



องค์การเภสัชกรรม

The Government Pharmaceutical Organization

PDPA & Cyber Security Policies



Thanakrit Vilasmongkolchai
22 Sep 22



PDPA Policies

- แต่งตั้งคณะทำงาน PDPA
- ระบบการจัดเก็บข้อมูลส่วนบุคคล

ชุดข้อมูลส่วนบุคคลของ GPO

ท่านสามารถเข้าชมข้อมูลส่วนบุคคลขององค์การเภสัชกรรม (PDPA) ซึ่งรวบรวมเอกสารและข้อมูลที่เกี่ยวข้องเพื่อใช้ในการสื่อสารด้านการจัดการข้อมูลส่วนบุคคลซึ่งใช้ภายในองค์กรเท่านั้น ผ่านทางระบบ CKAN ที่ปุ่มด้านล่างนี้

เข้าสู่ระบบ CKAN

- วิธีการปฏิบัติงานต่างๆที่เกี่ยวข้อง
- การสร้างความรู้ความเข้าใจในผู้ปฏิบัติงาน



ประกาศองค์การเภสัชกรรม
เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์การเภสัชกรรม
(Personal Data Protection Policy)

1. บททั่วไป

เพื่อเป็นการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งให้ความคุ้มครองแก่ข้อมูลส่วนบุคคล และป้องกันการละเมิดสิทธิของเจ้าของข้อมูล องค์การเภสัชกรรมจึงจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) ขององค์การเภสัชกรรมฉบับนี้ขึ้นเพื่ออธิบายให้ท่านทราบถึงวิธีการที่องค์การฯ 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 ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายความว่า ข้อมูลส่วนบุคคลที่ถูกจัดให้เป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อนมีความอ่อนไหวตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

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

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“นโยบายการให้คุกกี้” หมายความว่า นโยบายการใช้คุกกี้ขององค์การเภสัชกรรม

PDPA Policies

วิธีปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์การเภสัชกรรม

GPO | PDPA

PDPA (Personal Data Protection Act) คืออะไร

PDPA เป็นกฎหมายว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต

PDPA เกี่ยวข้องกับองค์การเภสัชกรรมอย่างไร

เนื่องจากองค์การเภสัชกรรมมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งลูกค้า คู่ค้า ผู้ปฏิบัติงาน และผู้มีส่วนได้ส่วนเสีย ที่ติดต่อกับองค์การเภสัชกรรม ซึ่งผู้ปฏิบัติงานขององค์การเภสัชกรรมก็มีส่วนในการควบคุมข้อมูลส่วนบุคคลเหล่านั้นด้วย

ประโยชน์ที่ได้รับจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- รับทราบวัตถุประสงค์ของการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลอย่างชัดเจน
- ขอให้ลบ ทำลาย หรือขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้
- สามารถร้องเรียนและขอให้ชดเชยค่าเสียหายทดแทน หากมีการใช้ข้อมูลฯ นอกเหนือจากวัตถุประสงค์ที่แจ้งไว้แต่แรก
- ลดความเสี่ยงต่อชื่อเสียง หรือความเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคล

***กฎหมาย PDPA Thailand (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ได้ประกาศไว้ในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 ผ่าน โฆษน์ได้รื้อฟื้นทั้งโทษทางแพ่ง ทางอาญา และทางปกครอง

ผลิตภัณฑ์ : กองประชาสัมพันธ์ องค์การเภสัชกรรม



บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลซึ่งมีอำนาจหน้าที่ในการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลซึ่งมีหน้าที่ดำเนินการตามคำสั่งหรือการมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

GPO | PDPA

Personal Data

ข้อมูลส่วนบุคคล (Personal Data)
ข้อมูลเกี่ยวกับบุคคลที่อาจเป็นอันตรายต่อ 1. มาตรการป้องกันข้อมูล

โทรศัพท์

อีเมล

บัตรประชาชน

ที่อยู่

รถยนต์

บัตรเครดิต

พาสปอร์ต

บัญชีธนาคาร

โซเชียลมีเดีย

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

ศาสนา

เชื้อชาติ

ความคิดเห็นทางการเมือง

วิถีทางเพศ

สุขภาพ

ข้อมูลพันธุกรรม

GPO | PDPA

หน้าที่

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- 1. จัดทำนโยบาย PDPA
- 2. จัดทำแผนการปฏิบัติตาม PDPA
- 3. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 4. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 5. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 6. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- 1. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 2. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 3. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 4. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 5. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- 6. จัดทำเอกสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล

GPO | PDPA

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)

1. สิทธิในการเข้าถึงข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอเข้าถึงข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวม ใช้ หรือเปิดเผย

2. สิทธิในการลบข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ลบหรือทำลายข้อมูลส่วนบุคคล หรือขอให้ระงับการใช้ข้อมูลส่วนบุคคล

3. สิทธิในการแก้ไขข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง

4. สิทธิในการระงับการใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ระงับการใช้ข้อมูลส่วนบุคคล

5. สิทธิในการโอนข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอให้โอนข้อมูลส่วนบุคคลไปยังผู้ให้บริการอื่น

6. สิทธิในการคัดค้านการประมวลผลข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถขอให้คัดค้านการประมวลผลข้อมูลส่วนบุคคล

GPO | PDPA

Cyber Security Policy

- นโยบายการเข้าถึงหรือควบคุมการใช้งานกับระบบสารสนเทศ
- นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ
- นโยบายการตรวจสอบและการประเมินความเสี่ยง
- นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์



สำเนา

ประกาศองค์การเภสัชกรรม

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

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม มีความน่าเชื่อถือ มีความมั่นคง ปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม หรือการถูกคุกคามจากภัยต่าง ๆ ที่ส่งผลกระทบต่อองค์การเภสัชกรรม 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) หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance

๓.๒ ผู้บริหารระดับสูง (CEO) หมายความว่า ผู้อำนวยการองค์การเภสัชกรรม

๓.๓ ผู้บริหาร (Manager) หมายความว่า ผู้อำนวยการองค์การเภสัชกรรม หรือ ผู้อำนวยการองค์การเภสัชกรรมมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์การเภสัชกรรม

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

๓.๕ หน่วยงาน (Section) หมายความว่า หน่วยงานในสังกัดองค์การเภสัชกรรม

๓.๖ หน่วยงาน IT (IT Department) หมายความว่า กองเทคโนโลยีสารสนเทศ องค์การเภสัชกรรม

๓.๗ ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้อำนวยการกองเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

Cyber Security Policy

NEW What's new?

Information Security Policies

ISMS-PL-001 Rev. 01
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ Data Governance

NEW What's new?

ประกาศองค์การเกสัชกรรม

ประกาศองค์การเกสัชกรรม เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ได้รับการทบทวน เมื่อวันที่ 12 มิถุนายน 2563

[คลิกเพื่ออ่านข้อมูลเพิ่มเติม](#)

NEW What's new?

แจ้งเตือน ระวัง Email spam !!

เนื่องด้วยในขณะนี้ มีการส่งอีเมลหลอกล่อให้ทำการต่ออายุ อัปเดต หรือลงทะเบียน Email ของท่าน

ห้าม!! ทำการคลิก link ใดๆทั้งสิ้น
 เนื่องจากเป็นการหลอกล่อเอาข้อมูล

NEW What's new?

Ransomware ป้องกันอย่างไร

รับมือได้แค่ไหน
 ข้อเสนอแนะจาก CAT cyfence

ThaiCERT แจ้งเตือนภัย Ransomware และข้อเสนอแนะในการป้องกันความเสียหาย

รูปแบบการโจมตีของ Ransomware เพื่อยึดข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อ

- ผู้ไม่ประสงค์ดีส่งอีเมลหรือข้อความที่มีไฟล์แนบที่เป็นอันตรายไปยังผู้ใช้งาน
- ผู้ใช้งานดาวน์โหลดไฟล์แนบดังกล่าว
- ไฟล์แนบดังกล่าวทำงานและติดตั้งซอฟต์แวร์ที่เป็นอันตรายลงในเครื่องคอมพิวเตอร์ของเหยื่อ
- ซอฟต์แวร์ที่เป็นอันตรายทำการเข้ารหัสข้อมูลสำคัญของเหยื่อ
- ผู้ใช้งานต้องจ่ายค่าไถ่เพื่อให้ได้ข้อมูลกลับคืนมา
- ผู้ไม่ประสงค์ดีส่งอีเมลหรือข้อความที่มีไฟล์แนบที่เป็นอันตรายไปยังผู้ใช้งาน

ข้อเสนอแนะในการป้องกันความเสียหายจากภัย Ransomware

- ดำเนินการกักกันเพื่อรักษาความปลอดภัยของข้อมูล
- สำรองข้อมูลสำคัญที่ใช้บ่อยอย่างสม่ำเสมอ
- ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ
- สร้างความตระหนักรู้ในการใช้โซเชียลมีเดีย
- ไม่คลิกลิงก์หรือเปิดไฟล์ที่มากับอีเมลที่น่าสงสัย
- ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น
- ในกรณีที่เกิดเป็นเหยื่อ
- ติดต่อขอความช่วยเหลือจากหน่วยงานที่เกี่ยวข้อง
- ให้ติดต่อหน่วยงานที่ IT ของหน่วยงานท่าน

ThaiCERT | ThaiCERT | thaicert.or.th | ThaiCERT | ETDA | ICT