล และการเปิดเผยข้อมูล
หมวดที่ ๑๑ การจัดการเหตุละเมิดที่เกี่ยวข้องกับข้อมูล
หมวดที่ ๑๒ การทำลายข้อมูล

หมวดที่ ๑ บททั่วไป

การบริหารจัดการข้อมูลภายในองค์กรให้อยู่ในรูปแบบดิจิทัลเพื่อเตรียมความพร้อมในการรองรับการจัดเก็บ แลกเปลี่ยน เชื่อมโยง และเปิดเผยข้อมูลทั้งภายในและภายนอกองค์กรตามกรอบธรรมาภิบาลข้อมูลสู่การนำไปใช้ประโยชน์ร่วมกัน เริ่มจากการวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล (Data Governance Metrics and Success Measures) เป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูล จะแสดงให้เห็นถึงสถานะปัจจุบันของหน่วยงานในเรื่องความพร้อมและความก้าวหน้าในการดำเนินการธรรมาภิบาลข้อมูล ซึ่งผลของการดำเนินการธรรมาภิบาลข้อมูลจะส่งผลถึงความสำเร็จของธรรมาภิบาลข้อมูลมีรายละเอียด คือ ด้านโครงสร้างธรรมาภิบาลข้อมูล กระบวนการธรรมาภิบาลข้อมูล นโยบายข้อมูลและการตรวจสอบ การประเมินคุณภาพและความมั่นคงปลอดภัยของข้อมูล การปรับปรุงอย่างต่อเนื่อง ซึ่งประกอบด้วยระดับดังนี้

- ระดับ ๐ None หมายถึง ไม่มีธรรมาภิบาลข้อมูลหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ อาจมีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ
- ระดับ ๑ Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ คือกระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Ad Hoc) ทำให้แต่ละส่วนงานหรือโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศ
- ระดับ ๒ Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงาน หรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล
- ระดับ ๓ Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือ ความมั่นคงปลอดภัย
- ระดับ ๔ Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางและระบบในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูล และความมั่นคงปลอดภัย
- ระดับ ๕ Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non Conformation) คุณภาพข้อมูลที่ต่ำและความไม่คุ้มทุนในการบริหารจัดการข้อมูล โดยดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างธรรมาภิบาลข้อมูล เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

บริหารจัดการ บูรณาการข้อมูล *และมีธรรมาภิบาลข้อมูล (Data Governance and Openness)*

๑. สำรวจชุดข้อมูล และกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูลภายในองค์กร รวมถึงจัดตั้งคณะทำงานที่เกี่ยวข้อง
๒. วางแผนธรรมาภิบาลข้อมูล และจัดทำแนวปฏิบัติธรรมาภิบาลข้อมูล ได้แก่ บัญชีข้อมูล (Data Catalog) ชุดข้อมูล (Data Set) คำอธิบายชุดข้อมูล (Metadata) การจำแนกชั้นความลับข้อมูล (Data Classification) รูปแบบของชุดข้อมูลของข้อมูลเปิด (Open Data Format) และกระบวนการจัดการข้อมูล การจัดส่งหรือ เชื่อมโยงชุดข้อมูล เป็นต้น
๓. กำหนดแนวทางการวัดระดับ ติดตาม และรวบรวมผลการประเมินธรรมาภิบาลข้อมูล

๔. ปรับปรุงและพัฒนาระบบคลังข้อมูล และระบบบริการข้อมูลให้รองรับการแลกเปลี่ยนเชื่อมโยงข้อมูลทั้งภายในและภายนอกคณะแพทยศาสตร์

บริหารจัดการด้าน*ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)*

๑. วางแผนกำหนดกระบวนการแนวปฏิบัติเกี่ยวกับการป้องกันข้อมูลในบริบทของการรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) ตามมาตรฐาน ISO/IEC27001 เช่น ระบบการจัดการฐานข้อมูล (Database Management System: DBMS), เทคโนโลยีจัดการข้อมูลเพื่อแสดงตัวตน (Identity Management Technology), ระบบจัดการการเปลี่ยนแปลง (Change Control System) หรือหนังสือให้ความยินยอม (Letter of Consent)

๒. กำหนดให้ระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจนในการดำเนินการอื่นใดเกี่ยวกับข้อมูล เพื่อรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)

พัฒนากลไกและมาตรการสนับสนุนเพื่อส่งเสริมการเชื่อมโยงและใช้ประโยชน์จากข้อมูล (*Data Accessibility and Usability)*

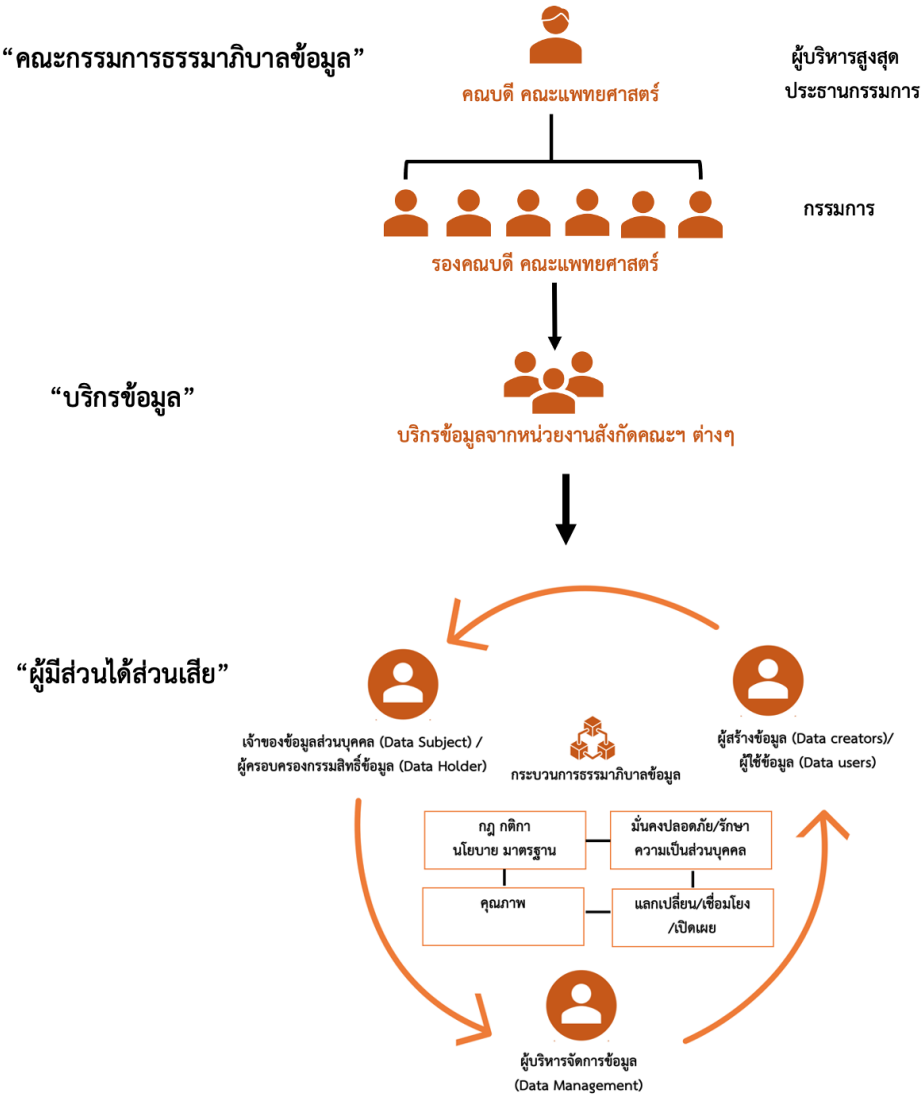
๑. สนับสนุนการเข้าถึงข้อมูลผ่านอุปกรณ์ที่หลากหลาย และปรับปรุงแนวทางการวิเคราะห์ การใช้ข้อมูล หรือรายงานเพื่อสร้างความสะดวกต่อผู้ใช้งาน เช่น การพัฒนาและใช้ Management Dashboard เพื่อการบริหารจัดการสำหรับผู้บริหารทุกระดับและกลุ่มภารกิจสำคัญ

๒. เสริมสร้างความความเข้าใจและความตระหนักด้านการใช้ประโยชน์ข้อมูลเปิด เพื่อให้เกิดการตรวจสอบการทำงาน และเกิดการนำข้อมูลไปต่อยอดเป็นนวัตกรรมบริการต่อไป รวมทั้งการเปิดเผย หรือ แลกเปลี่ยนข้อมูลตามกฎหมายที่เกี่ยวข้อง

๓. กำหนดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) เสริมสร้างความรู้และความเข้าใจ ทบทวนมาตรการรักษาความ มั่นคงปลอดภัยให้สอดรับกับกฎหมายและข้อบังคับที่เปลี่ยนแปลงไป

โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)

โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูล (Data Governance Structure) แบ่งออกเป็น ๓ ส่วน ประกอบด้วย (๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) (๒) กลุ่มบริกรข้อมูล (Data Steward Team) และ (๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) ดังรูปที่ ๑ แสดงตัวอย่างโครงสร้างธรรมาภิบาลข้อมูล และ รูปที่ ๒ แผนภาพการดำเนินการธรรมาภิบาลข้อมูล



รูปที่ ๑ โครงสร้างธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

คณะกรรมการธรรมาภิบาลข้อมูล คณะแพทยศาสตร์ฯ (Data Governance Committee) ประกอบไปด้วยผู้บริหารสูงสุด โดยกำหนดให้คณบดี คณะแพทยศาสตร์ ปฏิบัติหน้าที่ประธานกรรมการธรรมาภิบาลข้อมูล คณะแพทยศาสตรศาสตร์ ผู้บริหารระดับสูงด้านข้อมูล กำหนดให้รองคณบดีด้านเทคโนโลยีสารสนเทศปฏิบัติหน้าที่รองประธานกรรมการธรรมาภิบาลข้อมูลและผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและ

ฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึง หัวหน้ากลุ่มบริกรข้อมูล ปฏิบัติหน้าที่คณะกรรมการธรรมาภิบาลข้อมูล คณะแพทยศาสตรศาสตร์ คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการภายในคณะกรรมการธรรมาภิบาลข้อมูล

มีบทบาท

๑. พิจารณากำหนดนโยบาย แนวทางธรรมาภิบาลข้อมูล หลักเกณฑ์การกำหนดสิทธิ หน้าที่ ความรับผิดชอบ เกณฑ์การวัดคุณภาพ เกณฑ์ความมั่นคงปลอดภัย ชั้นความลับ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล และรวมไปถึงการจัดลำดับความสำคัญของข้อมูล ในการบริหารจัดการข้อมูลตามนโยบาย แนวทาง และแนวปฏิบัติธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ และประกาศเป็นนโยบาย แนวทางธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ต่อไป

๒. พิจารณากำหนดแผนธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ โดยวิเคราะห์ข้อมูล เพื่อจัดทำยุทธศาสตร์ และดำเนินการกำกับดูแลข้อมูลให้มีมาตรการควบคุมคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคลของข้อมูล เพื่อประกาศใช้ต่อไป

๓. พิจารณาให้ความเห็นและข้อเสนอแนะในด้านการจัดการและการกำกับดูแลข้อมูลต่อบริกรข้อมูล และให้การสนับสนุนทรัพยากร เช่น การสร้างกระบวนการทางสารสนเทศให้มีความปลอดภัยเพียงพอ ทั้งด้านการควบคุมข้อมูลและการใช้ข้อมูลในแต่ละหน่วยงาน/ฝ่าย โดยการปรับปรุงความมั่นคงทางกายภาพและความปลอดภัยด้านเทคโนโลยีให้มากขึ้น พร้อมทั้งต้องวิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูลทำให้เกิดการเชื่อมต่อระหว่างหน่วยงาน เพื่อให้การดำเนินงานสอดคล้องกับแผนกลยุทธ์ของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

๔. พิจารณากำหนดกรอบและหลักเกณฑ์การเปิดเผยข้อมูล และการขอใช้ข้อมูล ทั้งภายในและภายนอกคณะแพทยศาสตร์เพื่อประกาศใช้ต่อไป และเป็นตัวกลางระหว่างหน่วยงานภาครัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ข้อมูลมีคุณภาพ และเกิดประโยชน์สูงสุดต่อคณะแพทยศาสตร์

๕. พิจารณาทบทวนนโยบายและแนวทางธรรมาภิบาลข้อมูลของคณะแพทยศาสตร์ โดยจัดประชุมอย่างน้อยปีละ ๒ ครั้ง เพื่อรับทราบปัญหา ทบทวน ความสอดคล้องระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสีย และดำเนินการปรับปรุงอย่างต่อเนื่อง และตัดสินประเด็นสำคัญเชิงนโยบายด้านข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แก้ปัญหาและบริหารจัดการภายในคณะกรรมการธรรมาภิบาลข้อมูล

กลุ่มบริกรข้อมูล (Data Steward Team) ประกอบไปด้วยหัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Steward) บริกรข้อมูลด้านเทคนิค (Technical Data Steward) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Steward) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคง ปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลที่ดีภายในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ กลุ่มบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูล และควบคุมการดำเนินการกำกับดูแล ติดตาม และรายงานผล การดำเนินการธรรมาภิบาลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล หัวหน้าบริกรข้อมูลทำหน้าที่เป็นผู้ควบคุมและสั่งการภายในกลุ่มบริกรข้อมูล และเป็นหนึ่งในคณะกรรมการธรรมาภิบาลข้อมูล

๑. บริกรข้อมูลด้านธุรกิจ (Business Data Steward) มีหน้าที่ความรับผิดชอบ ในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย จัดทำนโยบาย แนวทาง แผนธรรมาภิบาลข้อมูล และ

หลักเกณฑ์ การกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการเปิดเผยข้อมูล รวมถึงการขอใช้ข้อมูล ทั้งภายในและภายนอกคณะแพทยศาสตร์ ของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูล กำหนดแนวปฏิบัติธรรมาภิบาลข้อมูล การจัดทำบัญชีข้อมูล (Data Catalog) ชุดข้อมูล (Data Set) คำอธิบายชุดข้อมูล (Metadata) การจำแนกชั้นความลับของข้อมูล (Data Classification) รูปแบบของชุดข้อมูลของข้อมูลเปิด (Open Data Format) การจัดส่งหรือเชื่อมโยงชุดข้อมูล โดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิกข้อมูล และนักวิเคราะห์ระบบ ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากผู้บริหารจัดการข้อมูล ควบคุมการดำเนินงานตามนโยบายจากคณะกรรมการธรรมาภิบาลข้อมูล ตรวจสอบติดตามการปฏิบัติตามนโยบายข้อมูล ประสานงานในปัญหาด้านข้อมูลจากบุคลากรในส่วนงาน รวบรวมข้อเสนอแนะต่างๆ และเสนอรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลเพื่อพิจารณา แจ้งผู้ที่เกี่ยวข้องอื่นๆ ให้ทราบ รวมถึงการดำเนินการจัดการให้ความรู้และการอบรมธรรมาภิบาลข้อมูลแก่เจ้าหน้าที่และผู้ใช้บริการ ในคณะแพทยศาสตรศาสตร์ ให้มีความเข้าใจในบทบาทหน้าที่ที่มีต่อข้อมูลในหน่วยงาน

๒. บริกรข้อมูลด้านเทคนิค (Technical Data Steward) มีหน้าที่ความรับผิดชอบ ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูลและนิยามคำอธิบายชุดข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัย รักษาและดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่างๆ และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค

๓. บริกรข้อมูลด้านคุณภาพ (Data Quality Steward) มีหน้าที่ความรับผิดชอบ คือ การนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย ซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล หรือผู้มีส่วนได้ส่วนเสียอื่นๆ ดำเนินการในเรื่อง คุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูลตามมาตรการควบคุมคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคลของข้อมูล ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูล และการวิเคราะห์คุณภาพข้อมูลและผลจากการตรวจสอบคุณภาพ กำหนดแนวทางในการวัดระดับ ติดตามและรวบรวมผลการประเมินธรรมาภิบาลข้อมูล

นอกเหนือจากคณะกรรมการธรรมาภิบาลข้อมูลและกลุ่มบริกรข้อมูล ยังมีผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) อื่นๆ ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลต่อกลุ่มบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย ผู้ถือสิทธิครอบครองข้อมูล (Data Holder) เจ้าของข้อมูลส่วนบุคคล (Data Subject) กลุ่มบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creator) และผู้ใช้ข้อมูล (Data User)

(๑) ผู้ถือสิทธิครอบครองข้อมูล หมายถึง บุคคล/คณะบุคคล สังกัดคณะแพทยศาสตร์ ที่ทำหน้าที่

- ตรวจสอบดูแลข้อมูลโดยตรง
- สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย
- ทบทวนและร่วมกันอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น ทำความสะอาดข้อมูล (Data Cleansing)
- ดำเนินงานตรวจสอบคุณภาพข้อมูลและการเชื่อมโยงข้อมูลร่วมกับบริกรข้อมูล
- มีส่วนในการระบุและกำหนดการให้สิทธิ์ในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลเพื่อให้คณะกรรมการธรรมาภิบาลข้อมูลอนุมัติ
- เป็นผู้ควบคุมการดำเนินงานของผู้ใช้ข้อมูล
- จัดเตรียมชุดข้อมูลและลงทะเบียนบัญชีชุดข้อมูล

(๒) เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลธรรมดาที่มีข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึงได้ไม่ว่าทางตรงหรือทางอ้อม

(๓) ผู้สร้างข้อมูล (Data Creators) หมายถึง บุคคล/คณะบุคคล สังกัดคณะแพทยศาสตร์ ที่ทำหน้าที่

- บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ ทั้งเป็นการปฏิบัติงานโดยตรง หรือผ่านระบบหรือโปรแกรมหรือเครื่องมือใด ๆ

- ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

(๔) ผู้ใช้ข้อมูล (Data Users) หมายถึง บุคคล/คณะบุคคล สังกัดคณะแพทยศาสตร์ ที่ทำหน้าที่

- นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร

- ให้ความร่วมมือและสนับสนุนการกำกับดูแลข้อมูลโดยการให้ความต้องการในการใช้ข้อมูล

- รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

(๕) กลุ่มบริหารจัดการข้อมูล (Data Management Team) หมายถึง บุคคล/คณะบุคคล สังกัดคณะแพทยศาสตร์ ที่ทำหน้าที่ควบคุม ติดตามและรายงานงานผลต่อกลุ่มบริกรข้อมูล ดำเนินการติดต่อและประสานงานกับหน่วยงานภายนอกใน การดำเนินการที่เกี่ยวข้องกับการบริหารจัดการข้อมูลตามนโยบายธรรมาภิบาลข้อมูลให้เป็นไปตามกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล ประกอบด้วย

- สถาปนิกข้อมูล (Data Architects) ความรับผิดชอบคือ กำหนดโครงสร้างและความสัมพันธ์ของข้อมูลโดยพิจารณาจากความต้องการข้อมูลทั้งหมดและวัตถุประสงค์พัฒนาสถาปัตยกรรมข้อมูลในภาพรวม โดยประเมินสถานะในปัจจุบันและออกแบบเพื่อปรับปรุงสำหรับอนาคต สร้างพิมพ์เขียว (Blueprint) สำหรับการบริหารจัดการข้อมูลต่าง ๆ เช่น การบูรณาการข้อมูล การไหลของข้อมูลตั้งแต่ต้นทางจนถึงปลายทาง

- นักจัดการฐานข้อมูล (Database Administrator: DBA) ความรับผิดชอบคือ บริหารจัดการและควบคุมเกี่ยวกับระบบฐานข้อมูลภายในคณะแพทยศาสตร์ กำหนดนโยบาย มาตรการและมาตรฐานของระบบฐานข้อมูลทั้งหมดภายในคณะแพทยศาสตร์ ตัวอย่างเช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล การกำหนดสิทธิการเข้าถึงข้อมูล

- วิศวกรข้อมูล (Data Engineer) ความรับผิดชอบคือ ออกแบบและดำเนินการเพื่อสร้างวิธีการจัดเก็บเรียกใช้งานและจัดการข้อมูล ตั้งแต่ระบุชนิดของข้อมูล การนิยามเมทาดาตา วางโครงสร้างของการเข้าและการออกของข้อมูล เพื่อให้ข้อมูลไหลได้อย่างเป็นระบบ

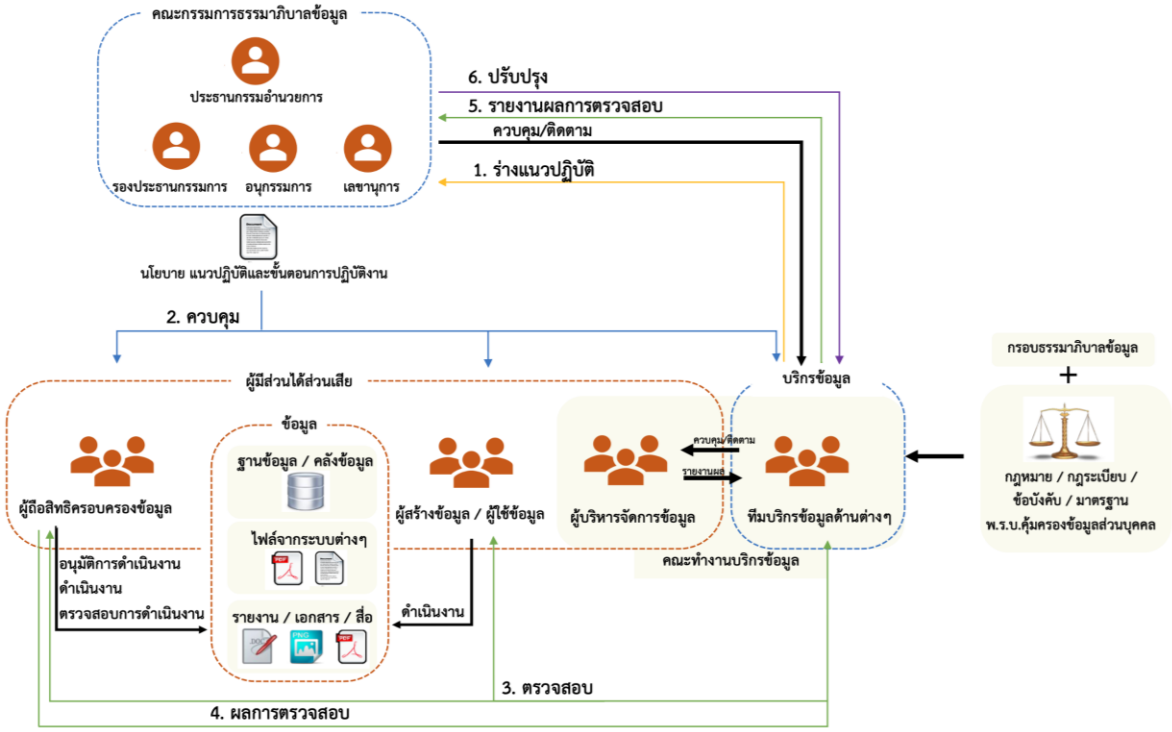
- นักวิเคราะห์ข้อมูล (Data Analyst) ความรับผิดชอบคือ นำข้อมูลมาวิเคราะห์แนวโน้มหรือแก้ปัญหาจากสิ่งที่ผิดแปลกไปจากแนวโน้มเดิมโดยใช้ประสบการณ์และหลักสถิติ ใช้โมเดลหรือเครื่องมือในการทำรายงานเพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ

- นักวิทยาการข้อมูล (Data Scientist) ความรับผิดชอบคือนำข้อมูลจากหลาย ๆ แหล่ง เพื่อประมวลผลข้อมูล สร้างแบบจำลอง และดำเนินการกับข้อมูล เพื่อหาคำตอบตามโจทย์ที่ได้รับ ด้วยวิธีการต่าง ๆ เช่น Machine Learning เป็นต้น

- นักวิเคราะห์ระบบ (System Analyst) ความรับผิดชอบคือวิเคราะห์และออกแบบระบบ โดยศึกษาเกี่ยวกับปัญหา รวบรวมความต้องการของผู้ใช้งานระบบ วิเคราะห์ระบบงานภายในหน่วยงาน

- นักวิเคราะห์ธุรกิจ (Business Analyst) ความรับผิดชอบคือศึกษาและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับเทคโนโลยี กลยุทธ์ กลุ่มเป้าหมาย และหน่วยงานที่เกี่ยวข้อง ทำความเข้าใจเป้าหมายและปัญหาของหน่วยงาน วิเคราะห์ความต้องการและหาคำตอบเพื่อวางแผนด้านกลยุทธ์ เพื่อผลักดันให้เกิดการเปลี่ยนแปลง

- นักออกแบบจำลองข้อมูล (Data Modeler) ความรับผิดชอบคือออกแบบและพัฒนาแบบจำลองข้อมูล (Data Model) เพื่ออธิบายลักษณะโครงสร้างและการทำงานของข้อมูลให้อย่างชัดเจน ด้วยเครื่องมือต่าง ๆ เช่น Entity Relationship Diagram และ Data Flow Diagram เป็นต้น



รูปที่ ๒ แผนภาพการดำเนินการธรรมาภิบาลข้อมูล

หมวดที่ ๒ การสร้างและการเก็บรวบรวมข้อมูล

วัตถุประสงค์

เพื่อให้การสร้างและการเก็บรวบรวมข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารข้อมูลและการให้บริการที่เกี่ยวกับข้อมูลของคณะแพทยศาสตร์ เป็นไปตามอำนาจหน้าที่ วัตถุประสงค์ในการดำเนินงานของคณะแพทยศาสตร์ และตามที่กฎหมายกำหนด

คำนิยาม

๑. กระบวนการสร้างข้อมูล (Create) หมายถึง การสร้างข้อมูลโดยวิธีการบันทึกด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการนำเข้าข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

๒. กระบวนการเก็บรวบรวมข้อมูล (Collect) หมายถึง การรวบรวมข้อมูลจากแหล่งต่าง ๆ ทั้งข้อมูลข้อมูลปฐมภูมิและข้อมูลทุติยภูมิ ตามวัตถุประสงค์ในการดำเนินงาน

นโยบาย

ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัด ในประเด็นดังต่อไปนี้

๑. กระบวนการสร้างข้อมูล ให้สร้างหรือรวบรวมข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือและอ้างอิงได้

๒. กระบวนการสร้างข้อมูล ห้ามสร้างข้อมูลที่บิดเบือน หรือปลอมแปลงไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่เพื่อจุดประสงค์การปกป้องความเป็นส่วนตัว รวมถึงข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงหรือการก่อการร้าย

๓. กระบวนการสร้างข้อมูล ห้ามสร้างข้อมูลที่ขัดต่อกฎหมายลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๔. กระบวนการเก็บรวบรวมข้อมูล ในกรณีที่มีข้อมูลซึ่งเป็นข้อมูลส่วนบุคคลและ/หรือข้อมูลส่วนบุคคลอ่อนไหว จำเป็นต้องได้รับคำยินยอม (Consent) จากเจ้าของข้อมูลด้วย เว้นแต่กรณีที่ได้รับการยกเว้นการขอคำยินยอมหรือไม่ต้องขอคำยินยอมตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง

แนวทาง

๑. ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล กลุ่มบริหารจัดการข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงหน่วยงานที่เกี่ยวข้อง ร่วมกันออกแบบและกำหนดมาตรฐานการสร้างและรวบรวมข้อมูลให้เป็นแบบเดียวกัน จากนั้นให้นำเสนอขออนุญาต ผู้บังคับบัญชาองค์กร หรือผู้บังคับบัญชาหน่วยงานที่มีอำนาจตัดสินใจภายใต้ขอบเขต หน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บังคับบัญชาองค์กรแล้วเท่านั้น เพื่อประกาศใช้

๒. จัดประชุม/อบรม/ประชาสัมพันธ์ ให้ผู้เกี่ยวข้อง มีความรู้ความเข้าใจถึงวิธีปฏิบัติการสร้างและรวบรวมข้อมูลอย่างถูกต้องตามขั้นตอนที่กำหนด มีการประชุมทบทวนการวิธีปฏิบัติการสร้างข้อมูลและรวบรวมข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบและปรับปรุงระบบที่ใช้ในการให้บริการหรือระบบงานสารสนเทศให้มีความ ทันสมัย มีความปลอดภัยจากภัยคุกคามทางดิจิทัล และเพิ่มมาตรการป้องกันช่องโหว่

๓. ผู้สร้างข้อมูลมีหน้าที่ตรวจสอบการบันทึกข้อมูลตั้งต้นให้ถูกต้อง ครบถ้วน ตรงกับข้อเท็จจริงที่ตรงกับเอกสารต้นฉบับ โดยมีการบันทึกข้อมูลและจัดเก็บตามขั้นตอนการรักษาความปลอดภัย รวมทั้งแจ้งเจ้าของข้อมูลส่วนบุคคลหรือผู้ใช้บริการให้ทราบเหตุผลในการจัดเก็บข้อมูลด้วย นอกจากนี้ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) มีการกำหนดมาตรฐาน แนวปฏิบัติและนโยบายที่เกี่ยวกับการรักษาความเป็นส่วนบุคคลของข้อมูล มีหนังสือให้ความยินยอม (Letter of Consent) เริ่มตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน

๔. กระบวนการเก็บรวบรวมข้อมูลเพื่อการวิจัยให้เก็บข้อมูลเฉพาะประการที่จำเป็นต่อการศึกษาวิจัยหรือสถิติเท่านั้น ข้อมูลที่ไม่จำเป็นหรือไม่สอดคล้องตามวัตถุประสงค์ไม่ควรเก็บรวบรวมมาหรือบันทึกในระบบภายหลัง

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๘ และที่แก้ไข เพิ่มเติม
๔. พระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
๑๐. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)
๑๑. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓
๑๒. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๑๓. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)
๑๔. มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล (Recommendation For Writing Data Management Policy) (มสพร. ๒-๑:๒๕๖๔ และ มสพร. ๒-๒:๒๕๖๔)

หมวดที่ ๓ การจัดเก็บและการสำรองข้อมูล

วัตถุประสงค์

เพื่อให้การจัดเก็บและการสำรองข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารข้อมูลและการให้บริการที่เกี่ยวกับข้อมูลของคณะแพทยศาสตร์เป็นไปตามอำนาจหน้าที่ วัตถุประสงค์ในการดำเนินงานของคณะแพทยศาสตร์และตามที่กฎหมายกำหนด

คำนิยาม

การจัดเก็บข้อมูล (Store) หมายถึง การจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System: DBMS) หรือวิธีการอื่น ๆ

กระบวนการจัดเก็บข้อมูลถาวร (Archive) หมายถึง การคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

การสำรองข้อมูล (Backup) หมายถึง การคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ภายในระยะเวลาที่เหมาะสมด้วยการกู้คืน (Restore)

นโยบาย

๑. ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล กลุ่มบริหารจัดการข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงหน่วยงานที่เกี่ยวข้อง ร่วมกันออกแบบและกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน มีวิธีการจัดก็บรักษาอย่างมั่นคงปลอดภัย และจัดทำข้อมูลอ้างอิง (Reference Data) เพื่อใช้สำหรับการตรวจสอบข้อมูล รวมถึงการกำหนดและออกแบบสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล พร้อมทั้งกำหนดวิธีปฏิบัติการสร้างการจัดเก็บรักษาและการควบคุมคุณภาพข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้องสมบูรณ์และเป็นปัจจุบันอยู่เสมอ โดยมีการจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ จากนั้นให้นำเสนอขออนุญาตผู้บังคับบัญชาองค์กร หรือผู้บังคับบัญชาหน่วยงานที่มีอำนาจตัดสินใจภายใต้ขอบเขต หน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บังคับบัญชาองค์กรแล้วเท่านั้น เพื่อประกาศใช้

๒. จัดประชุม/อบรม/ประชาสัมพันธ์ ให้ผู้เกี่ยวข้องมีความรู้ความเข้าใจถึงวิธีปฏิบัติการจัดเก็บและสำรองข้อมูล และมีทักษะในการใช้เครื่องมือที่ใช้จัดเก็บรักษาข้อมูลอย่างถูกต้องตามขั้นตอนที่กำหนด ชี้แจงให้ผู้ปฏิบัติตระหนักถึงความสำคัญและความจำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูล มีการประชุมทบทวนการจัดระดับชั้นความลับของข้อมูล สิทธิในการเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบและปรับปรุงระบบที่ใช้ในการให้บริการหรือระบบงานสารสนเทศให้มีความทันสมัย มีความปลอดภัยจากภัยคุกคามทางดิจิทัล และเพิ่มมาตรการป้องกันช่องโหว่

๓. ให้ผู้ตรวจสอบคุณภาพข้อมูลในแต่ละหน่วยงานตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บไปแล้ว หากตรวจพบว่าข้อมูลผิด ให้แจ้งผู้ถือสิทธิครอบครองข้อมูลเพื่อปรับปรุงแก้ไขข้อมูลให้ถูกต้องครบถ้วน

๔. การเปลี่ยนแปลงข้อมูลสามารถกระทำได้ หากเป็นการปรับปรุงเปลี่ยนแปลงให้เป็นปัจจุบัน ครบถ้วนถูกต้องเป็นไปเพื่อการควบคุมคุณภาพข้อมูลหรือเหตุผลอื่น ๆ ซึ่งเป็นประโยชน์ตามประกาศฉบับนี้

๕. ให้กลุ่มบริหารจัดการข้อมูลและบริการข้อมูลด้านเทคนิคกำหนดสิทธิการเข้าถึงระบบและโปรแกรม โดยวิธีการใด ๆ ที่เป็นไปตามขั้นตอนการดำเนินงานตามที่ผู้ถือสิทธิครอบครองข้อมูลกำหนด โดยไม่ขัดต่อหลักกฎหมายที่ประกาศใช้อยู่ในขณะนั้น

๖. ผู้ดูแลข้อมูลและผู้ดูแลระบบสารสนเทศร่วมกัน กำหนดวิธีและขั้นตอนการสำรองและกู้คืนข้อมูลตามมาตรฐานสากลเพื่อให้องค์กรสามารถใช้ข้อมูลได้ภายในระยะเวลาที่เหมาะสมเมื่อมีความจำเป็นต้องกู้คืน

แนวทาง

๑. แนวปฏิบัตินี้หมายความรวมถึงการจัดเก็บข้อมูลทั้งที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจะเป็นไฟล์ข้อมูลธรรมดา (Plain File) ไฟล์ข้อมูลที่มีการเข้ารหัส (Encryption File) ไฟล์ข้อมูลที่ผ่านการประมวลผล (Information File) หรือไฟล์ข้อมูลรูปแบบอื่น ๆ

๒. ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัด ต้องจัดเก็บข้อมูล ให้ถูกต้องเหมาะสมตามระดับการเปิดเผยข้อมูลตามหมวดหมู่ของข้อมูลคณะแพทยศาสตร์โดยคณะแพทยศาสตร์

๓. การจัดเก็บไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

- ผู้ถือสิทธิครอบครองข้อมูล หรือผู้สร้างข้อมูลต้องกำหนดและตรวจสอบความถูกต้องของการกำหนดสิทธิการเข้าถึงข้อมูล
- ต้องแจกแจงประเภทของข้อมูลตามลำดับชั้นความลับ รวมถึงกำหนดผู้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานอย่างเหมาะสม และในกรณีจำเป็นที่ต้องมีการจำกัดการเข้าถึงข้อมูลลับให้แก่บุคคลผู้ที่มีหน้าที่เกี่ยวข้อง ให้จัดทำรายชื่อผู้ได้รับอนุญาตให้เข้าถึงดังกล่าวอย่างรอบคอบ
- เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดีไม่ให้เกิดความเสียหาย
- ต้องมีวิธีการป้องกันไฟล์ข้อมูลที่เป็นความลับด้วยวิธีที่ที่เหมาะสม เช่น กรณีที่มีการจัดเก็บไว้ในระบบคอมพิวเตอร์ ระบบคอมพิวเตอร์นั้นต้องมีการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยเพียงพอ หรือใช้วิธีการป้องกันอื่น ๆ เพื่อมิให้ข้อมูลถูกใช้งานได้โดยมิได้รับอนุญาต เช่น การเข้ารหัส (Encryption) เป็นต้น
- รหัสผ่านถือเป็นข้อมูลลับและเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านให้มีความมั่นคงปลอดภัย

๔. ผู้ถือสิทธิครอบครองข้อมูล กลุ่มบริหารจัดการข้อมูลและผู้ใช้ข้อมูลภายในคณะแพทยศาสตร์จะต้องตรวจสอบมาตรการความปลอดภัยที่มีประสิทธิภาพอย่างสม่ำเสมอ อย่างน้อยดังนี้

- มาตรการความปลอดภัย จะต้องปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งาน การเปลี่ยนแปลง การเปิดเผย การถูกกำจัดหรือความเสี่ยงอื่น ๆ ไม่ว่าจะตั้งใจหรือไม่ก็ตาม
- ผู้ใช้งานข้อมูลในจะต้องปฏิบัติตามขั้นตอนการรักษาความปลอดภัยเพิ่มเติมทั้งหมดที่กำหนดโดยผู้ถือสิทธิครอบครองข้อมูลสำหรับข้อมูลชุดนั้น ๆ
- ผู้ใช้งานข้อมูลภายในคณะแพทยศาสตร์จะต้องประเมินความต้องการ และความเกี่ยวข้องของข้อมูลที่ได้รับและทำลายข้อมูลเมื่อไม่มีการใช้งานอีกต่อไปหรือสิ้นสุดระยะเวลาการข้อใช้งาน
- ในกรณีที่มีเหตุรั่วไหลของข้อมูล หรือการดำเนินการซึ่งอาจเป็นความเสี่ยงต่อคณะแพทยศาสตร์หรือเห็นว่าขัดต่อกฎหมายที่เกี่ยวข้อง ผู้พบเห็นจะต้องรายงานการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หรือ

การสูญหายของข้อมูลต่อกลุ่มบริกรข้อมูลของคณะแพทยศาสตร์ โดยทันทีที่พบเหตุ เพื่อดำเนินการแก้ไขได้อย่างเหมาะสมและทันท่วงที

๕. กลุ่มบริการข้อมูลมีการติดตามตรวจสอบและประเมินผลการปฏิบัติการดูแลรักษาความมั่นคงปลอดภัยข้อมูลอย่างสม่ำเสมอและมีแนวทางการจัดการในกรณีที่เกิดความเสียหายจากภัยพิบัติภัยคุกคามหรือการละเมิดข้อมูลที่อาจเกิดขึ้นทั้งจากภายในและภายนอก

๖. มีการดำเนินการซักซ้อนแผนการสำรองและกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติลิขสิทธิ์พ.ศ. ๒๕๓๘ และที่แก้ไข เพิ่มเติม
๔. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
๑๐. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)
๑๑. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓
๑๒. มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (มรด. ๖:๒๕๖๖
๑๓. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๑๔. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)

หมวดที่ ๔ การจัดหมวดและการทำบัญชีข้อมูล

วัตถุประสงค์

เพื่อให้การจัดหมวดและการทำบัญชีข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารข้อมูลและการให้บริการที่เกี่ยวกับข้อมูลของคณะแพทยศาสตร์เป็นไปตามอำนาจหน้าที่ วัตถุประสงค์ในการดำเนินงานของคณะแพทยศาสตร์ และตามที่กฎหมายกำหนด ให้เป็นระบบสารสนเทศสำหรับการสืบค้นข้อมูลที่ช่วยให้ผู้ใช้สามารถสืบค้น ร้องขอ เข้าถึง และใช้ประโยชน์ข้อมูลอย่างเป็นรูปธรรม เพื่อให้หน่วยงานเกิดการสร้างวัฒนธรรมขับเคลื่อนด้วยข้อมูล (Data Driven)

คำนิยาม

บัญชีข้อมูล (Data Catalog) หมายถึง เอกสารแสดงรายการของชุดข้อมูลในความครอบครองหรือควบคุมของหน่วยงานคณะแพทยศาสตร์ ที่มีการจำแนก จัดกลุ่ม หรือจัดประเภทข้อมูลอย่างเป็นระบบ

การจัดหมวดหมู่ (Data Classification) หมายถึง การกำหนดสิทธิการเข้าถึงและการนำข้อมูลไปใช้ได้อย่างเหมาะสมตามหมวดหมู่และชั้นความลับของข้อมูล ที่กำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานคณะแพทยศาสตร์และความมั่นคงของประเทศ ซึ่งจะเป็นประโยชน์ในการกำหนดมาตรการรักษาความปลอดภัยของข้อมูล รวมถึงการอนุญาตให้สามารถทำการแลกเปลี่ยนหรือเปิดเผยข้อมูลได้ โดยกำหนดไว้ ๕ หมวดหมู่ ดังนี้

๑. ข้อมูลสาธารณะ
๒. ข้อมูลเปิดภายในคณะแพทยศาสตร์
๓. ข้อมูลที่ต้องได้รับอนุญาตจากคณะกรรมการธรรมาภิบาลข้อมูลคณะแพทยศาสตร์
๔. ข้อมูลที่ต้องได้รับอนุญาตจากหน่วยงานภายนอก
๕. ข้อมูลปกปิด

หมวดหมู่ข้อมูลของคณะแพทยศาสตร์	ระดับชั้นข้อมูล	คำอธิบาย
ข้อมูลสาธารณะ	ชั้นเปิดเผย (Open)	ชุดข้อมูลที่อนุญาตให้ผู้ใช้งานทั้งภายในและภายนอกคณะแพทยศาสตร์ สามารถเปิดเผยได้ให้เข้าถึงและใช้งานได้
ข้อมูลเปิดภายในคณะแพทยศาสตร์	ชั้นเผยแพร่ภายในองค์กร (Private)	ชุดข้อมูลที่อนุญาตให้เฉพาะผู้ใช้งานภายในคณะแพทยศาสตร์ สามารถเข้าถึงและใช้งานในภารกิจการดำเนินกิจการภายในของคณะแพทยศาสตร์
ข้อมูลที่ต้องได้รับอนุญาตจากคณะกรรมการธรรมาภิบาลข้อมูลคณะแพทยศาสตร์	ชั้นลับ (Confidential) หรือชั้นลับมาก (Secret)	ชุดข้อมูลที่ผู้ถือสิทธิครอบครองข้อมูลพิจารณาแล้วว่าจำเป็นต้องมีการอนุมัติผ่านคณะกรรมการธรรมาภิบาลข้อมูลคณะแพทยศาสตร์ ทั้งนี้การเปิดเผยจะต้องคำนึงถึงเงื่อนไข ชั้นความลับ ความมั่นคงปลอดภัย และข้อมูลส่วนบุคคลตามนโยบายและแนวปฏิบัติที่เกี่ยวข้อง

ข้อมูลที่ต้องได้รับอนุญาตจากหน่วยงานภายนอก	ชั้นเปิดเผย (Open) หรือ ชั้นลับ (Confidential) หรือ ชั้นลับมาก (Secret)	ชุดข้อมูลที่ได้รับจากหน่วยงานภายนอกคณะแพทยศาสตร์ เพื่อนำมาใช้ในการดำเนินการตามภารกิจของคณะแพทยศาสตร์ การอนุมัติให้ใช้งานต่อจะต้องมั่นใจว่าได้รับอนุญาตจากบุคคลหรือหน่วยงานที่มีข้อมูลที่เป็นหน่วยงานภายนอก และการเปิดเผยจะต้องคำนึงถึงเงื่อนไขชั้นความลับ ความมั่นคงปลอดภัย และข้อมูลส่วนบุคคลตามนโยบายและแนวปฏิบัติที่เกี่ยวข้อง
ข้อมูลปกปิด	ชั้นลับที่สุด (Top Secret)	ชุดข้อมูลที่ไม่อนุญาตให้เปิดเผยทั้งภายในและภายนอกคณะแพทยศาสตร์ ทั้งนี้จะได้รับสิทธิเฉพาะเจ้าของข้อมูลส่วนบุคคล ผู้ถือสิทธิครอบครองข้อมูล ตลอดทั้งกลุ่มบริกรข้อมูล และคณะกรรมการธรรมาภิบาลข้อมูลคณะแพทยศาสตร์เท่านั้น

ระดับชั้นข้อมูล (Data Classification Level) หมายถึง ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็นชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้นลับ (Confidential) ลับมาก (Secret) และลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลความลับทางราชการตามระเบียบการรักษาความลับทางราชการ

ระบบบัญชีข้อมูล หมายถึง ระบบโปรแกรมประยุกต์ที่ทำหน้าที่บริหารจัดการบัญชีข้อมูลของหน่วยงาน โดยมีความสามารถในการจัดการชุดข้อมูล คำอธิบายข้อมูล สามารถค้นหาข้อมูล และอาจมีความสามารถ Application Program Interface (API) สำหรับการเชื่อมต่อกับระบบอื่น ๆ

ชุดข้อมูล (Data Set) หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata) หมายถึง ข้อมูลที่ใช้กำกับและอธิบายชุดข้อมูลหรือกลุ่มข้อมูลอื่น ให้รายละเอียดเกี่ยวกับชุดข้อมูล ข้อจำกัด แหล่งข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้ผู้ใช้งานสามารถเข้าใจข้อมูลและทำงานได้ดีมีประสิทธิภาพมากขึ้น โดยการบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่การเก็บรวมรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา ทั้งนี้ข้อมูลทุกชุดควรมีเมทาดาตาประกอบ เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูลเบื้องต้น โดยที่เมทาดาตาแบ่งออกเป็น ๒ กลุ่ม ดังนี้

๑. เมทาดาตาเชิงธุรกิจ (Business Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Data Set) ในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) เช่น ชื่อข้อมูล คำสำคัญ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ คำอธิบายเบื้องต้น จัดประสงค์ข้อมูล เป็นต้น
๒. เมทาดาตาเชิงเทคนิค (Technical Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Data Set) ในด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการ

ฐานข้อมูล (Database Administrator) เช่น ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น ๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) เป็นต้น

คลังเมทาดาตา หรือพจนานุกรมข้อมูล (Metadata Repository หรือ Data Dictionary) หมายถึง เครื่องมือในการรวบรวมและจัดเก็บเมทาดาตา เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถค้นหาและเข้าถึงได้โดยสะดวก อย่างไรก็ตามผู้ที่มีสิทธิในการเข้าถึง ควรได้รับสิทธิ์ที่แตกต่างกันขึ้นอยู่กับบทบาทและความรับผิดชอบ เช่น ผู้ใช้งานข้อมูลทั่วไปสามารถเข้าถึงได้เฉพาะเมทาดาตาเชิงธุรกิจ ขณะที่บริกรข้อมูลสามารถเข้าถึงได้ทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค

แนวทาง

๑.บริกรข้อมูล (Data Steward) และนักวิเคราะห์ข้อมูล (Data Analyst) กับหน่วยงานที่เกี่ยวข้องต้องร่วมกันกำหนดมาตรฐานของคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาและคู่มือแนวปฏิบัติมาตรการการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา เช่น พจนานุกรมข้อมูล (Data Dictionary) การตั้งชื่อข้อมูล (Data Naming Convention) เป็นต้น โดยทำรายการข้อมูลประเภทต่าง ๆ ที่มีอยู่ในหน่วยงานและการใช้งาน จากนั้นระบุหมวดหมู่ข้อมูลตามเกณฑ์ที่กำหนด ตามนโยบายและกฎระเบียบของคณะแพทย์

๒. ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้องและให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้

- การเลือกชุดข้อมูลเพื่อจัดทำบัญชีข้อมูลให้สอดคล้องกับภารกิจหน่วยงาน มีเกณฑ์ที่ชัดเจนในการกำหนดระดับความสำคัญของชุดข้อมูลที่จำเป็นสำหรับการวางแผน การปฏิบัติงาน และการให้บริการของคณะแพทยศาสตร์ เช่น ข้อมูลที่ใช้ตอบยุทธศาสตร์ (Strategic) และตัวชี้วัด (KPI) ของหน่วยงาน ข้อมูลที่ใช้ในรายงานที่หน่วยงานต้องจัดทำเป็นประจำ (Critical) ข้อมูลที่ใช้เพื่อการให้บริการประชาชน และข้อมูลที่ต้องใช้หรือแบ่งปัน (Shared Data) ระหว่างหน่วยงานเพื่อตอบสนองนโยบาย จึงได้กำหนดเกณฑ์เพื่อใช้เป็นฐานการเลือกชุดข้อมูลดังนี้
    ๑. ลดความเสี่ยงที่เกิดการละเมิดกฎหมายเช่นข้อมูลส่วนบุคคลข้อมูลที่เป็นความลับ
    ๒. สนับสนุนตอบโจทย์ของประเทศ ตอบเกณฑ์ที่ต้องถูกประเมินจากหน่วยงานภายนอก
    ๓. นำมาใช้ปรับปรุงกระบวนการทำงานเดิมให้เกิดประสิทธิภาพ (Process Improvement)
- ข้อมูลที่นำมาจัดทำชุดข้อมูล เป็นได้ทั้งข้อมูลหลัก (Master Data) ซึ่งเป็นข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของคณะแพทยศาสตร์ เช่น ข้อมูลพนักงาน ข้อมูลผู้ป่วย ข้อมูลครุภัณฑ์ ข้อมูลสถานที่ หรือข้อมูลอ้างอิง (Reference Data) ที่เป็นข้อมูลที่เป็นสากล มีการกำหนดให้เป็นมาตรฐาน และใช้งานร่วมกัน มีการเปลี่ยนแปลงค่อนข้างน้อย ((*DCMI: DCMI Metadata Terms*, n.d.; *ISO/IEC ๑๑๑๗๙-๑:๒๐๒๓ - Information Technology — Metadata Registries (MDR) — Part ๑: Framework*, n.d.)
- จัดทำมาตรฐานชุดข้อมูล (Data Set Standard) หมายถึงการกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล กำหนดเมทาดาตาขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูลที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึง

องค์ประกอบของฟิลด์ข้อมูล เช่น ชื่อฟิลด์ข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ วันที่) การกำหนดใช้ ค.ศ. หรือ พ.ศ. ในการบันทึกข้อมูล เป็นต้น

- การประเมินผลกระทบและภารกิจของหน่วยงาน เพื่อกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล
- ดำเนินการติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Data Set) เมื่อได้รับการประเมินและระบุหมวดหมู่อย่างเหมาะสม โดยอาจติดป้ายกำกับสำรองสำหรับการระบุชั้นความลับของข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลที่ใช้ภายในหน่วยงาน หรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ
- การดำเนินการกับชุดข้อมูล (Data Handling) กับชุดข้อมูลที่ได้รับการจัดหมวดหมู่และชั้นความลับแล้ว ควรได้รับการจัดการตามแนวทางที่เหมาะสม รวมถึงคำนึงถึงการรักษาความปลอดภัยตามหมวดหมู่ ซึ่งขั้นตอนนี้ควรทำตามมาตรฐานการปฏิบัติงาน แต่สามารถปรับตามการเปลี่ยนแปลงเทคโนโลยี ความเหมาะสมและบริบทนั้น ๆ ได้
- กำกับติดตามอย่างต่อเนื่อง โดยตรวจสอบความทันสมัย และสิทธิของการเข้าถึงข้อมูล โดยสามารถทำได้ผ่านเครื่องมือหรือกระบวนการอัตโนมัติ หรือดำเนินการด้วยตนเอง ทั้งนี้ต้องอยู่ภายใต้การกำกับดูแลหรือระเบียบการทำงานของหน่วยงานที่สังกัด

เอกสารที่เกี่ยวข้อง

๑. รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ ในมาตราที่ ๕๙ ได้ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ
๒. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒
๓. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๕. พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.๒๕๖๒
๖. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๗. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)
๘. มรด. ๓-๑: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (Government Data Catalog Guideline)
๙. มรด. ๓-๒: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ (Government Data Catalog Registration Guideline)
๑๐. มรด. ๔-๑: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Policy)
๑๑. มรด. ๔-๒: ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline)

๑๒. มสพร. ๘-๒๕๖๕ มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework)
๑๓. มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (มรด. ๖:๒๕๖๖)
๑๔. มาตรฐาน มสพร. X-๒๕๖๕ ว่าด้วยร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ
๑๕. DCMI: DCMI Metadata Terms. (n. d.). Retrieved February ๑๔, ๒๐๒๔, from https://www.dublincore.org/specifications/dublin-core/dcmi-terms/
๑๖. ISO/IEC ๑๑๑๗๙-๑:๒๐๒๓ - Information technology — Metadata registries (MDR) — Part ๑: Framework. (n. d.). Retrieved February ๑๔, ๒๐๒๔, from https://www.iso.org/standard/78914.html

หมวดที่ ๕ การประมวลผลและการใช้ข้อมูล

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการขอใช้งาน รวมถึงการกำหนดวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก

คำนิยาม

การประมวลผลข้อมูล (Data Processing) หมายถึง การเปลี่ยนแปลงหรือจัดระเบียบข้อมูลให้อยู่ในรูปแบบที่เป็นประโยชน์ต่อผู้ใช้งาน

กระบวนการใช้ข้อมูล (Use) หมายถึง การนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์

นโยบาย

๑. ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล กลุ่มบริหารจัดการข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงหน่วยงานที่เกี่ยวข้อง ร่วมกันกำหนดวิธีปฏิบัติการประมวลผลและการใช้ข้อมูล จากนั้นให้นำเสนอขออนุมัติผู้บังคับบัญชาองค์กร หรือผู้บังคับบัญชาหน่วยงานที่มีอำนาจตัดสินใจ ภายใต้ขอบเขตหน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บังคับบัญชาองค์กรแล้วเท่านั้น เพื่อประกาศใช้

๒. มีการกำหนดแนวทางการขอสิทธิ์ในการใช้ข้อมูลที่ชัดเจน ผู้ใช้งานข้อมูลต้องขออนุมัติจากเจ้าของข้อมูลส่วนบุคคล หรือผู้ถือสิทธิครอบครองข้อมูล หรือกลุ่มบริหารจัดการข้อมูล ในการเข้าถึงข้อมูลที่เป็นความลับ ซึ่งในคำร้องขอการเข้าถึงข้อมูลของผู้ใช้งานข้อมูลนั้นจะรวมถึง ๑) ขอบเขตและความละเอียดของข้อมูลที่ร้องขอ เช่น ช่วงเวลาที่ต้องการใช้ข้อมูล ๒) วัตถุประสงค์ในการร้องขอข้อมูล ๓) ความถี่ในการเข้าใช้งานข้อมูล เช่น เป็นครั้งคราวหรือเป็นประจำ โดยมีการทบทวนสิทธิ์อย่างสม่ำเสมอ

๓. หน่วยงานผู้ใช้ข้อมูล ต้องประมวลผลและใช้ข้อมูลให้ตรงตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคลและผู้ถือสิทธิครอบครองข้อมูลแล้วเท่านั้น หากหน่วยงานผู้ใช้ข้อมูลต้องการประมวลผลหรือใช้ข้อมูลเพื่อวัตถุประสงค์อื่น ที่นอกเหนือไปจากวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคลและผู้ถือสิทธิครอบครองข้อมูล ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและผู้ถือสิทธิครอบครองข้อมูลก่อนเสมอ ผู้ใช้งานข้อมูลจะต้องไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจากแหล่งข้อมูล เว้นแต่จะได้รับอนุญาตหรือเป็นไปตามที่กฎหมายกำหนด หรือข้อมูลนั้น ๆ ได้รับอนุมัติล่วงหน้าไว้แล้ว เพื่อคงไว้ซึ่งวัตถุประสงค์การใช้งานข้อมูลดังกล่าว

๔. ผู้ดูแลข้อมูลและผู้ดูแลระบบสารสนเทศร่วมกันจัดทำระบบสำหรับการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) ของผู้ใช้ข้อมูล

๕. ผู้ดูแลข้อมูลและผู้ดูแลระบบสารสนเทศ ร่วมกันจัดทำวิธีป้องกันมิเกิดการแก้ไขบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) ได้

๖. ผู้ดูแลข้อมูลและผู้ดูแลระบบสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้อง ร่วมกันจัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ที่สามารถใช้งานได้ตามวัตถุประสงค์ของคณะแพทยศาสตร์

๗. ดำเนินการให้มีช่องทางในการขอสิทธิ์และเข้าถึงข้อมูลและเข้าถึงข้อมูล ภายใต้กรอบการกำกับดูแลที่เหมาะสม

๘. อำนวยความสะดวกให้กลุ่มบริหารจัดการข้อมูลสามารถติดตาม ป้องกัน และควบคุมความเสี่ยงการรั่วไหลของข้อมูลหรือใช้ไม่ตรงตามวัตถุประสงค์

๙. กลุ่มบริหารจัดการข้อมูลจะต้องมีช่องทางสื่อสารกับผู้ใช้งานข้อมูลและสามารถตอบสนองต่อการร้องขอการเข้าถึงข้อมูลภายในระยะเวลาที่เหมาะสม

แนวทาง

๑. ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศและหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้

- ต้องปฏิบัติตามขั้นตอนการประมวลผลข้อมูลและการใช้ข้อมูลที่กำหนดขึ้น และกำหนดสิทธิ์การใช้งานระบบสารสนเทศตามความจำเป็น
- กรณีข้อมูลมีการควบคุมโดยการเข้ารหัส (Encryption) ในการประมวลผลข้อมูล เจ้าของข้อมูลต้องบันทึกหลักฐานการเข้าถึงจากผู้ใช้งานไว้ทุกครั้ง เพื่อการตรวจสอบและสามารถรายงานเพื่อการตรวจสอบได้ในภายหลัง
- ต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่ได้กำหนดชั้นข้อมูลตั้งแต่ลับขึ้นไปอย่างเหมาะสม
- ให้ใช้ข้อมูลทั้งที่มีอยู่ภายในหน่วยงาน หรือได้รับข้อมูลจากภายนอกหน่วยงานตามจุดประสงค์การขอใช้งานเท่านั้น
- ใช้ข้อมูลเฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิจากกลุ่มบริหารจัดการข้อมูลเท่านั้น
- กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิผู้ใช้งาน สิทธิในการเข้าถึง การยืนยันตัวตน และระยะเวลาที่นำข้อมูลไปใช้งานเสมอ
- ห้ามมิให้ใช้ข้อมูลเพื่อประโยชน์อื่นใดนอกเหนือจากที่ได้ขออนุญาต หรือใช้ข้อมูลเพื่อจุดประสงค์อันอาจก่อให้เกิดความเสียหายต่อหน่วยงานและคณะแพทยศาสตร์
- เจ้าของข้อมูลส่วนบุคคลและผู้ถือสิทธิครอบครองข้อมูลมีสิทธิ์ทักท้วงคำร้องขอการใช้ข้อมูลจากผู้ใช้งานข้อมูลภายในคณะแพทยศาสตร์ ในกรณีดังต่อไปนี้ ๑) ข้อมูลนั้นมีชั้นความลับ ๒) การร้องขอข้อมูลของผู้ใช้งานไม่มีเหตุผลที่ชอบธรรมหรือไม่สมเหตุสมผล ๓) การแบ่งปันข้อมูลเป็นสิ่งต้องห้ามอย่างชัดแจ้งตามกฎหมายหรือข้อตกลงการได้มาของข้อมูล
- หากผู้ร้องขอใช้ข้อมูลไม่สามารถเข้าถึงข้อมูลที่ร้องขอได้ สามารถส่งผ่านคำขอไปยังกลุ่มบริกรข้อมูลเพื่อดำเนินการในชั้นคณะกรรมการธรรมาภิบาลข้อมูลต่อไป

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม

๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการ ในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (มรด. ๖:๒๕๖๖
๑๐. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๑๑. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)

หมวดที่ ๖ การเข้ารหัสและการป้องกันข้อมูล

วัตถุประสงค์

เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล เป็นไปอย่างมีระบบและมาตรฐาน สามารถปกป้องความลับ รักษาความเป็นส่วนตัว เป็นไปตามวัตถุประสงค์การใช้งาน และรักษาความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholder)

คำนิยาม

การเข้ารหัสข้อมูล (Data Encryption) หมายถึง การแปลข้อมูลเป็นรูปแบบอื่น หรือรหัสเพื่อให้เฉพาะผู้ที่มีสิทธิ์เข้าถึงคีย์ลับ (เรียกอย่างเป็นทางการว่าคีย์ถอดรหัส) หรือรหัสผ่านเท่านั้นที่สามารถอ่านข้อมูลได้ โดยอาจเป็นการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) หรือแบบสมมาตร (Symmetric Encryption) ก็ได้

การป้องกันข้อมูล (Data Protection) หมายถึงกระบวนการ/การกระทำเพื่อให้มั่นใจได้ว่าผู้ที่ได้รับอนุญาตเท่านั้นถึงจะเข้าถึงข้อมูลนั้น ๆ ได้

การรักษาความปลอดภัยทางไซเบอร์ หมายถึง แนวปฏิบัติในการปกป้องคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์แอปพลิเคชัน ระบบที่สำคัญและข้อมูล จากภัยคุกคามทางดิจิทัลที่อาจเกิดขึ้นได้ โดยใช้มาตรการและเครื่องมืออย่างเหมาะสม

แนวทาง

๑. คณะกรรมการธรรมาภิบาลคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ มีหน้าที่
- สร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับจ้าง และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงข้อมูลทางสารสนเทศอย่างสม่ำเสมอ
- จัดให้มีเนื้อหาความปลอดภัยของข้อมูลและธรรมาภิบาลข้อมูลในการอบรมพนักงานใหม่
- ทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง ๑ ครั้ง

๒. หน่วยงานต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้องโดยเคร่งครัดในประเด็นดังต่อไปนี้
- วางโครงสร้างในการจัดระเบียบการใช้งานข้อมูลของหน่วยงาน โดยการกำหนด Access Control ให้เหมาะสม เช่น การใช้ Principle of Least Privilege
- มีแนวปฏิบัติในการกำกับดูแลข้อมูลโดยการเข้ารหัสและ/หรือการป้องกันข้อมูลให้เหมาะสมตามการจัดหมวดหมู่ (Data Classification) ของคณะแพทย์ฯ และจัดให้มีมาตรการกับข้อมูลในสถานะดังต่อไปนี้

(๑) ขณะที่ข้อมูลถูกจัดเก็บ ต้องมีการเลือกใช้ประเภทของสื่อในการจัดเก็บที่เหมาะสม มีการกำหนดสิทธิการเข้าถึงและมีการทบทวนสิทธิอย่างสม่ำเสมอ

(๒) ขณะที่ข้อมูลถูกส่งผ่านหรือส่งต่อ ต้องมีการเลือกใช้ช่องทางหรือวิธีการที่เหมาะสม หากเป็นการส่งผ่านโดยวิธีการฝากไฟล์หรือเปิดให้มีช่องทางที่ให้ผู้อื่นเข้ามาใช้งานต้องมีการกำหนดวันที่สิ้นสุดของสิทธิการใช้งานนั้น ๆ เสมอ และต้องมีการคำนึงถึงกรณีที่ถูกเข้าถึง

ระหว่างการส่งผ่านโดยผู้ที่ได้ไม่ได้รับอนุญาตเสมอ เช่น การส่งผ่านโดยใช้ Physical Storage เป็นสื่อการ ควรมีการเข้ารหัสข้อมูลก่อนการขนส่ง เป็นต้น

(๓) ขณะที่ข้อมูลถูกใช้งาน ต้องเป็นไปตามข้อกำหนดการขอใช้งาน โดยจะมีการส่งผ่านข้อมูลหรืออนุญาตให้ผู้อื่นเข้าถึงโดยเด็ดขาด กรณีที่ข้อมูลเป็นข้อมูลในกลุ่มชั้นความลับ ต้องมีการดำเนินมาตรฐานป้องกันที่เหมาะสมในขณะที่ข้อมูลถูกใช้งานในระบบคอมพิวเตอร์นั้น ๆ เสมอ

- กรณีที่การดำเนินการจำเป็นต้องเกี่ยวข้องกับบุคคล หรือกลุ่มบุคคล หรือส่วนงานที่สาม ที่อยู่นอกเหนือจากเจ้าของข้อมูลและผู้ขอใช้ข้อมูลแล้ว ถือให้เป็นความรับผิดชอบของผู้ขอใช้ข้อมูล โดยผู้ขอใช้ข้อมูลมีหน้าที่ควบคุม บันทึก และกำหนดวิธีการในการเข้าถึงข้อมูลอย่างเหมาะสม เช่น กรณีที่ต้องดำเนินการกับหน่วยงานอื่น ๆ จากภายนอก เป็นต้น
- หลีกเลี่ยงดำเนินการใด ๆ กับข้อมูลชั้นความลับบนเครื่องมือ หรือระบบปฏิบัติ หรือโปรแกรมที่สิ้นสุดระยะเวลาสนับสนุนความปลอดภัยจากผู้ผลิตไปแล้ว

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to Protect the Personally Identifiable Information)
๔. พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.๒๕๖๒
๕. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม
๖. แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคลและสถานที่ ที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒
๗. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒
๘. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๙. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕
๑๐. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

หมวดที่ ๗ การจัดทำข้อมูลนิรนาม (Data Anonymization)

วัตถุประสงค์

เพื่อให้เกิดการประยุกต์ใช้แนวทางการจัดทำข้อมูลนิรนามในการลดความเสี่ยงในการเผยแพร่ข้อมูลที่เข้าข่ายข้อมูลที่มีความอ่อนไหว โดยเฉพาะอย่างยิ่งในการเผยแพร่ข้อมูลแบบเปิด

คำนิยาม

การจัดทำข้อมูลนิรนาม (Data Anonymization) หมายถึง กระบวนการที่ทำให้ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ โดยในประกาศนี้มีจุดประสงค์ด้านการคุ้มครองข้อมูลส่วนบุคคล

การขจัดตัวตน (Data De-identification) หมายถึง กระบวนการหรือขั้นตอนวิธีการใด ๆ ที่กระทำกับส่วนใดส่วนหนึ่งของข้อมูล เพื่อการป้องกันไม่ให้เกิดการย้อนรอยเพื่อระบุตัวตน (Re-identification) ของเจ้าของข้อมูลที่ผ่านการทำการจัดทำข้อมูลนิรนามได้

การทำให้คละ (Randomization) หมายถึง กระบวนการหรือขั้นตอนวิธีการใด ๆ ที่กระทำการกับข้อมูลให้มีลักษณะคละเคล้าและเปลี่ยนไปจากข้อมูลเดิม โดยจุดประสงค์เพื่อตัดความสัมพันธ์ระหว่างบุคคลกับชิ้นข้อมูลโดยไม่ทำให้เสียคุณค่าข้อมูล ตัวอย่างเทคนิคในกลุ่มการทำให้คละ เช่น การเพิ่มตัวเลขรบกวน (Noise Addition), การสับเปลี่ยนใหม่ (Permutation) และเทคนิคความเป็นส่วนตัวที่แตกต่างกัน (Differential Privacy)

การปิดทับข้อมูล (Masking) หมายถึง กระบวนการหรือขั้นตอนวิธีการใด ๆ ที่กระทำการกับข้อมูลโดยการเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูลออกไป

การลดความชัดเจนของข้อมูล (Blurring or Noising) หมายถึง การใช้ข้อมูลโดยประมาณแทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง เช่น การเผยแพร่เพียงเลข 4 หลักท้ายของหมายเลขโทรศัพท์

การแฝงข้อมูล (Pseudonymization) หมายถึง กระบวนการหรือขั้นตอนวิธีการใด ๆ ในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรงด้วยข้อมูลแฝงที่สร้างขึ้นมา

การทำข้อมูลหยาบ (Coarsening) หมายถึง กระบวนการหรือขั้นตอนวิธีการใด ๆ ในการทำให้ข้อมูลขาดหายไปและถูกปกปิดมากขึ้น เช่น การทำให้เป็นสามัญ (Generalization) ที่ลดความละเอียดของชั้นข้อมูลเพื่อให้ข้อมูลสูญเสียความเฉพาะเจาะจง เช่น การลดความละเอียดจากตำบลเป็นอำเภอ หรือจากจังหวัดเชียงใหม่เป็นภาคเหนือ เป็นต้น

นโยบาย

ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้

๑. ต้องมีการกำหนดแนวปฏิบัติในการการจัดทำข้อมูลนิรนามตามมาตรฐานและความเหมาะสม โดยคำนึงถึงลักษณะของข้อมูล รูปแบบวิธีการใช้ข้อมูล และบริบทการใช้งานประกอบด้วย
๒. ข้อมูลที่มีความสำคัญ หรือมีเข้าข่ายเป็นข้อมูลที่มีความอ่อนไหว หรือชั้นความลับ จำเป็นต้องมีการพิจารณาการจัดทำข้อมูลนิรนามอย่างเพียงพอ ตามดุลยพินิจของคณะกรรมการธรรมาภิบาลข้อมูล หรือส่วนงานที่ได้รับมอบหมาย

แนวทาง

๑. มีการกำหนดแนวปฏิบัติการจัดทำข้อมูลนิรนามที่ชัดเจน โดยอาจระบุวิธีการหรือเครื่องมือที่ใช้ อาทิ การขจัดตัวตน การทำให้คละ การทำให้เป็นสามัญ การปิดทับข้อมูล การลดความชัดเจนของข้อมูล การแฝงข้อมูล หรือการทำข้อมูลหยาบ เป็นต้น
๒. มีการทำให้ข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหวนั้นกลายเป็นข้อมูลนิรนาม เมื่อสามารถทำได้ โดยที่ยังคงรักษาประโยชน์ของข้อมูลในการวิเคราะห์ในระดับที่เหมาะสม
๓. หน่วยงานมีการทบทวนแนวปฏิบัติการจัดทำข้อมูลนิรนามตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ ๑ ครั้ง

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๓. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๔. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๕. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)
๖. ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑
๗. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)

หมวดที่ ๘ การควบคุมการเข้าถึงข้อมูล (Data Access Control)

วัตถุประสงค์

๑. เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่เกี่ยวข้องกับการควบคุมการเข้าถึงและการบันทึกการเข้าถึงข้อมูล
๒. เพื่อให้ผู้มีส่วนร่วมและส่วนงานสามารถปฏิบัติตามแนวทางปฏิบัติในการควบคุมการเข้าถึงข้อมูล

คำนิยาม

๑. การควบคุมการเข้าถึงข้อมูล หมายถึง วิธีการใด ๆ เพื่อจำกัดสิทธิการใช้งานทั้งอ่าน เขียน และประมวลผลข้อมูลของบุคคล หรือกลุ่มบุคคล หรือส่วนงาน ให้มีความรัดกุมมากที่สุดแต่ยังสามารถปฏิบัติงานได้อย่างมีประสิทธิผลและประสิทธิภาพ เช่น หลัก Principle of Least Privilege เป็นต้น
๒. บันทึกการเข้าถึงข้อมูล หมายถึง บันทึกที่สามารถบันทึกได้ว่าบุคคล หรือกลุ่มบุคคล หรือหน่วยงานได้มีการดำเนินการกับข้อมูลใด ณ เวลาใด หรือสิ่งอื่นใดที่เทียบกับบันทึกข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติคอมพิวเตอร์ พ.ศ. ๒๕๖๔

นโยบาย

ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัด ในประเด็นดังต่อไปนี้

๑. ผู้ถือสิทธิครอบครองข้อมูล กลุ่มบริหารจัดการข้อมูล และผู้ใช้ข้อมูลภายในคณะแพทยศาสตร์ จะต้องตรวจสอบมาตรการความปลอดภัยที่มีประสิทธิภาพอย่างสม่ำเสมอในด้านการปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตอย่างชัดเจน
๒. ส่วนงานต้องจัดให้มีการควบคุมการเข้าถึงอย่างเพียงพอและเหมาะสม
๓. กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิผู้ใช้งานและสิทธิในการเข้าถึง โดยอ้างอิงจากระยะเวลาที่นำข้อมูลไปใช้งานและวัตถุประสงค์ในการใช้งานข้อมูล โดยต้องมีการยืนยันตัวตนผู้เข้าถึงข้อมูล (User Authentication)
๔. การสร้างข้อมูลและการเข้าถึงข้อมูลต้องมีการเก็บบันทึกทุกครั้ง
๕. เจ้าของข้อมูลส่วนบุคคลและผู้ถือสิทธิครอบครองข้อมูลจะต้องไม่ปฏิเสธคำร้องขอการใช้ข้อมูลจากผู้ใช้งานข้อมูลภายในคณะแพทยศาสตร์ เว้นแต่กรณี ดังต่อไปนี้ ๑) ข้อมูลนั้นมีชั้นความลับและการร้องขอข้อมูลของผู้ใช้งานไม่มีเหตุผลที่ชอบธรรมหรือไม่สมเหตุสมผล ๒) การแบ่งปันข้อมูลเป็นสิ่งต้องห้ามอย่างชัดแจ้งตามกฎหมาย หรือข้อตกลงการได้มาของข้อมูล
๖. หากโดยสิทธิ์ผู้ร้องขอใช้ข้อมูลไม่สามารถเข้าถึงข้อมูลที่ร้องขอได้ให้ส่งผ่านคำขอไปยังกลุ่มบริกรข้อมูลเพื่อ เสนอขออนุมัติการใช้ไปยังคณะกรรมการธรรมาภิบาลข้อมูลต่อไป

แนวทาง

๑. มีการกำหนดแนวทางการบริหารจัดการสิทธิ (Access Authorization Management) และขอสิทธิในการใช้ข้อมูลที่ชัดเจน โดยผู้มีความประสงค์ใช้งานข้อมูลต้องขออนุมัติจากเจ้าของข้อมูลส่วนบุคคล หรือผู้ถือสิทธิครอบครองข้อมูล หรือกลุ่มบริหารจัดการข้อมูล ในการเข้าถึงข้อมูลที่

เป็นความลับ ซึ่งในคำร้องขอการเข้าถึงข้อมูลจะประกอบด้วย ๑) ขอบเขตและความละเอียดของข้อมูลที่ร้องขอ เช่น ช่วงเวลาที่ต้องการใช้ข้อมูล ๒) วัตถุประสงค์ในการร้องขอข้อมูล ๓) ความถี่ในการเข้าใช้งานข้อมูล เช่น เป็นครั้งคราวหรือเป็นประจำ

๒. การควบคุมการเข้าถึงประกอบด้วยการยืนยันตัวตน (Authentication) และการอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization) เพื่อแสดงความรับผิดชอบต่อผลการกระทำ (Accountability) ที่เกิดขึ้น

๓. การกำหนดสิทธิ์ควรใช้แนวทางการจำกัดสิทธิ์ให้น้อยที่สุดเท่าที่เพียงพอสำหรับการใช้งาน ดังเช่น แนวทาง Least Privilege

๔. หน่วยงานจัดให้มีช่องทางในการขอสิทธิ์และเข้าถึงข้อมูลและเข้าถึงข้อมูลที่สะดวกรวดเร็วภายใต้กรอบการกำกับดูแลที่เหมาะสม และช่วยให้กลุ่มบริหารจัดการข้อมูลสามารถติดตามและประเมินความคุ้มค่าของข้อมูลที่มีการป้องกัน ความเสี่ยงการรั่วไหลของข้อมูลหรือใช้ไม่ตรงตามวัตถุประสงค์

๕. ให้กลุ่มบริหารจัดการข้อมูลและบริการข้อมูลด้านเทคนิคกำหนดสิทธิการเข้าถึงระบบและโปรแกรม โดยวิธีการใด ๆ ที่เป็นไปตามขั้นตอนการดำเนินงานตามที่ผู้ถือสิทธิครอบครองข้อมูลกำหนด โดยไม่ขัดต่อหลักกฎหมายที่ประกาศใช้อยู่ในขณะนั้น

๖. การกำหนดสิทธิ์ใด ๆ ต้องมีการระบุวันสิ้นสุดเสมอ และให้มีการทบทวนสิทธิการเข้าถึงของผู้ขอใช้ข้อมูล (Review of User Access Rights) ตามระยะเวลาที่กำหนดไว้

๗. รหัสผ่านถือเป็นข้อมูลลับและเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านให้มีความมั่นคงปลอดภัย

๘. กำหนดหน่วยงานที่เป็นผู้ดูแลพื้นที่เก็บข้อมูลที่อนุญาตให้ผู้อื่นเข้าถึงได้ต้องมีการเก็บรักษาบันทึกการเข้าถึงข้อมูลไว้อย่างน้อย ๙๐ วัน ตามพระราชบัญญัติคอมพิวเตอร์ ๒๕๖๔

๙. ห้ามมิให้มีการกำหนดสิทธิ์การเข้าถึงข้อมูลในกลุ่มชั้นความลับโดยการอ่านแบบสาธารณะ (Publicly Read) โดยเด็ดขาด เว้นแต่จะได้รับอนุญาตในขั้นตอนการขอใช้ข้อมูลหรือได้รับอนุญาตจากส่วนงานที่เกี่ยวข้องเป็นลายลักษณ์อักษร

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๑๐. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)
๑๑. ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑
๑๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)
๑๓. พระราชบัญญัติคอมพิวเตอร์ พ.ศ. ๒๕๖๔ มาตรา ๒๖ การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์
๑๔. Schneider, F. B. (๒๐๐๓). Least privilege and more [computer security]. IEEE Security & Privacy, ๑(๕), ๕๕–๕๙. https://doi.org/10.1109/MSECP.2003.1236236

หมวดที่ ๙ การควบคุมคุณภาพและมาตรฐานข้อมูล (Data Quality Control and Standard)

วัตถุประสงค์

เพื่อให้ผู้มีส่วนได้ส่วนเสียมีความรู้ ความเข้าใจ และสามารถปฏิบัติตามแนวทางปฏิบัติในการควบคุมคุณภาพและมาตรฐานข้อมูลให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงาน

คำนิยาม

ผู้ประเมินคุณภาพข้อมูล (Data Assessment Team) หมายความว่า คณะบุคคล/ทีมงานที่กำหนดขึ้นเพื่อทำหน้าที่การประเมินคุณภาพข้อมูลขององค์กร ในที่นี้อาจเป็นทีมบริกรข้อมูล (Data Steward Team) หรือฝ่ายตรวจสอบภายใน หรือผู้ไม่มีส่วนได้ส่วนเสียกับการดำเนินงานเพื่อให้ไม่เกิดผลประโยชน์ทับซ้อน

คุณภาพข้อมูล (Data Quality) หมายความว่า ข้อมูลนั้นได้มาตรฐานและเป็นไปตามดัชนีตัวชี้วัดคุณภาพข้อมูลที่กำหนดไว้มีความเหมาะสมและสามารถนำไปใช้งานได้ตามวัตถุประสงค์ของการเก็บและการขอใช้ข้อมูล

ความถูกต้องและสมบูรณ์แบบ (Accuracy and Completeness) หมายความว่า ข้อมูลนั้นมีความถูกต้อง แม่นยำ ปราศจากข้อผิดพลาด เชื่อถือได้ มีความสมบูรณ์ของข้อมูลหรือไม่ขาดหาย มีความครบถ้วนเพียงพอสำหรับการใช้งานตามที่ผู้ใช้ต้องการ

ความสอดคล้องกัน (Consistency) หมายความว่า ข้อมูลเป็นไปในรูปแบบเดียวกัน มีความสัมพันธ์กัน มีความสอดคล้อง หรือไม่ขัดแย้งกัน มีแนวคิด คำนิยาม วิธีการ และการอ้างอิงที่ทำให้ข้อมูลจากต่าง ๆ แหล่งกันสามารถเปรียบเทียบและบูรณาการรวมกันได้

ความเป็นปัจจุบัน (Timeliness) หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการใช้งานตามกรอบเวลาที่ได้กำหนดไว้

ตรงตามความต้องการของผู้ใช้ (Relevancy) หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับงานที่ทำอยู่ได้ เป็นข้อมูลที่ผู้ใช้งานต้องการหรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมอง และความละเอียดเพียงพอต่อการนำไปใช้งาน

ความพร้อมใช้ (Availability) หมายความว่า ข้อมูลสามารถเข้าถึงได้เมื่อต้องการใช้งาน

นโยบาย

ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้

๑. ต้องมีการกำหนดวิธีปฏิบัติในการบริหารจัดการและควบคุมคุณภาพข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และมีความพร้อมใช้ (Availability)

๒. ต้องมีการจัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้

แนวทาง

๑. ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล กลุ่มบริหารจัดการข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงหน่วยงานที่เกี่ยวข้องร่วมกันออกแบบและกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน จากนั้นให้นำเสนอขออนุญาตผู้บังคับบัญชาองค์กร หรือผู้บังคับบัญชาหน่วยงานที่มีอำนาจตัดสินใจภายใต้ขอบเขตหน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บังคับบัญชาองค์กรแล้วเท่านั้น เพื่อประกาศใช้

๒. ให้ผู้ประเมินคุณภาพข้อมูลในแต่ละหน่วยงานตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บไปแล้ว หากตรวจพบว่าข้อมูลไม่ถูกต้อง ให้แจ้งผู้ถือสิทธิครอบครองข้อมูลเพื่อปรับปรุงแก้ไขข้อมูลให้ถูกต้องครบถ้วน

๓. จัดประชุม/อบรม/ประชาสัมพันธ์ ให้ผู้เกี่ยวข้องมีความรู้ความเข้าใจถึงวิธีปฏิบัติการควบคุมคุณภาพข้อมูล และมีทักษะในการใช้ระบบและเครื่องมือที่ใช้เพื่อควบคุมคุณภาพข้อมูลอย่างถูกต้องตามขั้นตอนที่กำหนด ชี้แจงให้ผู้ปฏิบัติตระหนักถึงความสำคัญและความจำเป็นในการควบคุมคุณภาพข้อมูล

๔. มีการประชุมทบทวนแนวปฏิบัติ ขั้นตอน ระบบและเครื่องมือสำหรับควบคุมคุณภาพข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบและปรับปรุงระบบที่ใช้ในการ ให้บริการหรือระบบงานสารสนเทศให้มีความทันสมัย เหมาะสม และเป็นไปตามมาตรฐานการควบคุมคุณภาพข้อมูล

๕. การเปลี่ยนแปลงข้อมูลสามารถกระทำได้ หากเป็นการปรับปรุงหรือเปลี่ยนแปลงให้เป็นปัจจุบัน ครบถ้วน ถูกต้องเป็นไปเพื่อการควบคุมคุณภาพข้อมูล

๖. การกำหนดตัวชี้วัดในแต่ละมิติคุณภาพข้อมูล

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness)	การประเมินเรื่องความถูกต้อง แม่นยำ ครบถ้วน ข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบความถูกต้อง	- มีแหล่งข้อมูลที่น่าเชื่อถือ - มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาดของข้อมูล - มีการตรวจสอบความครบถ้วนของข้อมูล - มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ - มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกันของแนวคิด คำนิยาม วิธีการ และบูรณาการข้อมูลเพื่อใช้ประโยชน์ร่วมกันได้ตามมาตรฐานในการจัดทำข้อมูลของคณะแพทยศาสตร์	- มีการเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกันหรือมาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ - มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกัน - ข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน - มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกันทั้งภายในคณะแพทยศาสตร์ และหน่วยงานภายนอกคณะแพทยศาสตร์

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
		- มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
ตรงตามความต้องการ ของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ ต้องการหรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อนำไปใช้งาน	- ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน - มีผลประเมินความพึงพอใจของผู้ใช้ และมีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูล และแผนเรื่อง ระยะเวลา	- ข้อมูลมีการเผยแพร่ ส่งต่อตรงเวลา - ข้อมูลมีความเป็นปัจจุบัน - ข้อมูลมีการเผยแพร่หรือปรับปรับในเวลาที่เหมาะสมตามกรอบเวลาที่ได้กำหนดไว้ - มีการจัดทำปฏิทินเผยแพร่ข้อมูล
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอ หรือใช้ข้อมูล	- ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งานและเหมาะสมกับผู้ใช้งาน - มีการเผยแพร่ข้อมูลที่เหมาะสมและสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม - ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ทันที - มีคำอธิบายข้อมูลที่ชัดเจน - มีคำอธิบายขั้นตอนการขอข้อมูลที่ไม่เผยแพร่

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการ ในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๑๐. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)

๑๑. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)

๑๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (มรด. ๕: ๒๕๖๕)

หมวดที่ ๑๐ การแลกเปลี่ยน เชื่อมโยง และการเปิดเผยข้อมูล

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลระหว่าง หน่วยงานทั้งภายในและภายนอกได้ข้อมูลที่มีประสิทธิภาพ ถูกต้องตรงตามวัตถุประสงค์ข้อมูลสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

คำนิยาม

๑. การแลกเปลี่ยนข้อมูล หมายถึง วิธีการใด ๆ เพื่อส่งผ่านข้อมูลจากระบบหนึ่งไปยังอีกระบบหนึ่ง อาจดำเนินการได้แบบอัตโนมัติหรือดำเนินการโดยบุคคล ทั้งนี้ต้องเป็นวิธีการที่สามารถรับรองความครบถ้วน ถูกต้องและทันสมัยของข้อมูลได้

๒. การเชื่อมโยงข้อมูล หมายถึง วิธีการใด ๆ ที่เปิดช่องทางให้ระบบมากกว่าหนึ่งระบบสามารถประยุกต์ใช้งานข้อมูลร่วมกันได้ โดยอาจเป็นการกำหนดมาตรฐานของข้อมูลหรือวิธีการนำเข้าข้อมูลหรืออื่นใดเพื่อให้บรรลุตามวัตถุประสงค์

๓. การเปิดเผยข้อมูล หมายถึง ระเบียบการและขั้นตอนการปฏิบัติในการนำชุดข้อมูลใด ๆ ออกเผยแพร่ทั้งแบบสาธารณะและภายในกลุ่มผู้ใช้งานที่จำกัด ทั้งนี้หากข้อมูลดังกล่าวมีส่วนใดซึ่งเข้าข่าย Sensitive Data จำเป็นต้องผ่านขั้นตอนจัดการอย่างเหมาะสมก่อนเสมอ ทั้งนี้หน่วยงานผู้ครอบครองหรือดูแลข้อมูลต้องจัดให้มีช่องทางการยื่นคำขอการเปิดเผยข้อมูล

แนวทางปฏิบัติทั่วไป

๑. มีการกำหนดแนวทางปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัยคุณภาพข้อมูลและผู้ประสานงานหรือศูนย์ติดต่อของการแลกเปลี่ยนและเชื่อมโยงข้อมูล

๒. กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการระหว่างดำเนินการและเมื่อสิ้นสุดการดำเนินการ โดยทุกชุดข้อมูลที่มีการเชื่อมโยงกันระหว่างส่วนงานภายในคณะแพทยศาสตร์ฯ หรือภายนอกคณะแพทยศาสตร์ฯ จะต้องมีการจัดทำเอกสารมาตรฐานการเชื่อมโยงข้อมูล ซึ่งประกอบด้วย ชื่อชุดข้อมูล วันและเวลาการรับรองข้อมูล โดยบริกรข้อมูลด้านธุรกิจ คำอธิบายชุดข้อมูล (Metadata) ชั้นความลับของข้อมูล วันและเวลาในการส่งออกข้อมูล และวันและเวลาที่ผู้รับได้รับข้อมูล

๓. ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๔. ต้องกำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล เช่น ต้องมีการเข้ารหัสลับ (Encryption) ข้อมูลก่อนการแลกเปลี่ยนข้อมูลบางประเภท หรือช่องทางในการแลกเปลี่ยน เป็นต้น

๕. ทำการบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้ง (Log File) ระหว่างที่มีการแลกเปลี่ยนข้อมูลเพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. กลุ่มบริหารจัดการข้อมูลจะต้องแจ้งให้ผู้ขอใช้งานข้อมูลทราบ หากมีการรับส่งข้อมูลล่าช้าและประสานกับแหล่งข้อมูลเพื่อที่จะได้รับส่งข้อมูลได้โดยเร็วที่สุด

๗. กลุ่มบริหารจัดการข้อมูลจะต้องรับผิดชอบในการตรวจสอบความถูกต้องของข้อมูลภายในชุดของข้อมูล และเทียบกับข้อมูลอื่น ๆ ที่เกี่ยวข้องภายในคณะแพทยศาสตร์ หรือมหาวิทยาลัยเชียงใหม่ ประสานงานกับแหล่งข้อมูล ในการกู้คืนข้อความผิดพลาดของข้อมูลที่ส่ง ในกรณีที่ข้อมูลผิดพลาดด้วยการนำไปใช้

๘. สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยนและมาตรฐานตามที่กำหนด โดยการตรวจสอบข้อมูลจะต้องอ้างอิงตามคำอธิบายชุดข้อมูล (Metadata) และข้อมูลอ้างอิงของชุดข้อมูลนั้น

๙. มีการกำหนดสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามภารกิจของหน่วยงานนั้น ๆ

๑๐. การร้องขอข้อมูลและนำข้อมูลไปใช้ต้องเป็นไปตามวัตถุประสงค์ที่ร้องขอเท่านั้น

แนวทางปฏิบัติเรื่องการแลกเปลี่ยนและการเชื่อมโยงข้อมูล กรณีหน่วยงานภายในคณะแพทยศาสตร์

๑. ผู้ร้องขอใช้ข้อมูลจัดทำเอกสารการขอเชื่อมโยงข้อมูลตามแนวทางที่คณะแพทยศาสตร์ ได้กำหนดไว้

๒. กลุ่มบริหารจัดการข้อมูลหรือกลุ่มบริกรข้อมูลต้องพิจารณาตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๓. กลุ่มบริหารจัดการข้อมูลหรือกลุ่มบริกรข้อมูลต้องพิจารณาวัตถุประสงค์ รายละเอียดชุดข้อมูล และตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่

๔. หากผู้ร้องขอไม่มีสิทธิ์เพียงพอต่อการเชื่อมโยงข้อมูล ต้องส่งเรื่องร้องขอตามแนวทางที่คณะแพทยศาสตร์ ได้กำหนดไว้ กลุ่มบริกรข้อมูลต้องพิจารณารายละเอียดของข้อมูล พร้อมเสนอความเห็นและส่งคำขอไปยังคณะกรรมการธรรมาภิบาลข้อมูล เพื่อพิจารณาความเหมาะสม

๕. เมื่อคณะกรรมการธรรมาภิบาลข้อมูลเห็นชอบให้คำร้องขอผ่านการพิจารณา กลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลจัดทำเมทาดาตาของชุดข้อมูลที่ร้องขอ

๖. กลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลต้องจัดทำสัญญาอนุญาตหรือเงื่อนไขในการเชื่อมโยงแลกเปลี่ยนและการนำข้อมูลไปใช้อย่างชัดเจน

๗. กลุ่มบริหารจัดการข้อมูลต้องดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามเงื่อนไขและมาตรฐานการเชื่อมโยงและแลกเปลี่ยนที่กำหนดไว้

๘. กลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลต้องปรับปรุงเมทาดาตาเพิ่มเติมพร้อมติดตามและควบคุมประสิทธิภาพระหว่างการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๙. กลุ่มบริกรข้อมูลและหน่วยงานที่เกี่ยวข้องต้องสร้างความรู้ความเข้าใจในการแลกเปลี่ยนและเชื่อมโยงข้อมูลของสถาบันแก่ผู้เกี่ยวข้องในคณะแพทยศาสตร์

แนวทางปฏิบัติเรื่องการแลกเปลี่ยนและการเชื่อมโยงข้อมูล กรณีหน่วยงานภายนอกคณะแพทยศาสตร์

๑. ผู้ร้องขอใช้ข้อมูลจากหน่วยงานภายนอกจัดทำเอกสารการขอเชื่อมโยงข้อมูล ตามแนวทางคณะแพทยศาสตร์กำหนดไว้

๒. กรณีข้อมูลที่เป็นความลับ กลุ่มบริหารจัดการข้อมูลต้องพิจารณาตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากจำเป็นต้องแลกเปลี่ยนข้อมูล หน่วยงานของผู้ร้องขอใช้ข้อมูลจะต้องมีการจัดทำธรรมาภิบาลข้อมูลให้เหมาะสมตามระดับชั้นของข้อมูล

๓. หากคำร้องขอหน่วยงานผู้ร้องขอเหมาะสมเพียงพอ หรือมีความจำเป็นต่อการเชื่อมโยงข้อมูลของสถาบัน กลุ่มบริหารจัดการข้อมูลต้องส่งรายละเอียดการร้องขอไปยังเจ้าของข้อมูลส่วนบุคคลหรือผู้ถือสิทธิครอบครองข้อมูลเพื่อพิจารณา หากเจ้าของข้อมูลส่วนบุคคลยินยอมและเห็นชอบ กลุ่มบริหารจัดการข้อมูลต้องส่งคำร้องต่อไปกลุ่มบริกรข้อมูล

๔. กลุ่มบริกรข้อมูลต้องพิจารณารายละเอียดข้อมูลพร้อมเสนอความเห็นและส่งคำขอไปยังคณะกรรมการธรรมาภิบาลข้อมูล เพื่อพิจารณาความเหมาะสม

๕. เมื่อคณะกรรมการธรรมาภิบาลข้อมูลเห็นชอบให้คำร้องขอผ่านการพิจารณากลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลจัดทำเมทาดาตาของชุดข้อมูลที่ร้องขอ

๖. กลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลต้องจัดทำสัญญาอนุญาตหรือเงื่อนไขในการเชื่อมโยงและแลกเปลี่ยนและการนำข้อมูลไปใช้อย่างชัดเจน จะต้องมีการลงนามในเอกสารข้อตกลงการใช้และแบ่งปันข้อมูล (Data Use and Sharing Agreement) ระหว่างหน่วยงานหรือบุคคลผู้ขอแลกเปลี่ยนและเชื่อมโยงข้อมูลกับคณบดีคณะแพทยศาสตร์หรือผู้ที่ได้รับมอบหมาย

๗. กลุ่มบริหารจัดการข้อมูลต้องดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามเงื่อนไขและมาตรฐานการเชื่อมโยงและแลกเปลี่ยนที่กำหนดไว้

๘. กลุ่มบริหารจัดการข้อมูลและกลุ่มบริกรข้อมูลต้องปรับปรุงเมทาดาตาเพิ่มเติมพร้อมติดตามและควบคุมประสิทธิภาพ ระหว่างการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๙. กลุ่มบริกรข้อมูลและหน่วยงานที่เกี่ยวข้องต้องสร้างความรู้ความเข้าใจในการแลกเปลี่ยนและเชื่อมโยงข้อมูลของคณะแพทยศาสตร์ แก่ผู้เกี่ยวข้องในคณะแพทยศาสตร์และหน่วยงานภายนอกที่ขอแลกเปลี่ยนและเชื่อมโยงข้อมูล

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๔. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๕. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม
๖. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๗. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๘. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. ๒๕๖๓
๙. ประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เรื่อง นโยบายการจัดการและส่งเสริมการแบ่งปันข้อมูลสารสนเทศ เพื่อใช้ประโยชน์และเผยแพร่ข้อมูลทั้งภายในและภายนอกสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (พ.ศ. ๒๕๖๒)
๑๐. ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๑๑. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)
๑๒. ประกาศคณะแพทยศาสตร์ เรื่องแนวปฏิบัติการใช้ข้อมูลจากเวชระเบียนเพื่อการวิจัย พ.ศ.๒๕๖๕

หมวดที่ ๑๑ การจัดการเหตุละเมิดข้อมูล

วัตถุประสงค์

เพื่อกำหนดระเบียบ ช่องทาง แนวการปฏิบัติและผู้รับผิดชอบดำเนินการรับเหตุ เมื่อเกิดเหตุละเมิดกับข้อมูลในขณะที่อยู่ใต้การดูแลของคณะแพทย์ศาสตร์หรือผู้ข้อใช้ข้อมูล

คำนิยาม

เหตุละเมิดข้อมูล (Data Breach Incident) หมายถึง เหตุการณ์ที่ข้อมูลใด ๆ เกิดการรั่วไหลหรือสามารถเข้าถึงได้ด้วยวิธีการใด ๆ ที่อยู่นอกเหนือจากขอบเขตและวัตถุประสงค์ของข้อมูลนั้น ทั้งจากข้อผิดพลาดของบุคคลหรือระบบก็ตาม

แนวทางปฏิบัติ

๑. คณะแพทย์ศาสตร์มอบหมายให้จัดตั้งคณะกรรมการเพื่อศึกษาและจัดทำแผนการรับมือเหตุละเมิดข้อมูล (Data Breach Incident Plan) โดยจัดตั้งให้มีระบบรับแจ้งเหตุการณ์ละเมิดข้อมูล (Data Breach Incident Report System) ซึ่งครอบคลุมขั้นตอนดังต่อไปนี้
   - จัดให้มีช่องทางการรับแจ้งเหตุ ทั้งจากช่องทางสาธารณะและช่องทางอื่น ๆ ตามความเหมาะสม
   - ดำเนินการตรวจสอบเหตุรับแจ้งและประเมินความรุนแรงตามแผนการรับมือข้างต้นภายในระยะเวลาที่เหมาะสม
   - หากสามารถยืนยันเหตุการละเมิด ระบบหรือผู้รับผิดชอบต้องแจ้งไปยังส่วนงานที่เกี่ยวข้องกับข้อมูลนั้นทันทีและแจ้งไปยังผู้ที่ได้รับผลกระทบภายใน ๓๐ วันตามปฏิทิน
๒. ส่วนงานภายในคณะแพทย์ศาสตร์ หรือบุคคล หรือกลุ่มบุคคล ที่ได้รับมอบหมายถึงใช้งานหรือเก็บรักษาข้อมูลมีหน้าที่ในการรายงานไปยังระบบแจ้งเหตุดังกล่าว หากพบเหตุใด ๆ ที่อาจเป็นการละเมิดข้อมูลภายใต้การดูแลโดยทันที

เอกสารที่เกี่ยวข้อง

๑. คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ๑๕ ธันวาคม พ.ศ. ๒๕๖๕)
๒. PDPC | Guide on Managing and Notifying Data Breaches Under the PDPA. (n.d.). Retrieved February ๑๔, ๒๐๒๔, from https://www.pdpc.gov.sg/Help-and-Resources/2021/01/Data-Breach-Management-Guide

หมวดที่ ๑๒ การทำลายข้อมูล

วัตถุประสงค์

เพื่อกำหนดหลักการและแนวทางในการทำลายข้อมูลที่ได้จัดเก็บหรือขอใช้ให้เป็นไปตามขั้นตอนระเบียบการ หรือข้อกฎหมายที่เกี่ยวข้อง

คำนิยาม

กระบวนการทำลายข้อมูล (Data Disposal) หมายถึง วิธีการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีครบตามระยะจัดเก็บที่กำหนด หรือเสร็จสิ้นตามจุดประสงค์การใช้งาน หรือเมื่อมีผู้ร้องขอให้ทำลายข้อมูล เพื่อให้ไม่สามารถเข้าถึงหรือใช้งานข้อมูลนั้น ๆ ได้อย่างเป็นการถาวร

แนวทาง

แนวปฏิบัติการทำลายข้อมูล (Data Disposal) มีดังต่อไปนี้

๑. ต้องมีการตรวจสอบความสอดคล้องของวิธีปฏิบัติการทำลายข้อมูลให้สอดคล้องต่อกฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับข้อมูลต้องทำลาย โดยเฉพาะมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือมั่นใจได้ว่าสารสนเทศที่ตนดูแลรักษาอยู่นั้น ได้ถูกลบทำลายอย่างถาวร เพื่อป้องกันข้อมูลรั่วไหลจากการลักลอบกู้คืนข้อมูล

๒. การลบทำลายข้อมูลอย่างมั่นคงปลอดภัย ให้ดำเนินการด้วยวิธีการใดวิธีการหนึ่งดังต่อไปนี้
   - ลบทำลายข้อมูลในระดับไฟล์ด้วยวิธีการ Secure Delete
   - ลบทำลายคีย์ไฟล์สำหรับสารสนเทศที่มีการเข้ารหัสลับ (Encrypted Data) เพื่อไม่ให้สามารถถอดรหัสได้อีกต่อไป
   - ทำลายข้อมูลแบบ Secure Delete หรือ Secure Erase ด้วยวิธีการที่ผู้ผลิตกำหนด
   - ใช้ซอฟต์แวร์หรือฮาร์ดแวร์สำหรับการลบข้อมูลโดยเฉพาะ (Sanitization)
   - กรณีครุภัณฑ์ หรือส่วนใดส่วนหนึ่งของครุภัณฑ์ของสำนักงานให้ทำลายทิ้งในเชิงกายภาพ เช่น การทำให้เสื่อมภาพของจานแม่เหล็ก (Degauss) บดทำลาย เผาทำลาย โดยต้องผ่านกระบวนการทางพัสดุก่อน

๓. เมื่อสิ้นสุดการเป็นพนักงานหรือพนักงานโครงการ หรือสิ้นสุดการใช้เครื่องคอมพิวเตอร์ส่วนบุคคลหรือระบบใด ๆ ต้องทำการส่งคืนทรัพยากรนั้น ๆ คืนให้แก่หน่วยบริการเทคโนโลยีสารสนเทศเพื่อดำเนินการทำลายข้อมูลต่อไป

๔. มีการจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ของข้อมูลที่ทำลายหรือบันทึกอื่น ๆ ที่เทียบเท่าเพื่อการตรวจสอบในภายหลัง

๕. ต้องมีการจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนคุม และบันทึกการทำลายข้อมูลโดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖. ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้แล้วเสร็จในระยะเวลาที่เหมาะสม ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ขัดต่อข้อกฎหมายใด ๆ

เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๘ และที่แก้ไข เพิ่มเติม
๔. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม
๕. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม
๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม
๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องหลักเกณฑ์และวิธีการใน การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๙. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูล จราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
๑๐. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๕ (มรด. ๓-๑: ๒๕๖๕)
๑๑. พระราชกำหนดว่าด้วยการประชุมผ่านสื่อ อิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓
๑๒. ปประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
๑๓. แนวทางประกาศมหาวิทยาลัยเชียงใหม่ เรื่องนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเชียงใหม่ (CMU Privacy Policy)

การดำเนินการเพื่อให้เป็นไปตามนโยบายของประกาศนี้ให้เป็นไปตามข้อบังคับและประกาศที่คณะแพทยศาสตร์มหาวิทยาลัยเชียงใหม่กำหนด จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๗

(ศาสตราจารย์ (เชี่ยวชาญพิเศษ) นายแพทย์บรรณกิจ โลจนาภิวัฒน์)
คณบดีคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่