องค์การเภสัชกรรม
The Government Pharmaceutical Organization

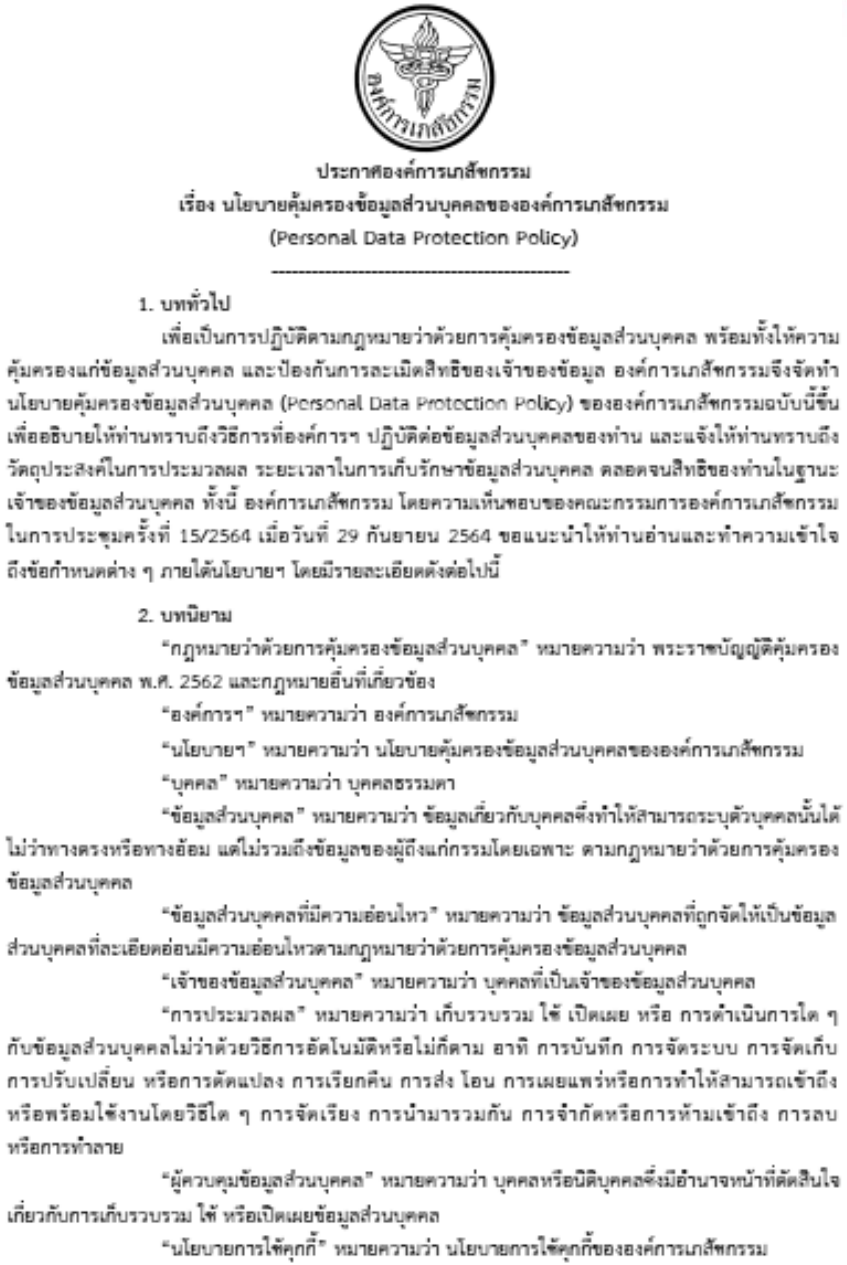
PDPA & Cyber Security Policies

Thanakrit Vilasmongkolchai
22 Sep 22

PDPA Policies

- แต่งตั้งคณะทำงาน PDPA
- ระบบการจัดเก็บข้อมูลส่วนบุคคล

- วิธีการปฏิบัติงานต่าง ๆที่เกี่ยวข้อง
- การสร้างความรู้ความเข้าใจในผู้ปฏิบัติงาน



ประกาศองค์การเภสัชกรรม
เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์การเภสัชกรรม
(Personal Data Protection Policy)

1. บททั่วไป

เพื่อเป็นการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งให้ความคุ้มครองแก่ข้อมูลส่วนบุคคล และป้องกันการละเมิดสิทธิของเจ้าของข้อมูล องค์การเภสัชกรรมจึงจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) ขององค์การเภสัชกรรมฉบับนี้ขึ้น เพื่ออธิบายให้ท่านทราบถึงวิธีการที่องค์การฯ ปฏิบัติต่อข้อมูลส่วนบุคคลของท่าน และแจ้งให้ท่านทราบถึงวัตถุประสงค์ในการประมวลผล ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล ตลอดจนสิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ องค์การเภสัชกรรม โดยความเห็นชอบของคณะกรรมการองค์การเภสัชกรรม ในการประชุมครั้งที่ 15/2564 เมื่อวันที่ 29 กันยายน 2564 ขอแนะนำให้ท่านอ่านและทำความเข้าใจถึงข้อกำหนดต่าง ๆ ภายใต้นโยบายฯ โดยมีรายละเอียดดังต่อไปนี้

2. บทนิยาม

"กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล" หมายความว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายอื่นที่เกี่ยวข้อง

"องค์การฯ" หมายความว่า องค์การเภสัชกรรม

"นโยบายฯ" หมายความว่า นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์การเภสัชกรรม

"บุคคล" หมายความว่า บุคคลธรรมดา

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

"ข้อมูลส่วนบุคคลที่มีความอ่อนไหว" หมายความว่า ข้อมูลส่วนบุคคลที่ถูกจัดให้เป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อนมีความอ่อนไหวตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

"เจ้าของข้อมูลส่วนบุคคล" หมายความว่า บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

"การประมวลผล" หมายความว่า เก็บรวบรวม ใช้ เปิดเผย หรือ การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลไม่ว่าด้วยวิธีการอัตโนมัติหรือไม่ก็ตาม อาทิ การบันทึก การจัดระบบ การจัดเก็บ การปรับเปลี่ยน หรือการดัดแปลง การเรียกคืน การส่ง โอน การเผยแพร่หรือการทำให้สามารถเข้าถึง หรือพร้อมใช้งานโดยวิธีใด ๆ การจัดเรียง การนำมารวมกัน การจำกัดหรือการห้ามเข้าถึง การลบ หรือการทำลาย

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"นโยบายการใช้คุกกี้" หมายความว่า นโยบายการใช้คุกกี้ขององค์การเภสัชกรรม

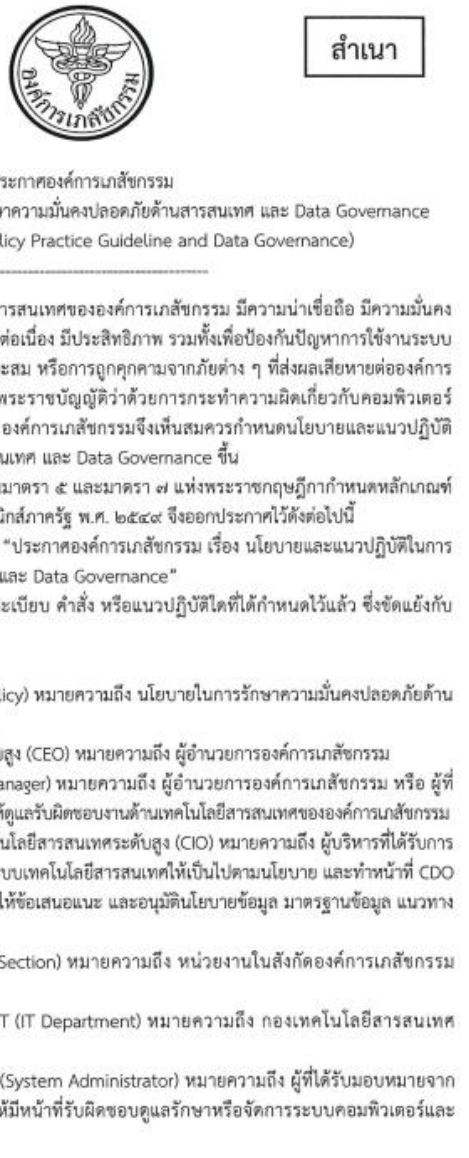
PDPA Policies

วิธีปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์การเภสัชกรรม

- แนวทางการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานต่าง ๆ ภายในองค์การเภสัชกรรม (WI-PDPA-GPO-001)
- แนวทางการดำเนินการจัดการข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลร้องขอ (WI-PDPA-GPO-002)
- แนวปฏิบัติเมื่อมีการร้องเรียนจากเจ้าของข้อมูลไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (WI-PDPA-GPO-003)
- แนวทางการรับมือเมื่อมีการรั่วไหลของข้อมูลส่วนบุคคล (WI-PDPA-GPO-004)
- การขอใช้สิทธิ์การเข้าถึง สร้าง แก้ไข และลบข้อมูล ในระบบการจัดการชุดข้อมูลส่วนบุคคล (PDPA CKAN) (WI-PDPA-GPO-005)

Cyber Security Policy

- นโยบายการเข้าถึงหรือควบคุมการใช้งานกับระบบสารสนเทศ
- นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ
- นโยบายการตรวจสอบและการประเมินความเสี่ยง
- นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์



สำเนา

ประกาศองค์การเภสัชกรรม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance
(Information Security Policy Practice Guideline and Data Governance)

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม มีความน่าเชื่อถือ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม หรือการถูกคุกคามจากภัยต่าง ๆ ที่ส่งผลเสียหายต่อองค์การเภสัชกรรม ซึ่งอาจเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง องค์การเภสัชกรรมจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance ขึ้น

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า "ประกาศองค์การเภสัชกรรม เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance"

ข้อ ๒. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๓. ในประกาศนี้

๓.๑ นโยบาย (Policy) หมายความถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance

๓.๒ ผู้บริหารระดับสูง (CEO) หมายความถึง ผู้อำนวยการองค์การเภสัชกรรม

๓.๓ ผู้บริหาร (Manager) หมายความถึง ผู้อำนวยการองค์การเภสัชกรรม หรือ ผู้ที่ผู้อำนวยการองค์การเภสัชกรรมมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม

๓.๔ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หมายความถึง ผู้บริหารที่ได้รับการมอบหมายหน้าที่ให้กำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามนโยบาย และทำหน้าที่ CDO (Chief Data Officer) โดยกำหนดทิศทาง ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติตามเกณฑ์คุณภาพ

๓.๕ หน่วยงาน (Section) หมายความถึง หน่วยงานในสังกัดองค์การเภสัชกรรมทุกระดับ

๓.๖ หน่วยงาน IT (IT Department) หมายความถึง กองเทคโนโลยีสารสนเทศ องค์การเภสัชกรรม

๓.๗ ผู้ดูแลระบบ (System Administrator) หมายความถึง ผู้ที่ได้รับมอบหมายจากผู้อำนวยการกองเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๓.๘ เจ้าของข้อมูล...

Cyber Security Policy