**ประกาศโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗**
**เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)**
**โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗**

---

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีการนำระบบเทคโนโลยีสารสนเทศและเทคโนโลยีดิจิทัลมาใช้ในการบริหารจัดการ การให้บริการทางการแพทย์ และการดำเนินงานของหน่วยงานอย่างต่อเนื่อง ซึ่งเกี่ยวข้องกับการจัดเก็บ การใช้ และการแลกเปลี่ยนข้อมูลจำนวนมาก จึงจำเป็นต้องกำหนดแนวทางในการบริหารจัดการข้อมูลให้มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ รวมทั้งมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปอย่างมีมาตรฐาน โปร่งใส ตรวจสอบได้ และสอดคล้องกับกฎหมายและแนวทางที่เกี่ยวข้อง อาทิ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งแนวทางธรรมาภิบาลข้อมูลภาครัฐ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ จึงกำหนด นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ เพื่อเป็นกรอบแนวทางในการบริหารจัดการข้อมูลของหน่วยงานให้มีความถูกต้อง เชื่อถือได้ มีความมั่นคงปลอดภัย และสามารถนำข้อมูลไปใช้ประโยชน์ในการบริหารจัดการและการให้บริการได้อย่างมีประสิทธิภาพ รายละเอียดเป็นไปตามเอกสาร “นโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗” ที่แนบมาพร้อมประกาศฉบับนี้

ทั้งนี้ ให้หน่วยงานภายในโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ถือปฏิบัติตามนโยบายดังกล่าวอย่างเคร่งครัด เพื่อให้การบริหารจัดการข้อมูลของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบได้ โดยให้มีผลบังคับใช้ตั้งแต่วันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๖ มีนาคม พ.ศ. ๒๕๖๙

(นายจิรภัทร กัลยาณพจน์พร)
ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

# เอกสารแนบท้ายประกาศ
# นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)
# โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

# นโยบายธรรมาภิบาลข้อมูล
# (Data Governance Policy)
# โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗


**จัดทำโดย**

กลุ่มงานเทคโนโลยีสารสนเทศ

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

# คำนำ

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ได้จัดทำนโยบายธรรมาภิบาลข้อมูล เพื่อกำหนดกรอบแนวทางในการบริหารจัดการข้อมูลสุขภาพ ข้อมูลทางการแพทย์ และข้อมูลสารสนเทศของหน่วยงาน ให้มีความโปร่งใส ตรวจสอบได้ และมีประสิทธิภาพ อันส่งผลต่อคุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการใช้ประโยชน์จากข้อมูลอย่างเหมาะสม โดยมุ่งเน้นให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งภายในหน่วยงานและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อสนับสนุนการบริหารจัดการ การให้บริการทางการแพทย์ และการตัดสินใจของผู้บริหาร

ในการดำเนินงานด้านธรรมาภิบาลข้อมูล โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ได้กำหนดโครงสร้างการกำกับดูแลข้อมูล โดยมีคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) และคณะบริกรข้อมูล (Data Steward Team) ทำหน้าที่กำหนดนโยบาย กำกับ ติดตาม และส่งเสริมการบริหารจัดการข้อมูลของโรงพยาบาลให้เป็นไปตามหลักธรรมาภิบาลข้อมูลภาครัฐ โดยมุ่งเน้นให้ข้อมูลผู้ป่วย ข้อมูลทางคลินิก และข้อมูลการให้บริการสาธารณสุขมีความถูกต้อง ครบถ้วน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ ภายใต้หลักการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

นโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลฉบับนี้ จัดทำขึ้นโดยอ้างอิงแนวทางธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และกฎหมายที่เกี่ยวข้อง อาทิ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปตามหลักการธรรมาภิบาลข้อมูล สามารถสนับสนุนการดำเนินงานของหน่วยงาน และสร้างความเชื่อมั่นให้แก่ผู้รับบริการและผู้มีส่วนเกี่ยวข้องในระบบบริการสุขภาพ

# สารบัญ

# บทสรุปผู้บริหาร

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องพัฒนาการบริหารงานและการให้บริการสาธารณะผ่านระบบดิจิทัล เพื่อเพิ่มประสิทธิภาพการดำเนินงานของภาครัฐ และยกระดับคุณภาพการให้บริการแก่ประชาชน โดยเน้นการบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ สามารถเชื่อมโยง แลกเปลี่ยน และใช้ประโยชน์จากข้อมูลร่วมกันระหว่างหน่วยงานได้อย่างมั่นคงปลอดภัย ภายใต้หลักธรรมาภิบาลข้อมูลภาครัฐ

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ในฐานะหน่วยงานด้านบริการสาธารณสุขที่มีการใช้ระบบสารสนเทศและข้อมูลสุขภาพจำนวนมาก จึงได้จัดทำนโยบายธรรมาภิบาลข้อมูลของโรงพยาบาล เพื่อกำหนดกรอบแนวทางในการบริหารจัดการข้อมูลสุขภาพ ข้อมูลทางการแพทย์ และข้อมูลสารสนเทศของหน่วยงานให้มีคุณภาพ มีความถูกต้องครบถ้วน มีความมั่นคงปลอดภัย และสามารถนำข้อมูลไปใช้สนับสนุนการบริหารจัดการ การพัฒนาคุณภาพบริการ และการตัดสินใจเชิงนโยบายของผู้บริหารได้อย่างมีประสิทธิภาพ

นโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลมุ่งเน้นการกำกับดูแลการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเชื่อมโยงและแลกเปลี่ยนข้อมูล ตลอดจนการเปิดเผยและการคุ้มครองข้อมูล เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง โดยเฉพาะการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพของผู้ป่วย

การดำเนินงานตามนโยบายธรรมาภิบาลข้อมูลดังกล่าว จะช่วยเสริมสร้างระบบการบริหารจัดการข้อมูลของโรงพยาบาลให้มีความเป็นระบบ โปร่งใส และตรวจสอบได้ สามารถสนับสนุนการพัฒนาระบบบริการสุขภาพ การบูรณาการข้อมูลด้านสาธารณสุข และการยกระดับองค์กรสู่การเป็นองค์กรดิจิทัลด้านสุขภาพได้อย่างยั่งยืน

## ๑. บทนำ

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีการนำระบบเทคโนโลยีสารสนเทศและเทคโนโลยีดิจิทัลมาใช้ในการบริหารจัดการ การให้บริการทางการแพทย์ และการดำเนินงานของหน่วยงานอย่างต่อเนื่อง ซึ่งเกี่ยวข้องกับการจัดเก็บ การใช้ และการแลกเปลี่ยนข้อมูลจำนวนมาก โดยเฉพาะข้อมูลสุขภาพ ข้อมูลทางการแพทย์ และข้อมูลการให้บริการสาธารณสุข การบริหารจัดการข้อมูลดังกล่าวจึงจำเป็นต้องดำเนินการภายใต้หลักธรรมาภิบาลข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการและการให้บริการได้อย่างมีประสิทธิภาพ

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ได้กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการข้อมูลของหน่วยงานอย่างเป็นระบบ มีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล รวมทั้งมีการกำหนดมาตรการควบคุมคุณภาพข้อมูล การจัดหมวดหมู่ข้อมูล การจัดทำบัญชีข้อมูล และการกำหนดมาตรการด้านความมั่นคงปลอดภัยของข้อมูล เพื่อให้ข้อมูลของหน่วยงานสามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการการใช้งานได้อย่างมีประสิทธิภาพและปลอดภัย

เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ เป็นไปอย่างมีมาตรฐาน สอดคล้องกับกฎหมายและแนวทางธรรมาภิบาลข้อมูลภาครัฐ โรงพยาบาลจึงได้จัดทำนโยบายธรรมาภิบาลข้อมูลของหน่วยงาน เพื่อใช้เป็นกรอบแนวทางในการกำกับดูแล การบริหารจัดการ และการใช้ประโยชน์จากข้อมูลของโรงพยาบาล โดยครอบคลุมการบริหารจัดการข้อมูลตลอดวงจรชีวิตข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเชื่อมโยง การเปิดเผย และการทำลายข้อมูล ภายใต้หลักการด้านความมั่นคงปลอดภัยของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล

นโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ประกอบด้วยแนวทางการบริหารจัดการข้อมูลใน ๘ หมวด ได้แก่ หมวดทั่วไป การสร้างและการจัดเก็บข้อมูล การประมวลผลและการใช้ข้อมูล การเชื่อมโยงและการแลกเปลี่ยนข้อมูล การเปิดเผยและการรักษาความลับข้อมูล มาตรฐานข้อมูล การจัดชั้นความลับข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลมีความเป็นระบบ โปร่งใส สามารถตรวจสอบได้ และสนับสนุนการพัฒนาระบบบริการสุขภาพของโรงพยาบาลอย่างมีประสิทธิภาพ

## ๒. วัตถุประสงค์

การจัดทำนโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อกำหนดกรอบแนวทางในการบริหารจัดการข้อมูลของโรงพยาบาลให้มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๒.๒ เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของโรงพยาบาลให้ชัดเจน

๒.๓ เพื่อส่งเสริมการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย และสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

๒.๔ เพื่อสนับสนุนการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภายในโรงพยาบาล และหน่วยงานภายนอกที่เกี่ยวข้องอย่างมีประสิทธิภาพ

๒.๕ เพื่อสนับสนุนการนำข้อมูลไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การติดตามประเมินผล และการพัฒนาคุณภาพการให้บริการทางการแพทย์ของโรงพยาบาล

## ๓. ขอบเขตการบังคับใช้

นโยบายธรรมาภิบาลข้อมูลฉบับนี้ ใช้บังคับกับการบริหารจัดการข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ครอบคลุมข้อมูลทุกประเภทที่เกิดขึ้นจากการดำเนินงานของโรงพยาบาล ทั้งในรูปแบบเอกสารและข้อมูลดิจิทัล รวมถึงข้อมูลที่จัดเก็บในระบบสารสนเทศต่าง ๆ ของโรงพยาบาล เช่น ระบบสารสนเทศโรงพยาบาล (Hospital Information System) ระบบข้อมูลทางคลินิก และระบบสนับสนุนการบริหารจัดการ

การดำเนินงานตามนโยบายนี้ครอบคลุมกระบวนการบริหารจัดการข้อมูลตลอดวงจรชีวิตข้อมูล (Data Lifecycle) ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเชื่อมโยงและแลกเปลี่ยน การเปิดเผย และการทำลายข้อมูล โดยให้หน่วยงานและบุคลากรของโรงพยาบาลที่เกี่ยวข้องกับการจัดเก็บหรือใช้ข้อมูลถือปฏิบัติตามนโยบายนี้ ประกอบด้วย ๘ หมวด ดังนี้

หมวดที่ ๑ ทั่วไป (General Domain)
หมวดที่ ๒ การสร้าง การจัดเก็บ และการทำลายข้อมูล (Data Creating, Storage and Destruction Domain)
หมวดที่ ๓ การประมวลผลและการใช้ข้อมูล (Data Processing and Use Domain)
หมวดที่ ๔ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล (Data Integration and Exchange Domain)
หมวดที่ ๕ การเปิดเผยและการรักษาความลับข้อมูล (Data Disclosure and Confidentiality Domain)
หมวดที่ ๖ มาตรฐานข้อมูล (Data Standard Domain)
หมวดที่ ๗ มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard Domain)
หมวดที่ ๘ การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Domain)

# หมวด ๑ ทั่วไป

## (General Domain)

### ๑. คำนิยาม

นิยามที่ใช้ในนโยบายธรรมาภิบาลข้อมูลโรงพยาบาล มีความหมาย ดังนี้

ตารางที่ ๑ คำนิยามที่ใช้ในนโยบายธรรมาภิบาลข้อมูลโรงพยาบาล

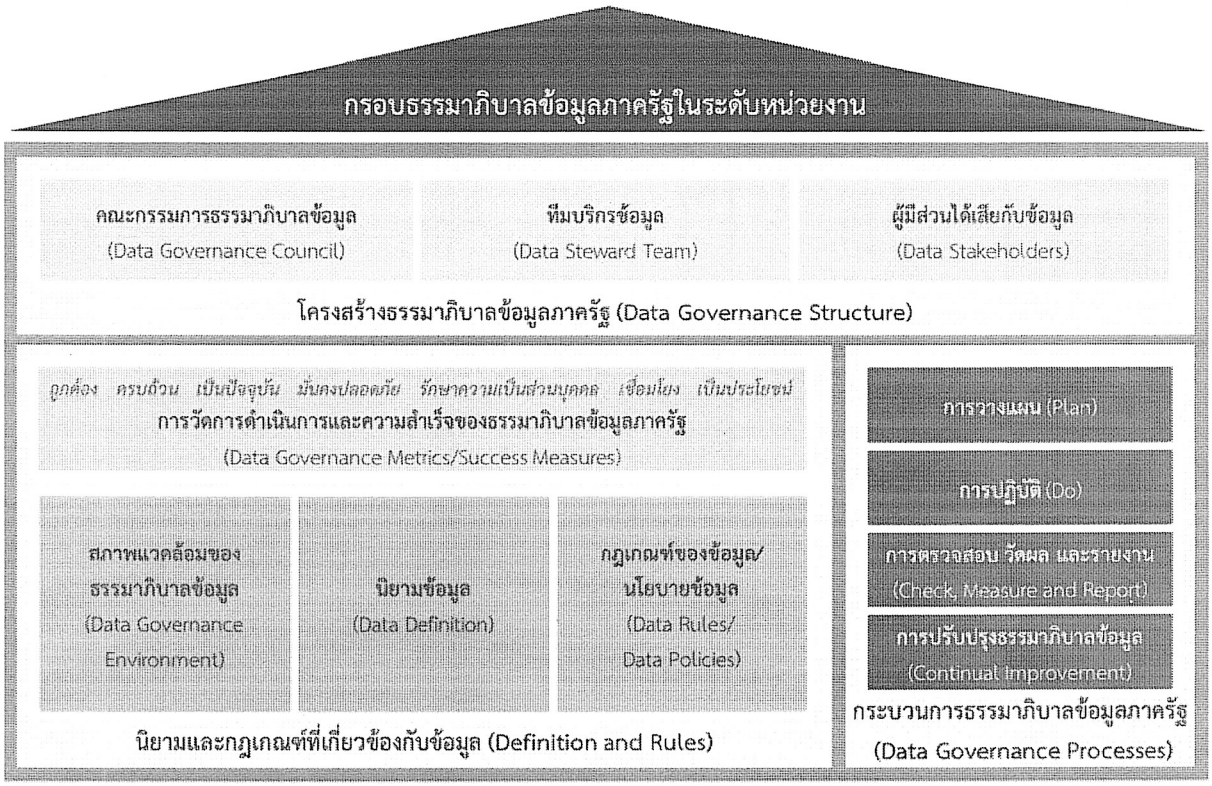
| คำนิยาม | ความหมาย |
|---|---|
| "โรงพยาบาล" | โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ |
| "ผู้บังคับบัญชา" | ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาล |
| "บุคลากร" | ผู้บริหาร แพทย์ พยาบาล เภสัชกร นักวิชาชีพสุขภาพ ข้าราชการ พนักงาน ลูกจ้าง และอาสาสมัครของโรงพยาบาล |
| "ผู้ป่วย / ผู้รับบริการ" | บุคคลที่มารับบริการทางการแพทย์และสาธารณสุขจาก โรงพยาบาล ทั้งผู้ป่วยนอก (OPD) ผู้ป่วยใน (IPD) และผู้ที่มาติดต่อผ่านช่องทางต่างๆ |
| "หน่วยงานภายนอก" | องค์กรหรือหน่วยงานที่โรงพยาบาลอนุญาตให้มีสิทธิ์เข้าถึงหรือใช้ข้อมูล เช่น สปสช. กรมสนับสนุนบริการสุขภาพ สำนักระบาดวิทยา สถานพยาบาลเครือข่าย |
| "ข้อมูล" (Data) | ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ ไม่ว่าจะอยู่ในรูปแบบเอกสาร ระบบคอมพิวเตอร์ หรือสื่ออิเล็กทรอนิกส์ใดๆ |
| "ข้อมูลสุขภาพ" (Health Data) | ข้อมูลที่เกี่ยวข้องกับสภาวะสุขภาพ การเจ็บป่วย การวินิจฉัยโรค การรักษาพยาบาล ผลการตรวจ และประวัติทางการแพทย์ของผู้ป่วย ซึ่งถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง |
| "ข้อมูลทางคลินิก" (Clinical Data) | ข้อมูลที่เกิดจากกระบวนการดูแลรักษาผู้ป่วย เช่น การวินิจฉัยโรค (ICD-๑๐) ผลการตรวจทางห้องปฏิบัติการ ผลภาพรังสี การสั่งยา และการให้ยา บันทึกทางการพยาบาล และสรุปการรักษา |
| "ข้อมูลส่วนบุคคล" (Personal Data) | ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ |

| คำนิยาม | ความหมาย |
|---|---|
| "ข้อมูลส่วนบุคคลที่มีความอ่อนไหว" (Sensitive Personal Data) | ข้อมูลที่ต้องได้รับการคุ้มครองเป็นพิเศษ ในบริบทโรงพยาบาล ได้แก่ ข้อมูลสุขภาพ ความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลสุขภาพจิต ประวัติการใช้สารเสพติด ข้อมูลโรคติดต่อทางเพศสัมพันธ์ |
| "ข้อมูลหลัก" (Master Data) | ข้อมูลอ้างอิงหลักที่ใช้ร่วมกันทั่วทั้งองค์กร เช่น รหัสผู้ป่วย รหัสบุคลากร รหัสหน่วยงาน รหัส ICD-๑๐ |
| "ข้อมูลเปิด" (Open Data) | ข้อมูลที่โรงพยาบาลอนุญาตให้เผยแพร่และนำไปใช้ได้โดยไม่มีข้อจำกัด ซึ่งไม่ระบุตัวตนผู้ป่วย |
| "เวชระเบียน" (Medical Record) | เอกสารหรือบันทึกทางการแพทย์ที่จัดทำขึ้นเพื่อบันทึกข้อมูลสุขภาพของผู้ป่วย ทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ (Electronic Medical Record: EMR / Electronic Health Record: EHR) |
| "ระบบเวชระเบียนอิเล็กทรอนิกส์" (EMR/EHR) | ระบบสารสนเทศที่ใช้บันทึกและจัดการข้อมูลผู้ป่วยในรูปแบบดิจิทัล ครอบคลุมประวัติการรักษา ผลการตรวจ การสั่งยา และข้อมูลทางคลินิกอื่นๆ |
| "มาตรฐานข้อมูลสุขภาพ" | ข้อกำหนดสากลสำหรับการจัดเก็บและแลกเปลี่ยนข้อมูลสุขภาพ เช่น ICD-๑๐ (รหัสโรค), ICD-๙-CM/ICD-๑๐-PCS (รหัสหัตถการ), HL๗ FHIR (มาตรฐานการแลกเปลี่ยนข้อมูล), และมาตรฐาน ๔๓ แฟ้มข้อมูลสุขภาพของไทย |
| "ชุดข้อมูล ๔๓ แฟ้ม" | มาตรฐานการจัดส่งข้อมูลบริการสาธารณสุขของประเทศไทย ที่สถานพยาบาลต้องส่งให้กับสปสช. และหน่วยงานที่เกี่ยวข้อง ประกอบด้วยข้อมูล ๔๓ แฟ้มหลัก |
| "การแลกเปลี่ยนข้อมูลสุขภาพ" (Health Information Exchange: HIE) | กระบวนการส่งต่อและแบ่งปันข้อมูลสุขภาพระหว่างสถานพยาบาลหรือหน่วยงานสาธารณสุข ตามมาตรฐาน HL๗ FHIR |
| "การทำงานร่วมกันได้" (Interoperability) | ความสามารถของระบบสารสนเทศต่างๆ ในการสื่อสารและแลกเปลี่ยนข้อมูลกันได้อย่างมีประสิทธิภาพ |
| "วงจรชีวิตของข้อมูล" (Data Life Cycle) | ลำดับขั้นตอนของข้อมูลตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การเผยแพร่ การจัดเก็บถาวร จนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ |

| คำนิยาม | ความหมาย |
|---|---|
| "การแบ่งปันข้อมูล" (Data Sharing) | การส่งต่อหรือแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภายในและภายนอกโรงพยาบาล ภายใต้ข้อตกลงและกฎหมาย |
| "การบูรณาการข้อมูล" (Data Integration) | กระบวนการรวมข้อมูลจากหลายแหล่งหรือหลายระบบ เช่น HIS, LIS, PACS ให้เป็นมุมมองเดียวที่สอดคล้องกัน |
| "การวิเคราะห์ข้อมูล" (Data Analytics) | กระบวนการตรวจสอบและวิเคราะห์ข้อมูลเพื่อสนับสนุนการตัดสินใจทางคลินิกและการบริหารโรงพยาบาล |
| "ธรรมาภิบาลข้อมูล" (Data Governance) | กรอบการบริหารจัดการข้อมูลขององค์กร ครอบคลุมนโยบาย บทบาทหน้าที่ มาตรฐาน กระบวนการ และเครื่องมือ เพื่อให้ข้อมูลมีคุณภาพ ปลอดภัย และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ |
| "นโยบายข้อมูล" (Data Policy) | เอกสารที่กำหนดทิศทาง หลักการ และข้อกำหนดในการบริหารข้อมูลของโรงพยาบาล ซึ่งได้รับการอนุมัติจากผู้บริหาร |
| "รายการข้อมูล" (Data Catalog) | รายการข้อมูลทั้งหมดขององค์กรพร้อมคำอธิบาย แหล่งที่มา ผู้รับผิดชอบ และข้อกำหนดการเข้าถึง |
| "พจนานุกรมข้อมูล" (Data Dictionary) | เอกสารที่อธิบายความหมาย ชนิด รูปแบบ และกฎเกณฑ์ของแต่ละเขตข้อมูลในระบบสารสนเทศโรงพยาบาล |
| "คณะกรรมการธรรมาภิบาลข้อมูล" (Data Governance Council) | คณะกรรมการธรรมาภิบาลข้อมูลของโรงพยาบาล ประกอบด้วยผู้บริหารระดับสูงและผู้แทนจากหน่วยงานสำคัญ ทำหน้าที่กำหนดนโยบาย ทิศทาง และกำกับดูแลการจัดการข้อมูลของโรงพยาบาล |
| "เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" (Data Protection Officer: DPO) | บุคคลที่โรงพยาบาลแต่งตั้งให้มีหน้าที่ให้คำแนะนำ ตรวจสอบ และประสานงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด |
| "เจ้าของข้อมูล" (Data Owner) | หัวหน้าหน่วยงานหรือบุคลากรที่รับผิดชอบข้อมูลโดยตรง มีอำนาจอนุมัติการเข้าถึงข้อมูล กำหนดชั้นความลับ และทบทวนการดำเนินการที่เกี่ยวข้อง |
| "บริกรข้อมูล" (Data Steward) | บุคลากรของโรงพยาบาลที่ได้รับมอบหมายให้มีหน้าที่ดำเนินงานด้านธรรมาภิบาลข้อมูลในส่วนที่รับผิดชอบ |
| "ผู้ควบคุมข้อมูลส่วนบุคคล" (Data Controller) | โรงพยาบาลในฐานะนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ตาม PDPA |
| "ผู้ประมวลผลข้อมูลส่วนบุคคล" (Data Processor) | บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่งของโรงพยาบาล เช่น บริษัทผู้ให้บริการระบบ |

| คำนิยาม | ความหมาย |
|---|---|
| "ผู้สร้างข้อมูล" (Data Creator) | บุคลากรที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลในระบบสารสนเทศโรงพยาบาล เช่น แพทย์ พยาบาล เจ้าหน้าที่งานเวชระเบียน |
| "ผู้ใช้ข้อมูล" (Data User) | บุคคลที่ได้รับอนุญาตให้เข้าถึงและใช้ข้อมูลของโรงพยาบาล ตามสิทธิ์และหน้าที่ที่กำหนด |
| "ผู้ดูแลระบบสารสนเทศ" (System Administrator) | บุคลากรของกลุ่มงานเทคโนโลยีสารสนเทศที่รับผิดชอบดูแลรักษาระบบคอมพิวเตอร์ เครือข่าย และฐานข้อมูลของโรงพยาบาล |
| "การจัดชั้นความลับข้อมูล" (Data Classification) | การกำหนดระดับความลับของข้อมูล เพื่อกำหนดสิทธิ์การเข้าถึงให้เหมาะสม โดยไม่ขัดต่อกฎหมาย ระเบียบ และความเป็นส่วนตัวของผู้ป่วย |
| "การรักษาความมั่นคงปลอดภัยของข้อมูล" (Data Security) | มาตรการทางเทคนิคและการบริหารเพื่อปกป้องข้อมูลจากการเข้าถึง เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต |
| "การควบคุมการเข้าถึงข้อมูล" (Data Access Control) | กระบวนการกำหนดและจัดการสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ของบุคลากร (Role-Based Access Control) |
| "ความเป็นส่วนตัวของข้อมูล" (Data Privacy) | สิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง และหน้าที่ของโรงพยาบาลในการปกป้องสิทธิ์นั้น |
| "การทำให้ข้อมูลไม่ระบุตัวตน" (De-identification) | กระบวนการลบหรือเปลี่ยนแปลงข้อมูลที่สามารถระบุตัวตนได้ออกเพื่อใช้ข้อมูลในการวิจัยหรือวิเคราะห์ |
| "การละเมิดข้อมูลส่วนบุคคล" (Personal Data Breach) | เหตุการณ์ที่ทำให้ข้อมูลส่วนบุคคลถูกเข้าถึง ใช้งาน เปลี่ยนแปลง เปิดเผย หรือทำลายโดยไม่ได้รับอนุญาต หรือโดยอุบัติเหตุ |
| "คุณภาพข้อมูล" (Data Quality) | ตัวชี้วัดความพร้อมใช้ข้อมูลอย่างมีประโยชน์ ประกอบด้วย ๕ มิติ ได้แก่ ความถูกต้องและสมบูรณ์ (Accuracy & Completeness), ความสอดคล้องกัน (Consistency), ตรงตามความต้องการ (Relevancy), ความเป็นปัจจุบัน (Timeliness), และความพร้อมใช้ (Availability) |
| "การตรวจสอบคุณภาพข้อมูล" (Data Quality Audit) | กระบวนการตรวจสอบและประเมินคุณภาพข้อมูลอย่างเป็นระบบตามรอบเวลาที่กำหนด |

## ๒. โครงสร้างการกำกับดูแลธรรมาภิบาลข้อมูล




รูปภาพที่ ๑ กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

จากรูปแสดงกรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน ซึ่งประกอบด้วย นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure) และกระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes) โดยบุคลากรที่เกี่ยวข้องกับโครงสร้างดังกล่าวจะได้รับการแต่งตั้งโดยผู้บริหารของหน่วยงาน เพื่อทำหน้าที่กำหนดยุทธศาสตร์และแนวทางการบริหารจัดการข้อมูล รวมทั้งกำกับ ติดตาม และตรวจสอบการดำเนินงานให้เป็นไปตามนโยบายและกฎเกณฑ์ที่กำหนด

ดังนั้นเพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ เป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับหลักธรรมาภิบาลข้อมูลภาครัฐ โรงพยาบาลได้กำหนดโครงสร้างการกำกับดูแลธรรมาภิบาลข้อมูล โดยแต่งตั้งบุคลากรที่เกี่ยวข้องในการดำเนินงานด้านการบริหารจัดการข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

**(๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)**

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบด้วยผู้บริหารระดับสูงของโรงพยาบาล ทำหน้าที่กำหนดนโยบายและกำกับดูแลการบริหารจัดการข้อมูลของโรงพยาบาลให้เป็นไปตามกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง รวมทั้งกำหนดทิศทาง แผนการดำเนินงาน และมาตรการด้านธรรมาภิบาลข้อมูล เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลมีคุณภาพ มีความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการและการให้บริการทางการแพทย์ได้อย่างมีประสิทธิภาพ

**(๒) คณะทำงานบริกรข้อมูล (Data Steward Team)**

คณะทำงานบริกรข้อมูล (Data Steward Team) ประกอบด้วยบุคลากรจากหน่วยงานต่าง ๆ ของโรงพยาบาลที่ได้รับมอบหมายให้ดูแลข้อมูลในส่วนที่รับผิดชอบ ทำหน้าที่สนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูลในระดับปฏิบัติ เช่น การกำหนดนิยามข้อมูล การจำแนกหมวดหมู่ข้อมูล การกำหนดมาตรฐานข้อมูล การจัดทำคำอธิบายข้อมูลและบัญชีข้อมูล รวมทั้งการติดตามและพัฒนาคุณภาพข้อมูลให้สอดคล้องกับนโยบายธรรมาภิบาลข้อมูลของโรงพยาบาล

**(๓) ผู้มีส่วนได้ส่วนเสียด้านข้อมูล (Data Stakeholders)**

ผู้มีส่วนได้ส่วนเสียด้านข้อมูล (Data Stakeholders)ประกอบด้วยบุคลากรและหน่วยงานที่เกี่ยวข้องกับการสร้าง การจัดเก็บ การบริหารจัดการ และการใช้ข้อมูลของโรงพยาบาล ได้แก่

- **(ก) เจ้าของข้อมูล (Data Owner)** ทำหน้าที่กำกับดูแลและรับผิดชอบข้อมูลของหน่วยงาน รวมทั้งพิจารณาการเข้าถึงและการใช้ข้อมูลให้เป็นไปตามนโยบายที่กำหนด
- **(ข) ผู้สร้างข้อมูล (Data Creator)** ทำหน้าที่บันทึก แก้ไข หรือปรับปรุงข้อมูลให้ถูกต้องตามมาตรฐานและโครงสร้างข้อมูลของโรงพยาบาล
- **(ค) ผู้ใช้ข้อมูล (Data User)** ทำหน้าที่นำข้อมูลไปใช้ประโยชน์ในการปฏิบัติงาน การบริหารจัดการและการตัดสินใจของหน่วยงาน
- **(ง) ทีมบริหารจัดการข้อมูล (Data Management Team)** ทำหน้าที่ดูแลระบบและโครงสร้างพื้นฐานด้านข้อมูลของโรงพยาบาล เช่น การบริหารฐานข้อมูล การดูแลระบบสารสนเทศ และการสนับสนุนด้านเทคนิคที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูล

## หมวด ๒ การสร้าง การจัดเก็บ และการทำลายข้อมูล
## (Data Creating, Storage and Destruction Domain)

### ๑. วัตถุประสงค์

เพื่อกำหนดแนวทางในการสร้าง การจัดเก็บ การใช้ และการทำลายข้อมูลของโรงพยาบาลให้เป็นไปอย่างมีคุณภาพ มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน ตลอดวงจรชีวิตของข้อมูล (Data Lifecycle) พร้อมทั้งมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมาย มาตรฐานข้อมูลสุขภาพ และข้อกำหนดที่เกี่ยวข้องกับการจัดเก็บเวชระเบียนและข้อมูลสุขภาพ

### ๒. ขอบเขต

นโยบายนี้ครอบคลุมการบริหารจัดการข้อมูลของโรงพยาบาลตั้งแต่กระบวนการสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลและใช้ข้อมูล การจัดเก็บรักษาข้อมูล และการทำลายข้อมูล โดยคำนึงถึงความถูกต้อง คุณภาพ และความมั่นคงปลอดภัยของข้อมูล ครอบคลุมประเด็นสำคัญ ดังนี้

(ก) การกำหนดแนวทางการสร้างและบันทึกข้อมูลให้เป็นไปตามมาตรฐานข้อมูลสุขภาพ เช่น มาตรฐาน ๔๓ แฟ้ม มาตรฐาน ICD-๑๐ และมาตรฐานข้อมูลสุขภาพที่เกี่ยวข้อง

(ข) การกำหนดระบบและสภาพแวดล้อมในการจัดเก็บข้อมูลให้มีความมั่นคงปลอดภัย และสามารถรองรับการใช้งานของระบบสารสนเทศของโรงพยาบาล เช่น ระบบ Hospital Information System (HIS) และระบบสารสนเทศอื่นที่เกี่ยวข้อง

(ค) การกำหนดมาตรฐานการจัดชั้นความลับของข้อมูลและการควบคุมสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามบทบาทหน้าที่ของผู้ใช้งาน

(ง) การจัดเก็บข้อมูลให้สอดคล้องกับวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลต้องมีความถูกต้องสมบูรณ์ และสามารถตรวจสอบได้

(จ) การกำหนดระยะเวลาการจัดเก็บข้อมูลให้สอดคล้องกับข้อกำหนดด้านเวชระเบียน ข้อมูลสุขภาพ และกฎหมายที่เกี่ยวข้อง

(ฉ) การกำหนดแนวทางในการทำลายข้อมูลเมื่อหมดความจำเป็นในการใช้งาน หรือเมื่อครบกำหนดระยะเวลาการจัดเก็บ โดยต้องสามารถตรวจสอบย้อนหลังได้

### ๓. แนวทางปฏิบัติและความรับผิดชอบ

เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพ ได้กำหนดบทบาทและแนวทางการปฏิบัติของผู้ที่เกี่ยวข้อง ดังนี้

(๑) ผู้สร้างข้อมูล ซึ่งได้แก่บุคลากรทางการแพทย์และสาธารณสุข ต้องจัดทำข้อมูลให้เป็นไปตามมาตรฐานข้อมูลของโรงพยาบาล และกำหนดระดับชั้นความลับของข้อมูลก่อนนำเข้าสู่ระบบสารสนเทศ

(๒) คณะทำงานบริกรข้อมูล (Data Steward Team) มีหน้าที่ตรวจสอบคุณภาพข้อมูล และจัดทำเมทาดาต้าและพจนานุกรมข้อมูลให้ครบถ้วนก่อนจัดเก็บข้อมูลเข้าสู่ระบบ

(๓) คณะทำงานบริกรข้อมูลต้องแจ้งเจ้าของข้อมูลให้ดำเนินการแก้ไขเมื่อพบปัญหาด้านคุณภาพข้อมูล และติดตามจนกว่าการแก้ไขจะแล้วเสร็จ

(๔) คณะทำงานบริกรข้อมูลต้องกำหนดมาตรฐานการจัดเก็บข้อมูล และเลือกใช้เครื่องมือหรือเทคโนโลยีที่เหมาะสม เพื่อให้ข้อมูลสามารถใช้งานได้อย่างต่อเนื่องและปลอดภัย

(๕) โรงพยาบาลต้องกำหนดขั้นตอนในการทำลายข้อมูลให้เป็นไปตามกฎหมาย รวมถึงต้องบันทึกรายละเอียดของข้อมูลที่ถูกทำลาย ผู้ดำเนินการ และวันที่ดำเนินการ

(๖) โรงพยาบาลต้องส่งเสริมให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับการสร้าง การจัดเก็บ และการทำลายข้อมูล ผ่านการอบรมหรือการสื่อสารภายในองค์กร

(๗) กรณีเจ้าของข้อมูลส่วนบุคคลร้องขอให้ทำลายข้อมูล โรงพยาบาลต้องดำเนินการตามกระบวนการที่กฎหมายกำหนด โดยไม่กระทบต่อภาระหน้าที่ตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

## ๔. ระยะเวลาการจัดเก็บข้อมูลและเวชระเบียน (Data Retention Policy)

โรงพยาบาลกำหนดระยะเวลาการเก็บรักษาข้อมูลและเวชระเบียน เพื่อให้สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง ดังนี้

ตารางที่ ๒ ระยะเวลาการเก็บรักษาข้อมูล

| ประเภทข้อมูล | ระยะเวลาการเก็บรักษา | หมายเหตุ |
|---|---|---|
| เวชระเบียนผู้ป่วยนอก | ๑๐ ปี | นับจากวันที่รับบริการครั้งสุดท้าย |
| เวชระเบียนผู้ป่วยใน | ๕ ปี | นับจากวันที่รับบริการครั้งสุดท้าย |
| เวชระเบียนผู้ป่วยเสียชีวิต | ๕ ปี | นับจากวันที่เสียชีวิต |
| เวชระเบียนคดีความ | ๑๐ ปี | ต้องแจ้งฝ่ายกฎหมายก่อนทำลาย |
| ภาพรังสี (X-ray / CT / MRI) | ๑๐ ปี | นับจากวันที่รับบริการครั้งสุดท้าย |
| ผลตรวจห้องปฏิบัติการ | ๑๐ ปี | นับจากวันที่รับบริการครั้งสุดท้าย |
| บันทึก Log ระบบสารสนเทศ | ๙๐ วัน | เพื่อการตรวจสอบย้อนหลัง |
| ข้อมูลการเงิน / การเบิกจ่าย | ๑๐ ปี | ตามกฎหมายบัญชีและข้อกำหนดหน่วยงานรัฐ |

## ๕. การสำรองข้อมูลและการกู้คืนข้อมูล (Data Backup and Recovery)

โรงพยาบาลต้องจัดให้มีมาตรการสำรองข้อมูลและแผนการกู้คืนข้อมูล เพื่อป้องกันการสูญหายของข้อมูลและรองรับกรณีเกิดเหตุการณ์ฉุกเฉิน โดยรายละเอียดให้เป็นไปตามแผนบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ (IT Business Continuity Plan) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan) ของโรงพยาบาล

**๖. การทำลายข้อมูลและเวชระเบียน**

**<u>เวชระเบียนอิเล็กทรอนิกส์</u>**

(๑) การลบข้อมูลต้องดำเนินการโดยผู้ดูแลระบบสารสนเทศ ภายใต้การอนุมัติของเจ้าของข้อมูล

(๒) ต้องใช้วิธีการลบข้อมูลแบบปลอดภัย (Secure Erasure) สำหรับข้อมูลที่มีความอ่อนไหว

(๓) ต้องบันทึกรายละเอียดของข้อมูลที่ถูกทำลาย วันที่ทำลาย และผู้ดำเนินการ เพื่อการตรวจสอบ

**<u>เวชระเบียนกระดาษ</u>**

(๑) โรงพยาบาลต้องแต่งตั้งคณะกรรมการทำลายเวชระเบียน

(๒) ต้องจัดทำบัญชีรายการเวชระเบียนที่จะทำลาย และให้คณะกรรมการตรวจสอบก่อนดำเนินการ

(๓) การทำลายเวชระเบียนต้องใช้วิธีการที่ไม่สามารถนำกลับมาอ่านหรือใช้งานได้ เช่น การสับหรือตัดย่อย

(๔) ต้องจัดทำรายงานการทำลายเวชระเบียนเสนอผู้บริหารโรงพยาบาลทราบ

**๗. แผนภาพวงจรชีวิตข้อมูลของโรงพยาบาล (Hospital Data Lifecycle)**

การบริหารจัดการข้อมูลของโรงพยาบาลดำเนินการตามวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การสร้างข้อมูล การจัดเก็บ การใช้งาน การเชื่อมโยงข้อมูล การเก็บรักษา และการทำลายข้อมูล เพื่อให้ข้อมูลมีคุณภาพ มีความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ในการให้บริการทางการแพทย์และการบริหารจัดการได้อย่างมีประสิทธิภาพ

ตารางที่ ๓ วงจรชีวิตข้อมูลของโรงพยาบาล

| ขั้นตอน | รายละเอียด | ตัวอย่างระบบ |
|---|---|---|
| ๑. การสร้างข้อมูล (Create) | การบันทึกข้อมูลผู้ป่วยและข้อมูลบริการทางการแพทย์ | HIS / EMR |
| ๒. การจัดเก็บข้อมูล (Store) | การจัดเก็บข้อมูลในระบบฐานข้อมูลและเวชระเบียนอิเล็กทรอนิกส์ | HIS / EMR |
| ๓. การใช้ข้อมูล (Use) | การนำข้อมูลไปใช้ในการวินิจฉัย รักษา และบริหารจัดการ | HIS / LIS |
| ๔. การเชื่อมโยงข้อมูล (Share / Exchange) | การแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก เช่น สปสช. หรือโรงพยาบาลเครือข่าย | HIE / PACS |
| ๕. การเก็บรักษาข้อมูล (Archive) | การจัดเก็บข้อมูลระยะยาวตามระยะเวลาที่กำหนด | HIS / PACS |

**๘. ความสัมพันธ์ของระบบสารสนเทศกับวงจรชีวิตข้อมูล**

เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ ระบบสารสนเทศของโรงพยาบาลมีบทบาทสำคัญในแต่ละขั้นตอนของวงจรชีวิตข้อมูล ดังนี้

ตารางที่ ๔ บทบาทสำคัญในแต่ละขั้นตอนของวงจรชีวิตข้อมูล

| ระบบสารสนเทศ | ประเภทข้อมูล | บทบาทใน Data Lifecycle |
|---|---|---|
| HIS / EMR | ข้อมูลผู้ป่วยและเวชระเบียน | สร้าง จัดเก็บ ใช้ และเก็บรักษาข้อมูล |
| LIS | ผลตรวจทางห้องปฏิบัติการ | สร้าง ใช้ และเชื่อมโยงข้อมูล |
| PACS | ภาพทางการแพทย์ | จัดเก็บและเก็บรักษาข้อมูลภาพ |
| ERP / Financial System | ข้อมูลการเงินและบัญชี | จัดเก็บและบริหารข้อมูลการเงิน |
| Data Warehouse / Analytics | ข้อมูลสถิติและการวิเคราะห์ | ใช้ข้อมูลเพื่อการวิเคราะห์และบริหารจัดการ |

## ๙. แนวทางการกำกับดูแลวงจรชีวิตข้อมูล

โรงพยาบาลกำหนดให้การบริหารจัดการข้อมูลในแต่ละขั้นตอนของวงจรชีวิตข้อมูลอยู่ภายใต้การกำกับดูแลของโครงสร้างธรรมาภิบาลข้อมูล

ตารางที่ ๕ การบริหารจัดการข้อมูลในแต่ละขั้นตอนของวงจรชีวิตข้อมูล

| บทบาท | หน้าที่ |
|---|---|
| คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) | กำหนดนโยบายและกำกับดูแลการบริหารจัดการข้อมูล |
| คณะทำงานบริกรข้อมูล (Data Steward Team) | ตรวจสอบคุณภาพข้อมูลและกำกับมาตรฐานข้อมูล |
| เจ้าของข้อมูล (Data Owner) | รับผิดชอบและอนุมัติการใช้ข้อมูล |
| ผู้สร้างข้อมูล (Data Creator) | บันทึกและปรับปรุงข้อมูล |
| ผู้ใช้ข้อมูล (Data User) | ใช้ข้อมูลตามสิทธิ์ที่กำหนด |
| ผู้ดูแลระบบสารสนเทศ (IT / Data Management) | ดูแลระบบสารสนเทศและโครงสร้างพื้นฐานข้อมูล |
| ผู้มีส่วนได้ส่วนเสียด้านข้อมูล (Data Stakeholders) | สนับสนุนการดำเนินงานด้านข้อมูล |

## หมวด ๓ การประมวลผลและการใช้ข้อมูล
## (Data Processing and Use Domain)

### ๑. วัตถุประสงค์

เพื่อกำหนดแนวทางในการประมวลผลและการใช้ข้อมูลของโรงพยาบาลให้เป็นไปอย่างถูกต้อง เหมาะสม และตรงตามวัตถุประสงค์ของการใช้ข้อมูล โดยเฉพาะข้อมูลสุขภาพและข้อมูลส่วนบุคคลของผู้ป่วยและผู้รับบริการ พร้อมทั้งมีมาตรการควบคุมการเข้าถึงข้อมูล การตรวจสอบการใช้งาน และการรักษาความมั่นคงปลอดภัยของข้อมูลให้เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

### ๒. ขอบเขต

การประมวลผลและการใช้ข้อมูลของโรงพยาบาลครอบคลุมการดำเนินงานที่เกี่ยวข้องกับการเข้าถึง การวิเคราะห์ การประมวลผล และการใช้ประโยชน์จากข้อมูลในระบบสารสนเทศของโรงพยาบาล โดยมีหลักการสำคัญ ดังนี้

(๑) การกำหนดแนวปฏิบัติและมาตรฐานในการประมวลผลข้อมูลและการสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบ

(๒) การใช้ข้อมูลสุขภาพและข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ที่ได้รับอนุญาตหรือได้รับความยินยอมจากเจ้าของข้อมูล

(๓) การจัดทำและปรับปรุงเมทาดาต้าสำหรับข้อมูลที่จัดเก็บในระบบหรือคลังข้อมูลของโรงพยาบาล

(๔) การบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log) เพื่อให้สามารถตรวจสอบย้อนหลังได้

### ๓. แนวทางปฏิบัติและความรับผิดชอบ

(๑) คณะทำงานบริกรข้อมูล (Data Steward Team) ต้องกำหนดแนวทางและมาตรฐานการประมวลผลข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูล และกำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ของผู้ใช้งาน (Role-Based Access Control)

(๒) โรงพยาบาลต้องกำหนดมาตรการควบคุมการเข้าถึงข้อมูล เพื่อป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงหรือแก้ไขข้อมูล

(๓) ผู้ใช้ข้อมูลต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้รับอนุญาตเท่านั้น และต้องไม่ใช้ข้อมูลนอกเหนือจากขอบเขตที่ได้รับอนุญาต

(๔) ผู้ใช้ระบบต้องออกจากระบบทุกครั้งเมื่อสิ้นสุดการใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๕) คณะทำงานบริกรข้อมูลต้องดูแลและปรับปรุงเมทาดาต้าและข้อมูลเกี่ยวกับผู้ใช้งาน เพื่อให้สามารถติดตามและตรวจสอบการใช้ข้อมูลได้

(๖) โรงพยาบาลต้องจัดให้มีการอบรมหรือสื่อสารให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับแนวทางการประมวลผลและการใช้ข้อมูลอย่างเหมาะสม

**๔. ข้อจำกัดในการใช้ข้อมูลทางคลินิก**

(๑) บุคลากรต้องเข้าถึงข้อมูลผู้ป่วยเฉพาะเท่าที่จำเป็นต่อการปฏิบัติหน้าที่ (Minimum Necessary Principle)

(๒) การพิมพ์หรือดาวน์โหลดข้อมูลเวชระเบียนต้องได้รับอนุญาตตามกระบวนการที่กำหนด

(๓) ห้ามส่งข้อมูลผู้ป่วยผ่านช่องทางที่ไม่มีความปลอดภัย เช่น ระบบสื่อสารส่วนตัว หรือช่องทางที่ไม่ได้รับอนุญาต

(๔) การใช้ข้อมูลผู้ป่วยเพื่อการฝึกอบรม การนำเสนอทางวิชาการ หรือการเผยแพร่ ต้องดำเนินการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ก่อน (De-identification)

(๕) กรณีข้อมูลผู้ป่วยที่มีความอ่อนไหวสูง ต้องมีมาตรการควบคุมการเข้าถึงข้อมูลเป็นพิเศษ

**๕. การใช้ข้อมูลเพื่อการวิจัยและนวัตกรรม**

(๑) ผู้วิจัยต้องยื่นคำขอใช้ข้อมูลและได้รับอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูลก่อนเข้าถึงข้อมูล

(๒) ข้อมูลที่ใช้ในการวิจัยควรผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้ (De-identification) เว้นแต่มีความจำเป็นและได้รับความยินยอมจากเจ้าของข้อมูล

(๓) การนำเทคโนโลยีวิเคราะห์ข้อมูลขั้นสูง เช่น ปัญญาประดิษฐ์ (AI) หรือ Machine Learning มาใช้กับข้อมูลสุขภาพ ต้องผ่านการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลก่อนดำเนินการ

**๖. การบันทึกและตรวจสอบการเข้าถึงข้อมูล (Audit Trail)**

(๑) ระบบสารสนเทศที่จัดเก็บข้อมูลผู้ป่วยต้องมีระบบบันทึกการเข้าถึงข้อมูล (Audit Log)

(๒) บันทึก Audit Log ต้องประกอบด้วยข้อมูลผู้ใช้งาน วันเวลา ประเภทการดำเนินการ และข้อมูลที่ถูกเข้าถึง

(๓) บันทึก Audit Log ต้องไม่สามารถแก้ไขหรือเปลี่ยนแปลงได้โดยผู้ใช้งานทั่วไป และต้องจัดเก็บตามระยะเวลาที่กำหนด

(๔) คณะทำงานบริกรข้อมูลต้องทบทวน Audit Log เป็นระยะเพื่อตรวจสอบความผิดปกติของการใช้งานข้อมูล

(๕) หากพบการเข้าถึงข้อมูลโดยมิชอบ ต้องรายงานต่อผู้บริหารและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามขั้นตอนที่กำหนด

## หมวด ๔ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล
## (Data Integration and Exchange Domain)

**๑. วัตถุประสงค์**

เพื่อกำหนดแนวทางในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโรงพยาบาลให้มีความมั่นคงปลอดภัย มีความถูกต้อง และเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง รวมทั้งกำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูล โดยเฉพาะข้อมูลสุขภาพที่มีการเชื่อมโยงกับหน่วยงานในระบบสาธารณสุข

**๒. ขอบเขต**

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลของโรงพยาบาลครอบคลุมการรับ การส่ง และการใช้ข้อมูลระหว่างหน่วยงานภายในและภายนอกองค์กร เพื่อสนับสนุนการให้บริการทางการแพทย์ การบริหารจัดการ และการบูรณาการข้อมูลด้านสุขภาพ โดยมีหลักการสำคัญ ดังนี้

- การกำหนดแนวทางการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัยและมีคุณภาพ
- การกำหนดกระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลอย่างเป็นระบบ ตั้งแต่ขั้นตอนการเตรียมการ การดำเนินการ และการติดตามผล
- การจัดทำเมทาดาตาและรายละเอียดของชุดข้อมูลที่ใช้ในการแลกเปลี่ยนข้อมูล
- การกำหนดข้อตกลงหรือสัญญาที่เกี่ยวข้องกับการใช้และการแลกเปลี่ยนข้อมูล
- การกำหนดมาตรฐานเทคโนโลยีสำหรับการแลกเปลี่ยนข้อมูล เช่น API มาตรฐาน และมาตรฐานข้อมูลสุขภาพสากล
- การจัดเก็บบันทึกข้อมูลการแลกเปลี่ยนข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้

**๓. แนวทางปฏิบัติและความรับผิดชอบ**

(๑) คณะทำงานบริกรข้อมูล (Data Steward Team) ต้องจัดทำมาตรฐานและรายละเอียดของชุดข้อมูลที่ใช้ในการเชื่อมโยงข้อมูล ทั้งในด้านเมทาดาตาทางธุรกิจและเมทาดาตาทางเทคนิค

(๒) การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกต้องมีข้อตกลงหรือสัญญาที่กำหนดวัตถุประสงค์ ขอบเขต และมาตรการรักษาความปลอดภัยของข้อมูล

(๓) โรงพยาบาลต้องกำหนดช่องทางหรือระบบสำหรับการขอใช้ข้อมูลและการเชื่อมโยงข้อมูลอย่างเป็นทางการ

(๔) การเชื่อมโยงข้อมูลต้องใช้เทคโนโลยีและมาตรฐานที่เหมาะสม เช่น API มาตรฐาน หรือมาตรฐานข้อมูลสุขภาพสากล

(๕) ต้องมีการบันทึกประวัติการรับ ส่ง และเชื่อมโยงข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้

(๖) โรงพยาบาลต้องสื่อสารหรืออบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจเกี่ยวกับแนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูล

**๔. การเชื่อมโยงข้อมูลกับหน่วยงานด้านสาธารณสุข**

โรงพยาบาลมีหน้าที่จัดส่งข้อมูลสุขภาพให้แก่หน่วยงานที่กำกับดูแลหรือหน่วยงานในระบบสาธารณสุขตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง เช่น

- สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.)
- กรมสนับสนุนบริการสุขภาพ
- หน่วยงานด้านระบาดวิทยา
- สถานพยาบาลเครือข่าย

การจัดส่งข้อมูลต้องเป็นไปตามมาตรฐานข้อมูลสุขภาพที่หน่วยงานกำหนด เช่น มาตรฐานข้อมูล ๔๓ แฟ้ม โรงพยาบาลต้องมีการตรวจสอบความถูกต้องและความครบถ้วนของข้อมูลก่อนส่ง และต้องดำเนินการแก้ไขข้อมูลเมื่อพบข้อผิดพลาด

**๕. การแลกเปลี่ยนข้อมูลกรณีส่งต่อผู้ป่วย**

การแลกเปลี่ยนข้อมูลผู้ป่วยระหว่างสถานพยาบาลต้องดำเนินการตามมาตรฐานการส่งต่อผู้ป่วยของกระทรวงสาธารณสุข โดยข้อมูลที่ส่งต่อควรประกอบด้วยข้อมูลสำคัญ เช่น

- ข้อมูลระบุตัวผู้ป่วย
- การวินิจฉัยโรคตามมาตรฐาน ICD
- ประวัติแพ้ยาและประวัติการรักษา
- ผลตรวจทางห้องปฏิบัติการหรือการตรวจทางการแพทย์ที่สำคัญ
- แผนการรักษา

กรณีการส่งต่อผู้ป่วยฉุกเฉิน สามารถแลกเปลี่ยนข้อมูลที่จำเป็นเพื่อความปลอดภัยของผู้ป่วยได้ทันที โดยต้องดำเนินการตามกฎหมายและบันทึกเหตุผลการดำเนินการ

**๖. ข้อตกลงและสัญญาการใช้ข้อมูล**

การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกต้องดำเนินการภายใต้ข้อตกลงหรือสัญญาที่กำหนดเงื่อนไขการใช้ข้อมูลอย่างชัดเจน เช่น

- บันทึกข้อตกลงความร่วมมือ (MOU)
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)

ข้อตกลงดังกล่าวต้องระบุวัตถุประสงค์ของการใช้ข้อมูล ประเภทข้อมูลที่ใช้ มาตรการรักษาความปลอดภัย และระยะเวลาของข้อตกลง รวมทั้งต้องมีการทบทวนข้อตกลงตามระยะเวลาที่กำหนด

## หมวด ๕ การเปิดเผยและการรักษาความลับข้อมูล
## (Data Disclosure and Confidentiality Domain)

**๑. วัตถุประสงค์**

เพื่อกำหนดแนวทางในการเปิดเผยและการรักษาความลับของข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ให้เป็นไปอย่างถูกต้องตามกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง โดยเฉพาะข้อมูลสุขภาพและข้อมูลส่วนบุคคลของผู้ป่วย ผู้รับบริการ และบุคลากร เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยมิชอบ และเพื่อให้การใช้ข้อมูลเกิดประโยชน์ต่อการให้บริการทางการแพทย์และการบริหารจัดการอย่างเหมาะสม

**๒. ขอบเขต**

การเปิดเผยและการรักษาความลับข้อมูลของโรงพยาบาลครอบคลุมการเผยแพร่ การแบ่งปัน และการให้สิทธิ์เข้าถึงข้อมูลแก่บุคลากรภายในองค์กร หน่วยงานภายนอก และสาธารณะ โดยกำหนดระดับการเปิดเผยข้อมูล ดังนี้

ตารางที่ ๖ ระดับการเปิดเผยข้อมูล

| ระดับการเปิดเผยข้อมูล | ลักษณะข้อมูล |
|---|---|
| ระดับที่ ๑ ข้อมูลภายใน (Internal Use) | ข้อมูลที่ใช้ภายในหน่วยงาน โดยควบคุมการเข้าถึงผ่านระบบยืนยันตัวตน |
| ระดับที่ ๒ ข้อมูลสำหรับหน่วยงานที่มีสิทธิ์ (Restricted Sharing) | ข้อมูลที่สามารถแลกเปลี่ยนกับหน่วยงานภายนอกภายใต้ข้อตกลงหรือสัญญา |
| ระดับที่ ๓ ข้อมูลเปิด (Open Data) | ข้อมูลสาธารณะที่สามารถเผยแพร่ได้โดยไม่กระทบต่อความเป็นส่วนตัวหรือกฎหมาย |

ทั้งนี้ ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ หรือข้อบังคับ รวมถึงข้อมูลสุขภาพของผู้ป่วยโดยไม่ได้รับอนุญาตหรือความยินยอมตามที่กฎหมายกำหนด

**๓. แนวทางปฏิบัติและความรับผิดชอบ**

(๑) คณะทำงานบริกรข้อมูล (Data Steward Team) ต้องกำหนดระดับการเปิดเผยข้อมูลของชุดข้อมูลแต่ละรายการให้ชัดเจน โดยให้เจ้าของข้อมูล (Data Owner) เป็นผู้พิจารณาอนุมัติ

(๒) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) มีหน้าที่กำหนดนโยบายและแนวทางการเปิดเผยข้อมูลของโรงพยาบาล รวมทั้งกำกับดูแลให้การดำเนินการเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

(๓) คณะทำงานบริกรข้อมูลร่วมกับเจ้าของข้อมูล ต้องกำกับดูแลการนำเข้า การปรับปรุง และการจัดเตรียมข้อมูลให้เหมาะสมสำหรับการเปิดเผยหรือการแลกเปลี่ยนข้อมูล

(๔) การคัดเลือกชุดข้อมูลที่สามารถเปิดเผยได้ ต้องพิจารณาจากระดับชั้นความลับของข้อมูล และต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือสิทธิความเป็นส่วนตัวของผู้ป่วยและผู้รับบริการ

(๕) ข้อมูลที่เปิดเผยต้องจัดเตรียมให้อยู่ในรูปแบบที่สามารถนำไปใช้ประโยชน์ได้อย่างเหมาะสม และต้องไม่สามารถระบุตัวบุคคลได้ในกรณีข้อมูลสาธารณะ

(๖) ต้องมีการบันทึกประวัติการเปิดเผยข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้

(๗) โรงพยาบาลต้องจัดให้มีการสื่อสารหรืออบรมบุคลากรเกี่ยวกับแนวทางการเปิดเผยและการรักษาความลับของข้อมูล

**๔. การเปิดเผยข้อมูลตามกฎหมาย**

โรงพยาบาลสามารถเปิดเผยข้อมูลโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลในกรณีที่กฎหมายกำหนด เช่น

- การเปิดเผยข้อมูลตามคำสั่งศาล หรือคำสั่งของเจ้าพนักงานตามกฎหมาย
- การรายงานข้อมูลตามกฎหมายด้านสาธารณสุข เช่น การรายงานโรคติดต่อ
- การรายงานข้อมูลด้านสถิติสุขภาพหรือข้อมูลที่หน่วยงานรัฐกำหนด

การเปิดเผยข้อมูลดังกล่าวต้องดำเนินการเฉพาะข้อมูลที่จำเป็น และต้องมีการบันทึกการดำเนินการเพื่อการตรวจสอบ

**๕. การเปิดเผยข้อมูลเพื่อการรักษาพยาบาล**

การเปิดเผยข้อมูลผู้ป่วยเพื่อการรักษาพยาบาลหรือการส่งต่อผู้ป่วย สามารถดำเนินการได้ภายใต้หลักการที่จำเป็นต่อการรักษา โดยข้อมูลที่เปิดเผยต้องเป็นข้อมูลที่จำเป็นต่อการดูแลรักษาผู้ป่วย และต้องดำเนินการผ่านระบบหรือช่องทางที่มีความปลอดภัย

**๖. การเปิดเผยข้อมูลเพื่อการบริหารจัดการและการเบิกจ่าย**

โรงพยาบาลอาจเปิดเผยข้อมูลผู้ป่วยต่อหน่วยงานที่เกี่ยวข้องกับการเบิกจ่ายค่ารักษาพยาบาล เช่น สำนักงานหลักประกันสุขภาพแห่งชาติ หรือหน่วยงานประกันสุขภาพ ตามกฎหมายหรือข้อตกลงที่เกี่ยวข้อง โดยต้องเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อการดำเนินการ

**๗. การเปิดเผยข้อมูลต่อครอบครัวหรือผู้ดูแล**

การเปิดเผยข้อมูลสุขภาพแก่ครอบครัวหรือผู้ดูแลต้องเป็นไปตามหลักเกณฑ์ดังนี้

- ต้องได้รับความยินยอมจากผู้ป่วย เว้นแต่กรณีที่กฎหมายกำหนดหรือเป็นกรณีฉุกเฉิน
- ผู้ปกครองตามกฎหมายสามารถรับข้อมูลสุขภาพของผู้เยาว์ได้
- การเปิดเผยข้อมูลต้องคำนึงถึงความเป็นส่วนตัวของผู้ป่วยเป็นสำคัญ

**๘. การคุ้มครองข้อมูลที่มีความอ่อนไหว**

ข้อมูลสุขภาพบางประเภท เช่น ข้อมูลด้านสุขภาพจิต โรคติดต่อทางเพศสัมพันธ์ หรือข้อมูลที่มีความอ่อนไหวสูง ต้องมีมาตรการควบคุมการเข้าถึงข้อมูลเป็นพิเศษ และต้องปฏิบัติตามกฎหมายหรือข้อกำหนดเฉพาะที่เกี่ยวข้อง

## หมวด ๖ มาตรฐานข้อมูล
## (Data Standard Domain)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรฐานรูปแบบและข้อกำหนดของข้อมูล เมทาดาตา และรหัสข้อมูลของโรงพยาบาลให้มีความสอดคล้องและสามารถเข้าใจได้ตรงกันทั้งหน่วยงาน รวมทั้งสนับสนุนให้ข้อมูลสุขภาพและข้อมูลการให้บริการสามารถนำไปใช้ประโยชน์ได้อย่างถูกต้อง และสามารถเชื่อมโยงกับระบบข้อมูลสุขภาพระดับประเทศและมาตรฐานสากลได้

**๒. ขอบเขต**

มาตรฐานข้อมูลของโรงพยาบาลครอบคลุมการกำหนดรูปแบบและข้อกำหนดของข้อมูล เมทาดาตา และชุดข้อมูล เพื่อให้ข้อมูลสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ โดยประกอบด้วยรายละเอียด ดังนี้

(๑) การกำหนดมาตรฐานเมทาดาตาสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล เจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา และสิทธิ์การเข้าถึง

(๒) การกำหนดมาตรฐานข้อมูลสุขภาพที่เกี่ยวข้อง เช่น ICD-๑๐, CPT (Current Procedural Terminology), SNOMED CT, HL๗ FHIR และมาตรฐาน ๔๓ แฟ้มข้อมูลสุขภาพ เป็นต้น

(๓) การกำหนดโครงสร้างข้อมูลและคำอธิบายข้อมูลหลักให้สอดคล้องกับมาตรฐานที่หน่วยงานภาครัฐกำหนด

(๔) การจัดทำพจนานุกรมข้อมูล (Data Dictionary) เพื่ออธิบายความหมาย โครงสร้าง และการใช้งานของข้อมูลภายในระบบของโรงพยาบาล

(๕) การจัดเก็บเมทาดาตาและข้อมูลคำอธิบายชุดข้อมูลในรูปแบบดิจิทัล เพื่อให้สามารถสืบค้น ใช้งาน และแลกเปลี่ยนข้อมูลได้อย่างสะดวก

**๓. แนวทางปฏิบัติและความรับผิดชอบ**

(๑) คณะทำงานบริกรข้อมูล (Data Steward Team) มีหน้าที่สำรวจ รวบรวม และจัดทำรายการชุดข้อมูลดิจิทัลของโรงพยาบาล โดยระบุแหล่งที่มาของข้อมูลแต่ละชุดอย่างเป็นระบบ

(๒) คณะทำงานบริกรข้อมูลต้องกำหนดรายการชุดข้อมูลสำคัญของโรงพยาบาล โดยพิจารณาจากความจำเป็นต่อการให้บริการ การบริหารจัดการ และการรายงานข้อมูลด้านสาธารณสุข

(๓) คณะทำงานบริกรข้อมูลต้องจัดทำเมทาดาตาและพจนานุกรมข้อมูลสำหรับชุดข้อมูลต่าง ๆ ของโรงพยาบาล เพื่อให้ผู้ใช้งานสามารถเข้าใจและใช้ข้อมูลได้อย่างถูกต้อง

(๔) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ต้องกำกับและทบทวนมาตรฐานข้อมูลของโรงพยาบาลให้สอดคล้องกับมาตรฐานสากลและข้อกำหนดของหน่วยงานที่เกี่ยวข้องอย่างสม่ำเสมอ

(๕) บุคลากรของโรงพยาบาลที่เกี่ยวข้องกับการสร้างหรือปรับปรุงข้อมูล ต้องปฏิบัติตามมาตรฐานข้อมูลที่กำหนด และแจ้งปัญหาหรือความไม่สอดคล้องของข้อมูลต่อคณะทำงานบริกรข้อมูลเพื่อดำเนินการปรับปรุง

## หมวด ๗ มาตรฐานการจัดชั้นความลับข้อมูล
## (Data Classification Standard Domain)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรฐานการจัดชั้นความลับของข้อมูลของโรงพยาบาล สำหรับการกำหนดสิทธิ์การเข้าถึง การใช้งาน และการเปิดเผยข้อมูลอย่างเหมาะสม โดยเฉพาะข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลสุขภาพ และข้อมูลส่วนบุคคลของผู้ป่วย เพื่อให้การบริหารจัดการข้อมูลมีความมั่นคงปลอดภัย และเป็นไปตามกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง

**๒. ขอบเขต**

โรงพยาบาลกำหนดระดับชั้นความลับของข้อมูล เพื่อใช้เป็นแนวทางในการควบคุมการเข้าถึง การใช้งาน และการเปิดเผยข้อมูล ดังนี้

ตารางที่ ๗ ระดับชั้นความลับของข้อมูล

| ระดับชั้นข้อมูล | ประเภทข้อมูล | ตัวอย่างข้อมูลในโรงพยาบาล |
|---|---|---|
| ชั้นเปิดเผย (Open) | ข้อมูลที่สามารถเผยแพร่สู่สาธารณะได้ | สถิติผู้รับบริการ ข้อมูลบริการที่มีให้ ตารางออกตรวจ |
| ชั้นเผยแพร่ภายใน (Internal) | ข้อมูลที่ใช้เฉพาะภายในองค์กร | รายงานประชุม แผนงานโรงพยาบาล เอกสารการดำเนินงานภายใน |
| ชั้นลับ (Confidential) | ข้อมูลที่เข้าถึงได้เฉพาะผู้มีสิทธิ์ | ประวัติการรักษาผู้ป่วย เวชระเบียน ผลตรวจทางห้องปฏิบัติการ |
| ชั้นลับมาก (Secret) | ข้อมูลที่มีความอ่อนไหวสูง | ข้อมูลสุขภาพจิต ข้อมูลโรคติดต่อทางเพศสัมพันธ์ ข้อมูลผู้ป่วยยาเสพติด |
| ชั้นลับที่สุด (Top Secret) | ข้อมูลที่มีผลกระทบสูงหากรั่วไหล | ข้อมูลที่เกี่ยวข้องกับความมั่นคง หรือข้อมูลเฉพาะที่ต้องได้รับการคุ้มครองเป็นพิเศษ |

**๓. แนวทางปฏิบัติและความรับผิดชอบ**

(๑) คณะทำงานบริกรข้อมูล (Data Steward Team) มีหน้าที่กำหนดระดับชั้นความลับของข้อมูลแต่ละชุด และเสนอให้คณะกรรมการธรรมาภิบาลข้อมูลพิจารณาให้ความเห็นชอบ

(๒) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ทำหน้าที่กำกับ ตรวจสอบ และให้ข้อเสนอแนะเกี่ยวกับการกำหนดระดับชั้นความลับของข้อมูลของโรงพยาบาล

(๓) คณะทำงานบริกรข้อมูลต้องทบทวนระดับชั้นความลับของข้อมูลและพจนานุกรมข้อมูลอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับลักษณะการใช้งานข้อมูลและข้อกำหนดที่เกี่ยวข้อง

(๔) เจ้าของข้อมูล (Data Owner) มีหน้าที่พิจารณาอนุมัติการเข้าถึงหรือการใช้ข้อมูล โดยคำนึงถึงระดับชั้นความลับของข้อมูลและวัตถุประสงค์ในการใช้งาน

(๕) ข้อมูลที่มีระดับชั้นความลับสูง เช่น ข้อมูลสุขภาพและข้อมูลส่วนบุคคล ต้องได้รับการควบคุมการเข้าถึงอย่างเหมาะสม และไม่สามารถเปิดเผยได้ เว้นแต่เป็นไปตามกฎหมายหรือได้รับอนุญาตตามระเบียบที่เกี่ยวข้อง

(๖) คณะทำงานบริกรข้อมูลต้องระบุระดับชั้นความลับของข้อมูลไว้ในเมทาดาตาของชุดข้อมูล เพื่อใช้เป็นข้อมูลประกอบในการบริหารจัดการข้อมูล

(๗) ต้องมีการจัดเก็บบันทึกการเข้าถึงข้อมูลในแต่ละระดับ เพื่อให้สามารถตรวจสอบและติดตามการใช้งานข้อมูลได้

(๘) โรงพยาบาลต้องมีการทบทวนระดับชั้นความลับของข้อมูลอย่างสม่ำเสมอ และปรับปรุงแนวทางการจัดชั้นข้อมูลให้เหมาะสมกับบริบทการดำเนินงานและข้อกำหนดทางกฎหมาย

## หมวด ๘ การคุ้มครองข้อมูลส่วนบุคคล
## (Personal Data Protection Domain)

**๑. วัตถุประสงค์**

เพื่อกำหนดหลักเกณฑ์และแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วย ผู้รับบริการ บุคลากร และบุคคลที่เกี่ยวข้องกับโรงพยาบาล ให้มีความมั่นคงปลอดภัยและเป็นไปตามกฎหมาย โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งเพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย หรือการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบ

**๒. ขอบเขต**

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนี้ใช้บังคับกับข้อมูลส่วนบุคคลของบุคคลที่มีความเกี่ยวข้องกับโรงพยาบาล ได้แก่

(๑) ผู้ป่วยและผู้รับบริการทุกประเภท รวมถึงผู้ที่มาติดต่อรับบริการ

(๒) ข้าราชการ พนักงาน ลูกจ้าง และอาสาสมัครของโรงพยาบาล

(๓) คู่สัญญา ผู้ให้บริการ หรือบุคคลภายนอกที่ดำเนินการประมวลผลข้อมูลแทนโรงพยาบาล

(๔) ผู้เข้าร่วมโครงการวิจัยทางการแพทย์หรือสาธารณสุขของโรงพยาบาล

(๕) ผู้สมัครงานหรือผู้สมัครเข้ารับการฝึกอบรมกับโรงพยาบาล

**๓. แนวทางปฏิบัติและความรับผิดชอบ**

**(๑) การเก็บรวบรวมข้อมูลส่วนบุคคล**

โรงพยาบาลอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลต่าง ๆ ได้แก่

- จากเจ้าของข้อมูลโดยตรง เช่น การลงทะเบียนเข้ารับบริการ การทำประวัติผู้ป่วย การสมัครงาน หรือการกรอกแบบฟอร์มรับบริการ
- จากการใช้งานระบบสารสนเทศของโรงพยาบาล เช่น ระบบทะเบียนผู้ป่วย ระบบเวชระเบียนอิเล็กทรอนิกส์ และระบบบริการสุขภาพอื่น
- จากหน่วยงานหรือแหล่งข้อมูลอื่นที่มีอำนาจตามกฎหมาย หรือได้รับความยินยอมจากเจ้าของข้อมูล เช่น การส่งต่อผู้ป่วยจากสถานพยาบาลอื่น หรือการเชื่อมโยงข้อมูลกับระบบสุขภาพของภาครัฐ

**(๒) วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล**

โรงพยาบาลอาจเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อการให้บริการด้านการแพทย์และสาธารณสุขแก่ผู้ป่วยและผู้รับบริการ

(๒) เพื่อการบริหารจัดการ การวางแผน และการพัฒนาคุณภาพบริการของโรงพยาบาล

(๓) เพื่อการดำเนินการตามภาระผูกพันทางกฎหมายหรือสัญญาของโรงพยาบาล

(๔) เพื่อการวิจัยทางการแพทย์และสาธารณสุขตามมาตรฐานจริยธรรมการวิจัย

(๕) เพื่อการรายงานข้อมูลด้านสุขภาพต่อหน่วยงานที่กำกับดูแล เช่น สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.) และหน่วยงานด้านสาธารณสุข

(๖) เพื่อการพิสูจน์ตัวตนและการรักษาความปลอดภัยของระบบสารสนเทศ

**(๓) ฐานทางกฎหมายในการประมวลผลข้อมูล**

โรงพยาบาลประมวลผลข้อมูลส่วนบุคคลตามฐานทางกฎหมายที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้แก่

- **ฐานสัญญา (Contract)**
  การประมวลผลเพื่อให้บริการทางการแพทย์ตามข้อตกลงระหว่างโรงพยาบาลกับผู้ป่วย
- **ฐานประโยชน์สำคัญ (Vital Interests)**
  การประมวลผลเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล โดยไม่ต้องขอความยินยอม
- **ฐานหน้าที่ตามกฎหมาย (Legal Obligation)**
  การรายงานโรคติดต่อ การรายงานเหตุการณ์ไม่พึงประสงค์ การส่งข้อมูลให้ สปสช. และหน่วยงานกำกับดูแล
- **ฐานประโยชน์สาธารณะ (Public Interest)**
  การเฝ้าระวังโรคระบาด การวิจัยทางการแพทย์ และการสาธารณสุข
- **ฐานความยินยอม (Consent)**
  กรณีที่ไม่มีฐานกฎหมายอื่น โรงพยาบาลต้องขอความยินยอมอย่างชัดแจ้งและเป็นลายลักษณ์อักษร โดยเฉพาะการใช้ข้อมูลเพื่อการวิจัยหรือวัตถุประสงค์อื่นนอกเหนือการรักษา

**(๔) การขอความยินยอม**

กรณีที่ต้องอาศัยความยินยอมในการประมวลผลข้อมูล โรงพยาบาลต้องดำเนินการ ดังนี้

(๑) จัดทำแบบฟอร์มขอความยินยอมที่ระบุวัตถุประสงค์ของการใช้ข้อมูลอย่างชัดเจน

(๒) ความยินยอมต้องแยกจากเงื่อนไขการรับบริการ และสามารถปฏิเสธได้

(๓) เจ้าของข้อมูลสามารถถอนความยินยอมได้ทุกเมื่อ

(๔) โรงพยาบาลต้องจัดเก็บหลักฐานการให้ความยินยอมตามระยะเวลาที่กฎหมายกำหนด

**(๕) ระยะเวลาการเก็บรักษาข้อมูล**

โรงพยาบาลกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามกฎหมายและความจำเป็นของภารกิจ เช่น

- เวชระเบียนผู้ป่วย เก็บรักษาไม่น้อยกว่า ๑๐ ปีนับจากวันที่มารับบริการครั้งสุดท้าย หรือตามกฎหมายกำหนด
- ข้อมูลบุคลากร เก็บรักษาตลอดระยะเวลาการจ้างงาน และต่อเนื่องตามระยะเวลาที่กฎหมายกำหนด
- บันทึก Log การเข้าถึงข้อมูล เก็บรักษาไม่น้อยกว่า ๙๐ วัน

เมื่อพ้นระยะเวลาการเก็บรักษา โรงพยาบาลต้องดำเนินการลบหรือทำลายข้อมูลตามขั้นตอนที่กำหนด

**(๖) การเปิดเผยข้อมูลส่วนบุคคล**

โรงพยาบาลอาจเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลหรือหน่วยงานภายนอกในกรณี ดังต่อไปนี้

- การเปิดเผยตามกฎหมายหรือคำสั่งของหน่วยงานรัฐ
- การส่งต่อผู้ป่วยระหว่างสถานพยาบาล
- การดำเนินงานตามสัญญาหรือภารกิจของโรงพยาบาล
- การประมวลผลข้อมูลโดยผู้ให้บริการภายนอก (Data Processor) ภายใต้สัญญาที่กำหนดมาตรการคุ้มครองข้อมูล

**(๗) สิทธิของเจ้าของข้อมูลส่วนบุคคล**

เจ้าของข้อมูลมีสิทธิ์ตามกฎหมาย ดังต่อไปนี้

- สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)
- สิทธิในการเข้าถึงข้อมูล (Right of Access)
- สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (Right to Rectification)
- สิทธิในการลบข้อมูล (Right to Erasure / Right to be Forgotten)
- สิทธิในการระงับการประมวลผลข้อมูล (Right to Restriction of Processing)
- สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)
- สิทธิในการคัดค้านการประมวลผลข้อมูล (Right to Object)

โรงพยาบาลต้องจัดให้มีช่องทางในการรับคำขอใช้สิทธิและดำเนินการตามระยะเวลาที่กฎหมายกำหนด

**(๘) มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล**

โรงพยาบาลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ครอบคลุมมาตรการดังนี้

- มาตรการด้านการบริหารจัดการ
- มาตรการด้านเทคนิคของระบบสารสนเทศ
- มาตรการด้านกายภาพของสถานที่จัดเก็บข้อมูล

รวมถึงกำหนดสิทธิ์การเข้าถึงข้อมูลตามหลัก Need-to-Know และ Least Privilege และต้องมีการบันทึกประวัติการเข้าถึงข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้

**(๙) การกำกับดูแลและการทบทวน**

โรงพยาบาลต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อกำกับดูแลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล และต้องมีการทบทวนมาตรการและแนวปฏิบัติด้านการคุ้มครองข้อมูลอย่างสม่ำเสมอ

## ๔. สรุปกรอบธรรมาภิบาลข้อมูล

การดำเนินงานด้านธรรมาภิบาลข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีวัตถุประสงค์เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพ โปร่งใส สามารถตรวจสอบได้ และสอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ รวมทั้งแนวทางการบริหารจัดการข้อมูลภาครัฐ (Data Governance Framework) ของประเทศไทย

โรงพยาบาลได้กำหนดกรอบธรรมาภิบาลข้อมูลเพื่อใช้เป็นแนวทางในการกำกับดูแล การบริหารจัดการและการใช้ประโยชน์จากข้อมูลของหน่วยงาน โดยครอบคลุมการดำเนินงานตลอดวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การเชื่อมโยงและแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการทำลายข้อมูล เพื่อให้ข้อมูลของโรงพยาบาลมีคุณภาพ มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถนำไปใช้ประโยชน์ได้อย่างเหมาะสม

นโยบายธรรมาภิบาลข้อมูลของโรงพยาบาลประกอบด้วย ๘ หมวด ได้แก่

หมวดที่ ๑ ทั่วไป
หมวดที่ ๒ การสร้าง การจัดเก็บ และการทำลายข้อมูล
หมวดที่ ๓ การประมวลผลและการใช้ข้อมูล
หมวดที่ ๔ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล
หมวดที่ ๕ การเปิดเผยและการรักษาความลับข้อมูล
หมวดที่ ๖ มาตรฐานข้อมูล
หมวดที่ ๗ มาตรฐานการจัดชั้นความลับข้อมูล
หมวดที่ ๘ การคุ้มครองข้อมูลส่วนบุคคล

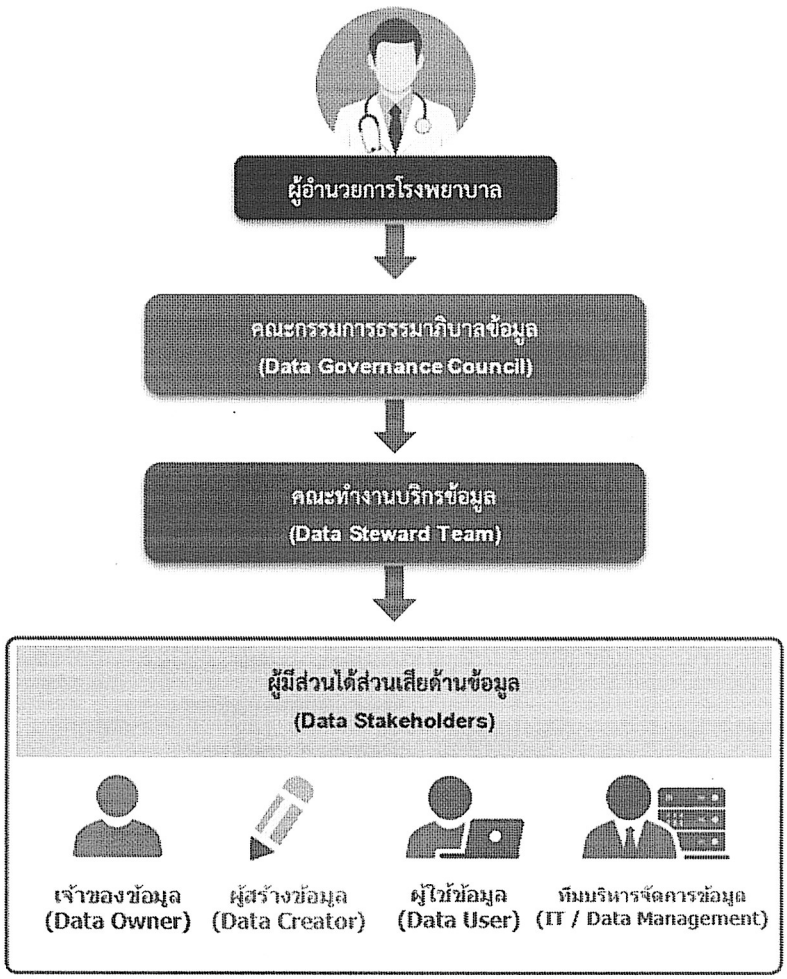
เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูลเป็นไปอย่างมีประสิทธิภาพ โรงพยาบาลได้กำหนดโครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการข้อมูลอย่างชัดเจน

โครงสร้างดังกล่าวประกอบด้วย ผู้อำนวยการโรงพยาบาลในฐานะผู้กำหนดนโยบายและให้การสนับสนุนการดำเนินงาน คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ทำหน้าที่กำหนดนโยบายและกำกับดูแลการบริหารจัดการข้อมูล คณะทำงานบริกรข้อมูล (Data Steward Team) ทำหน้าที่กำกับดูแลคุณภาพข้อมูลและมาตรฐานข้อมูล และผู้มีส่วนได้ส่วนเสียด้านข้อมูล (Data Stakeholders) ซึ่งประกอบด้วยเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และผู้ดูแลระบบเทคโนโลยีสารสนเทศ

ทั้งนี้ โครงสร้างดังกล่าวมีวัตถุประสงค์เพื่อให้การบริหารจัดการข้อมูลของโรงพยาบาลเป็นไปอย่างเป็นระบบ มีคุณภาพ มีความมั่นคงปลอดภัย และสามารถนำข้อมูลไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน และการให้บริการทางการแพทย์ได้อย่างมีประสิทธิภาพ

## ๕. โครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure)

การดำเนินงานด้านธรรมาภิบาลข้อมูลของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ได้กำหนดโครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของโรงพยาบาลให้เป็นไปอย่างเป็นระบบ โดยมีวัตถุประสงค์เพื่อให้ข้อมูลของโรงพยาบาลมีคุณภาพ มีความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการและการให้บริการทางการแพทย์ได้อย่างมีประสิทธิภาพ




รูปภาพที่ ๒ โครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) ของโรงพยาบาล

ตารางที่ ๘ บทบาทและความรับผิดชอบด้านการกำกับดูแลข้อมูล

| ระดับ / บทบาท | หน้าที่และความรับผิดชอบ |
|---|---|
| ผู้อำนวยการโรงพยาบาล | กำหนดนโยบายและทิศทางการดำเนินงานด้านธรรมาภิบาลข้อมูลของโรงพยาบาล รวมทั้งให้การสนับสนุนและกำกับดูแลการดำเนินงานในภาพรวม |
| คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) | กำหนดนโยบาย มาตรฐาน และแนวทางในการบริหารจัดการข้อมูลของโรงพยาบาล รวมทั้งกำกับ ติดตาม และประเมินผลการดำเนินงานด้านธรรมาภิบาลข้อมูล |
| คณะทำงานบริกรข้อมูล (Data Steward Team) | ดำเนินการกำกับดูแลคุณภาพข้อมูล มาตรฐานข้อมูล และการบริหารจัดการข้อมูลให้เป็นไปตามนโยบายที่กำหนด |
| เจ้าของข้อมูล (Data Owner) | รับผิดชอบข้อมูลของหน่วยงาน กำหนดสิทธิ์การเข้าถึงข้อมูล อนุมัติการใช้ข้อมูล และกำกับดูแลการใช้ข้อมูลให้เป็นไปตามวัตถุประสงค์ |
| ผู้สร้างข้อมูล (Data Creator) | บันทึก สร้าง และปรับปรุงข้อมูลให้ถูกต้อง ครบถ้วน และเป็นปัจจุบันตามมาตรฐานข้อมูลที่กำหนด |
| ผู้ใช้ข้อมูล (Data User) | ใช้ข้อมูลตามสิทธิ์ที่ได้รับและตามวัตถุประสงค์ของการใช้งาน โดยต้องปฏิบัติตามนโยบายและมาตรการรักษาความปลอดภัยข้อมูล |
| ผู้ดูแลระบบสารสนเทศ (IT / Data Management) | ดูแลระบบสารสนเทศ ฐานข้อมูล และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูลของโรงพยาบาล |
| ผู้มีส่วนได้ส่วนเสียด้านข้อมูล (Data Stakeholders) | บุคลากรหรือหน่วยงานที่เกี่ยวข้องกับการใช้ข้อมูลและการสนับสนุนการดำเนินงานด้านข้อมูลของโรงพยาบาล |