ชี้แจงการดำเนินงานตามกฎหมาย PDPA และ Cyber และแผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud

วันที่ 7 มิถุนายน 2565 เวลา 13.30 น.

นายแพทย์ธงชัย เลิศวิไลรัตนพงศ์

รองปลัดกระทรวงสาธารณสุข

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ประจำกระทรวงสาธารณสุข

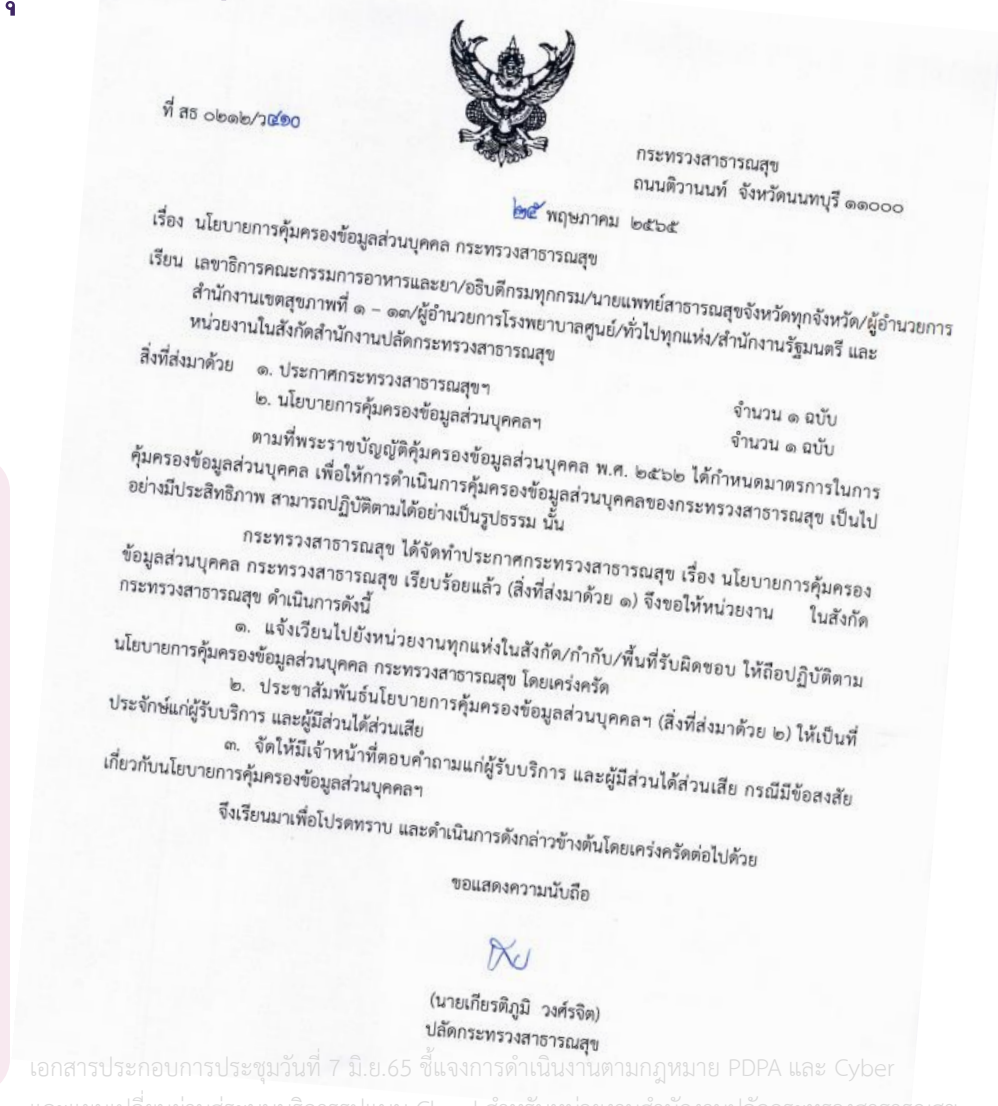
แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกระทรวงสาธารณสุข

ประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกระทรวงสาธารณสุข ครั้งที่ 2/2565 เมื่อวันที่ 18 พ.ค. 65 มีมติดังนี้

1) เห็นชอบ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กระทรวงสาธารณสุข และให้จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

ดำเนินการแล้ว :

- ✓ นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข
(รหัสเอกสาร : M–IT–SP–04Rev.00) หนังสือเวียน ที่ สธ 0212/ว 410 ลว. 25 พ.ค.65
- ✓ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข
(รหัสเอกสาร P-IT-SP-03.01Rev.00) หนังสือเวียน ที่ สธ 0212/ว 11424 ลว. 25 พ.ค.65
- ✓ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข
(รหัสเอกสาร P-IT-SP-03.02Rev.00) หนังสือเวียน ที่ สธ 0212/ว 11377 ลว. 25 พ.ค.65
- ✓ หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข (สำหรับผู้มาติดต่อเพื่อรับบริการทางการแพทย์และสาธารณสุข)
(รหัสเอกสาร F-IT-AC-07.02Rev.00) หนังสือเวียน ที่ สธ 0212/ว 11460 ลว. 26 พ.ค.65



ที่ สธ ๐๒๑๒/ว๔๑๐

กระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๕ พฤษภาคม ๒๕๖๕

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ – ๑๓/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง/สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย ๑. ประกาศกระทรวงสาธารณสุขฯ จำนวน ๑ ฉบับ
๒. นโยบายการคุ้มครองข้อมูลส่วนบุคคลฯ จำนวน ๑ ฉบับ

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม นั้น

กระทรวงสาธารณสุข ได้จัดทำประกาศกระทรวงสาธารณสุข เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข เรียบร้อยแล้ว (สิ่งที่ส่งมาด้วย ๑) จึงขอให้หน่วยงานในสังกัดกระทรวงสาธารณสุข ดำเนินการดังนี้

๑. แจ้งเวียนไปยังหน่วยงานทุกแห่งในสังกัด/กำกับ/พื้นที่รับผิดชอบ ให้ถือปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข โดยเคร่งครัด

๒. ประชาสัมพันธ์นโยบายการคุ้มครองข้อมูลส่วนบุคคลฯ (สิ่งที่ส่งมาด้วย ๒) ให้เป็นที่ประจักษ์แก่ผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย

๓. จัดให้มีเจ้าหน้าที่ตอบคำถามแก่ผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย กรณีมีข้อสงสัยเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคลฯ

จึงเรียนมาเพื่อโปรดทราบ และดำเนินการดังกล่าวข้างต้นโดยเคร่งครัดต่อไปด้วย

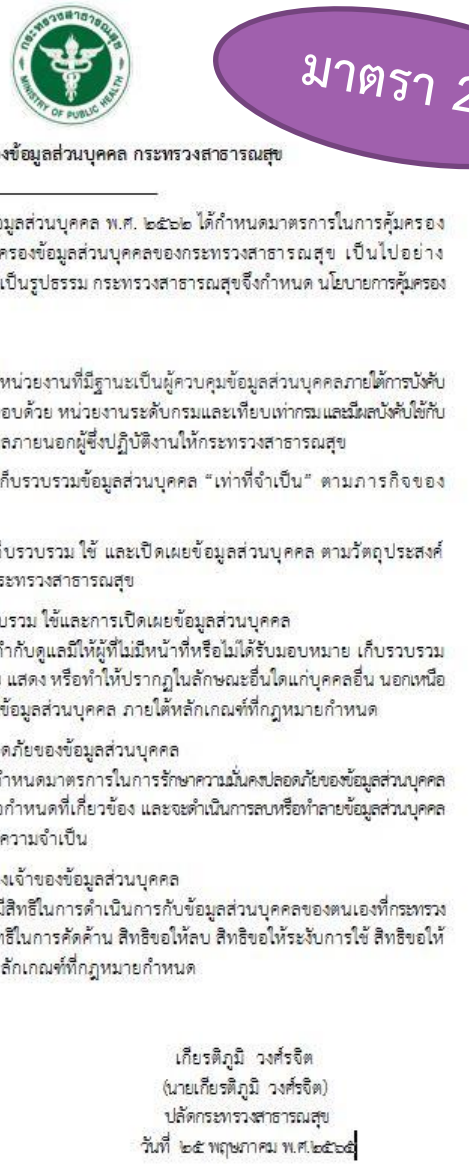
ขอแสดงความนับถือ

(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข

เอกสารประกอบการประชุมวันที่ 7 มิ.ย.65 ชี้แจงการดำเนินงานตามกฎหมาย PDPA และ Cyber และแผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud สำหรับหน่วยงานสำนักงานปลัดกระทรวงสาธารณสุข

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกระทรวงสาธารณสุข

มาตรา 23



นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม กระทรวงสาธารณสุขจึงกำหนด นโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ดังต่อไปนี้

ขอบเขตการบังคับใช้

"กระทรวงสาธารณสุข" หมายถึง หน่วยงานที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การบังคับบัญชาของปลัดกระทรวงสาธารณสุข ประกอบด้วย หน่วยงานระดับกรมและเทียบเท่ากรม และมีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงานและบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้กระทรวงสาธารณสุข

ข้อ ๑. กระทรวงสาธารณสุข จะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" ตามภารกิจของกระทรวงสาธารณสุข

ข้อ ๒. กระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ในการดำเนินงาน ภายใต้อำนาจหน้าที่ของกระทรวงสาธารณสุข

ข้อ ๓. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมาย เก็บรวบรวมข้อมูลส่วนบุคคลนำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ที่ได้กำหนดไว้ แต่อาจเปิดเผยข้อมูลส่วนบุคคล ภายใต้หลักเกณฑ์ที่กฎหมายกำหนด

ข้อ ๔. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเป็นไปตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง และจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็น

ข้อ ๕. สิทธิและการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการกับข้อมูลส่วนบุคคลของตนเองที่กระทรวงสาธารณสุขดูแล ได้แก่ สิทธิขอรับข้อมูล สิทธิในการคัดค้าน สิทธิขอให้ลบ สิทธิขอให้ระงับการใช้ สิทธิขอให้แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่กฎหมายกำหนด

เกียรติภูมิ วงศ์รจิต
(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข
วันที่ ๒๕ พฤษภาคม พ.ศ.๒๕๖๕

รหัสเอกสาร : M-IT-SP-04Rev.00

ขอบเขตการบังคับใช้

"กระทรวงสาธารณสุข" หมายถึง หน่วยงานที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การบังคับบัญชาของปลัดกระทรวงสาธารณสุข ประกอบด้วย หน่วยงานระดับกรมและเทียบเท่ากรม และมีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงานและบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้กระทรวงสาธารณสุข

ข้อ ๑. กระทรวงสาธารณสุข จะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" ตามภารกิจของกระทรวงสาธารณสุข

ข้อ ๒. กระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ในการดำเนินงาน ภายใต้อำนาจหน้าที่ของกระทรวงสาธารณสุข

ข้อ ๓. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมาย เก็บรวบรวมข้อมูลส่วนบุคคลนำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ที่ได้กำหนดไว้ แต่อาจเปิดเผยข้อมูลส่วนบุคคล ภายใต้หลักเกณฑ์ที่กฎหมายกำหนด

ข้อ ๔. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข จะกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเป็นไปตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง และจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็น

ข้อ ๕. สิทธิและการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการกับข้อมูลส่วนบุคคลของตนเองที่กระทรวงสาธารณสุขดูแล ได้แก่ สิทธิขอรับข้อมูล สิทธิในการคัดค้าน สิทธิขอให้ลบ สิทธิขอให้ระงับการใช้ สิทธิขอให้แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่กฎหมายกำหนด

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

ที่ สธ ๐๒๑๒/ว ๑๑๕๒๕ สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๕ พฤษภาคม ๒๕๖๕

เรื่อง แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑-๑๓ /ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง/สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข จำนวน ๑ ฉบับ

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะมีผลบังคับใช้โดยสมบูรณ์ในวันที่ ๑ มิถุนายน ๒๕๖๕ กระทรวงสาธารณสุข โดยสำนักงานปลัดกระทรวง จึงได้จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข เพื่อให้หน่วยงานระดับกรมในสังกัดและในกำกับของกระทรวงสาธารณสุข ได้ถือปฏิบัติและนำไปจัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม นั้น

สำนักงานปลัดกระทรวงสาธารณสุข จึงขอส่งแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข รายละเอียดตามสิ่งที่ส่งมาด้วย เพื่อให้หน่วยงานระดับกรม ได้ถือปฏิบัติและนำไปจัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน พร้อมทั้งสื่อสารให้หน่วยงานในสังกัดและในกำกับปฏิบัติตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานโดยเคร่งครัด

จึงเรียนมาเพื่อโปรดดำเนินการต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายธงชัย เลิศวิไลรัตนพงศ์)
รองปลัดกระทรวงสาธารณสุข
ปฏิบัติหน้าที่ผู้บริหารข้อมูลระดับสูง (CDO)
ประจำกระทรวงสาธารณสุข

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

เพื่อให้เป็นไปตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุขจึงได้กำหนดแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลไว้ดังต่อไปนี้

ส่วนที่ ๑. ผู้มีหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานของกระทรวงสาธารณสุข หมายถึง หน่วยงานที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การบังคับบัญชาของปลัดกระทรวงสาธารณสุขซึ่งประกอบ หน่วยงานระดับกรมและเทียบเท่ากรม จำนวน ๙ หน่วยงาน ได้แก่

๑. สำนักงานปลัดกระทรวงสาธารณสุข
๒. กรมสุขภาพจิต
๓. กรมควบคุมโรค
๔. กรมอนามัย
๕. กรมการแพทย์
๖. กรมวิทยาศาสตร์การแพทย์
๗. กรมสนับสนุนบริการสุขภาพ
๘. กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
๙. สำนักงานคณะกรรมการอาหารและยา

มีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงาน รวมถึงบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้หน่วยงานของกระทรวงสาธารณสุข

ส่วนที่ ๒. ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง

๑. ข้อมูลส่วนบุคคลของบุคลากรหน่วยงานของกระทรวงสาธารณสุข

เป็นข้อมูลส่วนบุคคลของ ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างประจำ ลูกจ้างชั่วคราว ของหน่วยงานในสังกัดหน่วยงานของกระทรวงสาธารณสุข

๒. ข้อมูลส่วนบุคคลของผู้มาติดต่องาน

เป็นข้อมูลส่วนบุคคลของ ผู้มาติดต่องาน สมัครงาน การทำธุรกรรม เช่น การขอใบอนุญาตต่าง ๆ การส่งตรวจสิ่งส่งตรวจทางห้องปฏิบัติการ เป็นต้น การทำนิติกรรม เช่น การทำสัญญาว่าจ้าง สัญญาซื้อขาย รวมถึงข้อมูลส่วนบุคคลของพนักงานหรือลูกจ้างของหน่วยงานที่ทำสัญญา หรือทำงานให้กับหน่วยงานของกระทรวงสาธารณสุข

ส่วนที่ ๑๐. การเปิดเผยเกี่ยวกับการดำเนินการ นโยบายและแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล

กระทรวงสาธารณสุข มีการดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กระทรวงสาธารณสุข โดยจะเผยแพร่ผ่านทางเว็บไซต์ https://pdpa.moph.go.th และเว็บไซต์ของหน่วยงาน รวมทั้งหากมีการปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็จะดำเนินการเผยแพร่ผ่านช่องทางดังกล่าว รวมทั้งผ่านสื่อที่กระทรวงสาธารณสุขใช้เพื่อการประชาสัมพันธ์ตามความเหมาะสมด้วย

(นายธงชัย เลิศวิไลรัตนพงศ์)
รองปลัดกระทรวงสาธารณสุข
ผู้บริหารข้อมูลระดับสูง ประจำกระทรวงสาธารณสุข

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

ที่ สธ ๐๒๑๒/ว ๑๑๓๗๗ สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๖ พฤษภาคม ๒๕๖๕

เรื่อง แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข

เรียน นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/สำนักงานเขตสุขภาพที่ ๑ – ๑๓/ผู้อำนวยการโรงพยาบาลศูนย์ ทั่วไปทุกแห่ง/สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข จำนวน ๑ ฉบับ

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะมีผลบังคับใช้โดยสมบูรณ์ในวันที่ ๑ มิถุนายน ๒๕๖๕ สำนักงานปลัดกระทรวงสาธารณสุข จึงได้จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข เพื่อให้หน่วยงานภายในสังกัดและในกำกับของสำนักงานปลัดกระทรวงสาธารณสุข ได้ถือปฏิบัติและนำไปจัดทำคู่มือปฏิบัติงานตามภารกิจที่ได้รับมอบหมาย นั้น

ในการนี้สำนักงานปลัดกระทรวงสาธารณสุข จึงขอส่งแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข รายละเอียดตามสิ่งที่ส่งมาด้วย เพื่อให้หน่วยงานในสังกัดและในกำกับของสำนักงานปลัดกระทรวงสาธารณสุข ได้ถือปฏิบัติและนำไปจัดทำคู่มือปฏิบัติงานตามภารกิจที่ได้รับมอบหมาย เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม พร้อมทั้งสื่อสารให้เจ้าหน้าที่และหน่วยงานที่เกี่ยวข้องปฏิบัติตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลโดยเคร่งครัด

จึงเรียนมาเพื่อโปรดดำเนินการต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายอนันต์ กนกศิลป์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ปฏิบัติหน้าที่ผู้บริหารข้อมูลระดับสูง (CDO)
ประจำสำนักงานปลัดกระทรวงสาธารณสุข

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุขในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลกระทรวงสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุขจึงได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ไว้ดังต่อไปนี้

ส่วนที่ ๑. ผู้มีหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานภายใต้สำนักงานปลัดกระทรวงสาธารณสุขซึ่งประกอบ หน่วยงานในส่วนกลางและส่วนภูมิภาค ดังนี้

๑. ราชการบริหารส่วนกลาง ๑๕ หน่วยงาน

๑. กองการพยาบาล
๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๓. กองยุทธศาสตร์และแผนงาน
๔. กองตรวจราชการ
๕. กองบริหารการสาธารณสุข
๖. กองกลาง
๗. กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ
๘. กองบริหารการคลัง
๙. กองบริหารทรัพยากรบุคคล
๑๐. กองการต่างประเทศ
๑๑. กองกฎหมาย
๑๒. กองสาธารณสุขฉุกเฉิน
๑๓. ศูนย์ปฏิบัติการต่อต้านการทุจริต
๑๔. กลุ่มพัฒนาระบบบริหาร
๑๕. กลุ่มตรวจสอบภายใน

๒. หน่วยงานตามภารกิจเฉพาะ ๑๖ หน่วยงาน

๑. สำนักตรวจราชการ กระทรวงสาธารณสุข
๒. สำนักวิชาการสาธารณสุข
๓. สำนักงานรัฐมนตรี
๔. กลุ่มเสริมสร้างวินัยและระบบคุณธรรม
๕. สำนักสารนิเทศ
๖. สำนักงานบริหารโครงการร่วมผลิตแพทย์เพิ่มเพื่อชาวชนบท

๑๑.๔ สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล โดยขอให้สำนักงานปลัดงกระทรวงสาธารณสุข ระงับการใช้ข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

๑๑.๕ สิทธิขอให้แก้ไขเปลี่ยนแปลง โดยขอให้ สำนักงานปลัดงกระทรวงสาธารณสุข ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ส่วนที่ ๑๒. แนวทางการคุ้มครองข้อมูลส่วนบุคคล

สำนักงานปลัดกระทรวงสาธารณสุข ได้มีการแต่งตั้งเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อการประสานงานในการคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลและสิทธิประโยชน์ของสำนักงานปลัดกระทรวงสาธารณสุข ช่วยให้สามารถบริหารความเสี่ยงและจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและประสิทธิผล ในกรณีที่เจ้าของข้อมูลต้องการใช้สิทธิ หรือมีคำถามเกี่ยวกับการใช้สิทธิของตน หรือความยินยอมที่เจ้าของข้อมูลได้ให้ไว้ สามารถติดต่อได้ที่ ส่งถึง : เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข
อาคาร ๒ ชั้น ๑ เลขที่ ๘๘/๒๐ หมู่๔ ถนนติวานนท์
ตำบลตลาดขวัญ อำเภอเมือง จังหวัดนนทบุรี ๑๑๐๐๐
อีเมล dpo@moph.go.th
โทรศัพท์ ๐ ๒๕๙๐ ๑๒๑๔

ส่วนที่ ๑๓. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติและนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

๑๓.๑ สำนักงานปลัดกระทรวงสาธารณสุข มีการดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กระทรวงสาธารณสุข โดยจะเผยแพร่ผ่านทางเว็บไซต์ https://pdpa.moph.go.th รวมทั้งหากมีการปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็จะดำเนินการเผยแพร่ผ่านช่องทางดังกล่าว รวมทั้งผ่านสื่อที่กระทรวงสาธารณสุขใช้เพื่อการประชาสัมพันธ์ตามความเหมาะสมด้วย

๑๓.๒ การดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ สำนักงานปลัดกระทรวงสาธารณสุข ประกาศใช้นี้ จะใช้เฉพาะสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกิจการของ สำนักงานปลัดกระทรวงสาธารณสุข ซึ่งรวมตลอดถึงการบริหารงาน การให้บริการ และการเข้าถึงเว็บไซต์ของ สำนักงานปลัดกระทรวงสาธารณสุข เท่านั้น หากผู้ใช้บริการมีการเชื่อมโยง (Link) ไปยังเว็บไซต์อื่นผ่านทางเว็บไซต์ของ สำนักงานปลัดกระทรวงสาธารณสุข ผู้ใช้บริการจะต้องศึกษาและปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ปรากฏในเว็บไซต์อื่นนั้นแยกต่างหากจากสำนักงานปลัดกระทรวงสาธารณสุขด้วย

สำนักงานปลัดกระทรวงสาธารณสุข

เอกสารประกอบการประชุมวันที่ 7 มิ.ย.65 ชี้แจงการดำเนินงานตามกฎหมาย PDPA และ Cyber และแผนการเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud สำหรับหน่วยงานสำนักงานปลัดกระทรวงสาธารณสุข

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

มาตรา 23

ที่ สธ ๐๒๑๒/ว ๑๑๘๖๐ สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๖ พฤษภาคม ๒๕๖๕

เรื่อง หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล

เรียน นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง

สิ่งที่ส่งมาด้วย หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข จำนวน ๑ ฉบับ

ตามที่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะมีผลบังคับใช้โดยสมบูรณ์ในวันที่ ๑ มิถุนายน ๒๕๖๕ ซึ่งมาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

สำนักงานปลัดกระทรวงสาธารณสุข จึงขอให้หน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลในการให้บริการทางการแพทย์และสาธารณสุข นำหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข (สำหรับการรับบริการทางการแพทย์และสาธารณสุข) รายละเอียดตามสิ่งที่ส่งมาด้วย ไปดำเนินการดังนี้

๑. เพิ่มเติมชื่อหน่วยงานในย่อหน้าที่สองของหนังสือ เช่น โรงพยาบาล ก. เป็นหน่วยงานในสังกัด...

๒. นำหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลที่เพิ่มชื่อหน่วยงานตาม ข้อ ๑ ประกาศ/เผยแพร่/ประชาสัมพันธ์ให้ผู้รับบริการทราบอย่างชัดเจนทุกช่องทางสื่อสาร ทั้งภายในพื้นที่หน่วยงาน เว็บไซต์ของหน่วยงาน และสื่อสังคมออนไลน์ต่างๆ (ถ้ามี)

ทั้งนี้ หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำหรับงานบุคลากร และผู้มาติดต่อราชการอยู่ระหว่างดำเนินการ

จึงเรียนมาเพื่อโปรดดำเนินการโดยเคร่งครัดต่อไปด้วย

หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข
(สำหรับการรับบริการทางการแพทย์และสาธารณสุข)

สำนักงานปลัดกระทรวงสาธารณสุขในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้การประมวลผลข้อมูลส่วนบุคคล เป็นไปตามที่กฎหมายกำหนด จึงขอแจ้งการประมวลผลข้อมูลให้แก่เจ้าของข้อมูลส่วนบุคคลทราบตามหนังสือฉบับนี้

.... ชื่อหน่วยงาน เช่น โรงพยาบาล..... เป็นหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข จะทำการประมวลผลข้อมูลส่วนบุคคลภายใต้การควบคุมข้อมูลของสำนักงานปลัดกระทรวงสาธารณสุข ดังนี้

๑. การเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูล

สำนักงานปลัดกระทรวงสาธารณสุขจะเก็บรวบรวมข้อมูลส่วนบุคคลและข้อมูลสุขภาพจากเจ้าของข้อมูลโดยตรง และอาจเก็บข้อมูลส่วนบุคคลและข้อมูลสุขภาพทางอ้อมจากข้อมูลที่เจ้าของข้อมูลหรือตัวแทนของเจ้าของข้อมูล ให้ไว้กับสำนักงานปลัดกระทรวงสาธารณสุข หรือผู้มีส่วนเกี่ยวข้องกับเจ้าของข้อมูล โรงพยาบาลหรือหน่วยงานภายในอื่น ๆ ของสำนักงานปลัดกระทรวงสาธารณสุข หน่วยงานพันธมิตร การให้บริการทางโทรศัพท์ บริการทางด้านดิจิทัลต่าง ๆ ของสำนักงานปลัดกระทรวงสาธารณสุข รวมถึง การใช้งานเว็บไซต์ การดาวน์โหลดข้อมูลจากแอปพลิเคชันจากแหล่งข้อมูลอื่นใดที่เชื่อถือได้ เช่น สมาคม องค์กรของรัฐ หน่วยงานภาครัฐ องค์กรเอกชน งานสัมมนา งานฝึกอบรม งานออกร้าน ทั้งที่สำนักงานปลัดกระทรวงสาธารณสุขจัดขึ้นเอง หรือองค์กรภาครัฐ และภาคเอกชนอื่น ๆ รวมไปถึงสื่อสังคมออนไลน์ต่าง ๆ เป็นต้น ทั้งนี้เป็นไปเพื่อประโยชน์ในการให้บริการสุขภาพและเพื่อการดูแลสุขภาพของเจ้าของข้อมูล ตามภารกิจภายใต้อำนาจหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุข

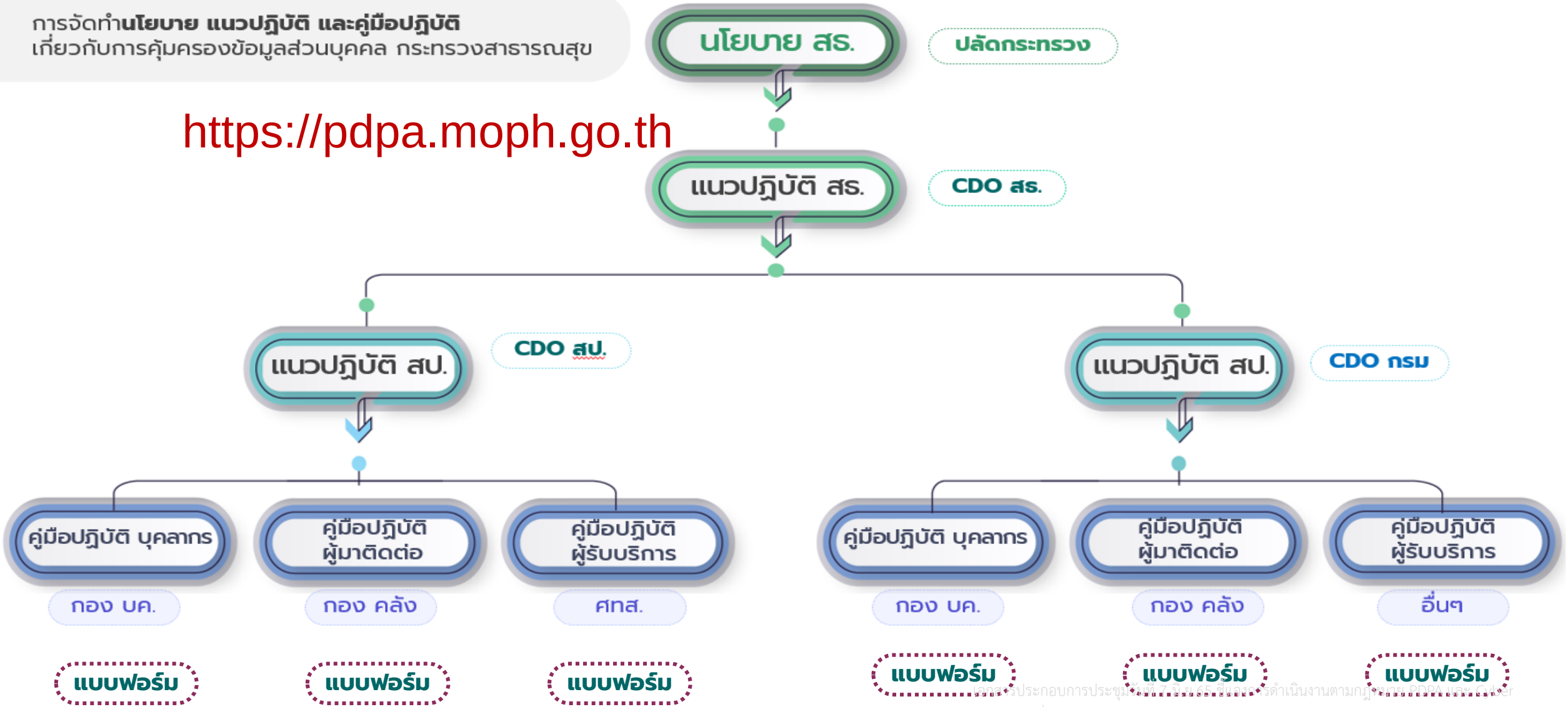
๒. ประเภทของข้อมูลส่วนบุคคลที่สำนักงานปลัดกระทรวงสาธารณสุขจัดเก็บ

- **ข้อมูลระบุตัวตน** เช่น ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน รูปถ่ายใบหน้า เพศ วันเดือนปีเกิด หนังสือเดินทาง หรือหมายเลขระบุตัวตนอื่น ๆ
- **ข้อมูลสำหรับการติดต่อ** เช่น ที่อยู่ อีเมล หมายเลขโทรศัพท์ หมายเลขโทรศัพท์มือถือ
- **ข้อมูลอ่อนไหว** เช่น ศาสนา ข้อมูลสุขภาพ รวมถึง หมู่โลหิต ประวัติการเจ็บป่วย ประวัติการรักษาพยาบาล ประวัติการแพ้ยาหรือแพ้อาหาร ประวัติการพบแพทย์เวชกรรม แพทย์แผนไทย ผู้ประกอบวิชาชีพด้านสุขภาพ ประวัติทันตกรรม ประวัติกายภาพบำบัด ความต้องการพิเศษในการรักษาพยาบาล ข้อมูลชีวภาพ เช่น ข้อมูลพันธุกรรม พฤติกรรมทางเพศ เป็นต้น

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกระทรวงสาธารณสุข

การจัดทำ**นโยบาย แนวปฏิบัติ และคู่มือปฏิบัติ**
เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข

https://pdpa.moph.go.th



แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

ประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกระทรวงสาธารณสุข ครั้งที่ 2/2565 เมื่อวันที่ 18 พ.ค. 65 มีมติดังนี้

4) ให้หน่วยงาน ดำเนินการในระยะเริ่มต้น ดังนี้

1. นำนโยบาย แนวปฏิบัติ คู่มือปฏิบัติ และเอกสารต่างๆ ไปใช้ โดยไม่ต้องจัดทำขึ้นใหม่เป็นของหน่วยงานเอง
2. ประชาสัมพันธ์ เผยแพร่ นโยบายการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข ให้ผู้รับบริการ ผู้ติดต่อราชการ ได้รับทราบอย่างชัดเจน ผ่านช่องทางสื่อสารทุกช่องทาง
3. ประชาสัมพันธ์ เผยแพร่ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ให้บุคลากรในหน่วยงานถือปฏิบัติและรับทราบโดยทั่วกัน
4. หน่วยงานที่มีบริการทางการแพทย์และสาธารณสุข/โรงพยาบาล ให้ทำการเพิ่มเติมชื่อหน่วยงาน ในย่อหน้าที่สองของหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข (สำหรับการรับบริการทางการแพทย์และสาธารณสุข) และประกาศ/ประชาสัมพันธ์ ให้ผู้รับบริการ ผู้ติดต่อราชการได้รับทราบอย่างชัดเจน
5. ทุกหน่วยงานต้องจัดทำ**บันทึกรายการของกิจกรรม**การประมวลผลข้อมูลส่วนบุคคล **(ROPA) ตามมาตรา 39** และกรณีโรงพยาบาล สามารถใช้เวชระเบียนแทนบัญชีบันทึกรายการของกิจกรรมการประมวลผลข้อมูลของผู้ป่วย/ผู้รับบริการ และใช้ทะเบียนการส่งตัวผู้ป่วย (Refer) แทนบัญชีบันทึกรายการเปิดเผยข้อมูลฯ ได้
6. ให้ความรู้และสร้างความเข้าใจแก่บุคลากรทุกระดับในหน่วยงาน เกี่ยวกับการปฏิบัติงานให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7. ข้อมูลส่วนบุคคลที่หน่วยงานเก็บรวบรวมไว้ก่อนวันที่ 1 มิถุนายน 2565 ให้ดำเนินการตามมาตรา 95 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

** **อยู่ระหว่างดำเนินการ** : หนังสือแจ้งเวียน นพ.สสจ. , ผอ.สำนักงานเขตสุขภาพ , ผอ.รพศ./รพท. และ หัวหน้าหน่วยงานในสังกัด สป.สธ. ทุกแห่ง

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

มาตรา ๙๕ ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

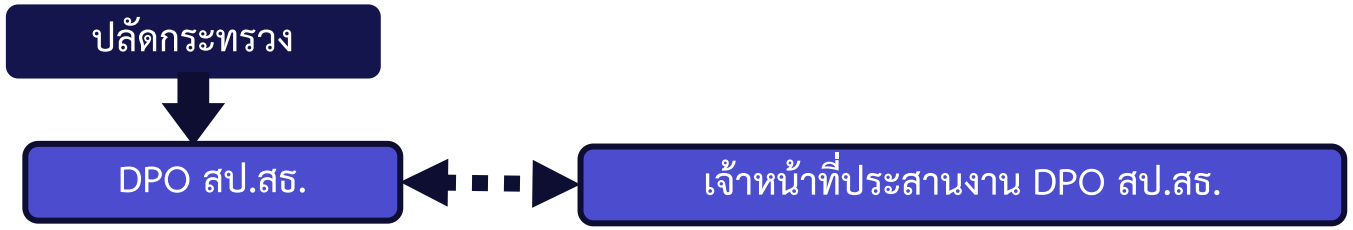
** **อยู่ระหว่างดำเนินการ** : จัดทำคู่มือปฏิบัติ ซึ่งจะมีการกำหนดวิธีการยกเลิกความยินยอม และจะเผยแพร่ผ่านเว็บไซต์ และแจ้งเวียนต่อไป

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกระทรวงสาธารณสุข

ประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกระทรวงสาธารณสุข ครั้งที่ 2/2565 เมื่อวันที่ 18 พ.ค. 65 มีมติดังนี้

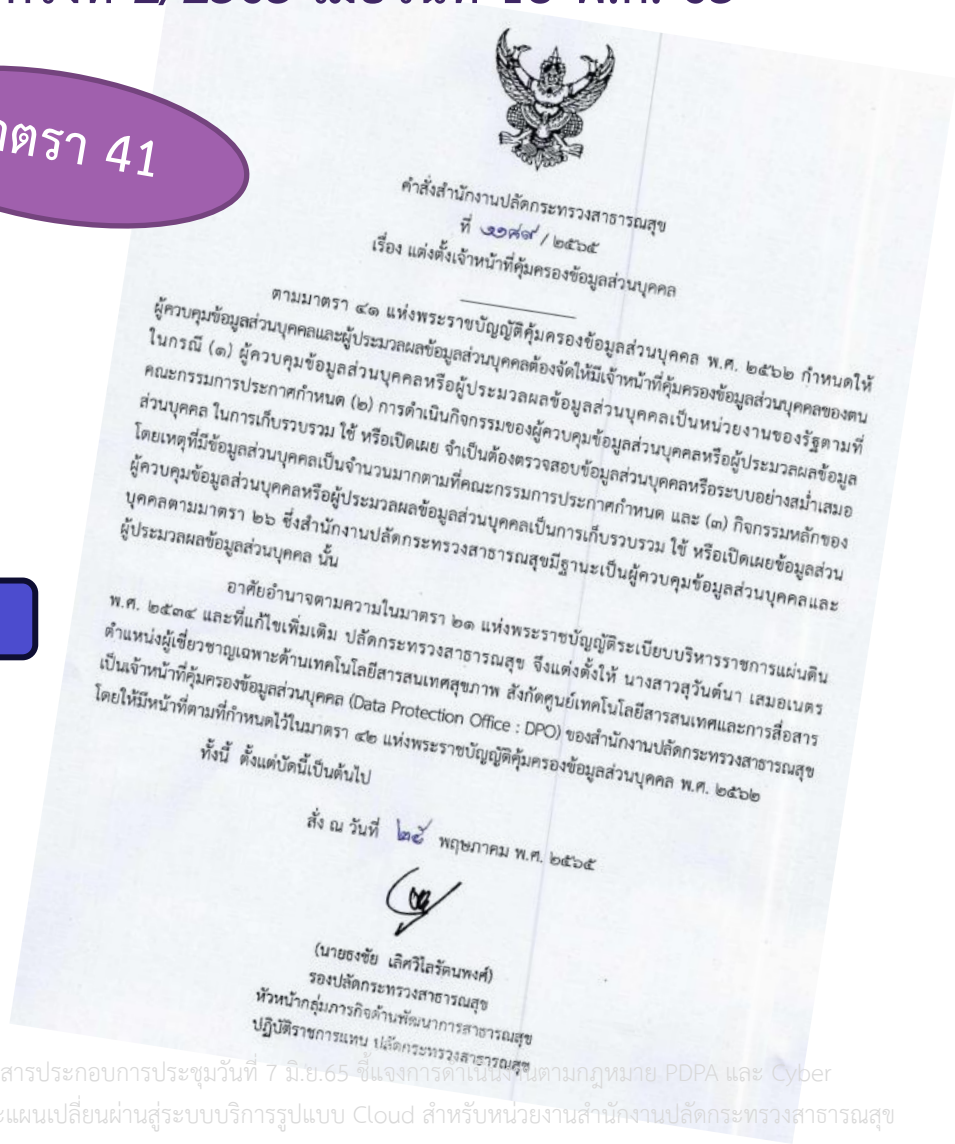
มาตรา 41

2) เห็นชอบให้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ประจำ สป.สธ. และแต่งตั้งเจ้าหน้าที่ประสานงาน DPO



ผู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีสารสนเทศสุขภาพ

1) เลขานุการคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพระดับจังหวัด
2) สำนัก/กอง ส่วนกลาง แต่งตั้งผู้แทน



คำสั่งสำนักงานปลัดกระทรวงสาธารณสุข
ที่ ๑๑๘๙ / ๒๕๖๕
เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณี (๑) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (๒) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด และ (๓) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖ ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล นั้น

อาศัยอำนาจตามความในมาตรา ๒๑ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ปลัดกระทรวงสาธารณสุข จึงแต่งตั้งให้ นางสาวสุวันต์นา เสมอเนตร ตำแหน่งผู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีสารสนเทศสุขภาพ สังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office : DPO) ของสำนักงานปลัดกระทรวงสาธารณสุข โดยให้มีหน้าที่ตามที่กำหนดไว้ในมาตรา ๔๒ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๕

(นายธงชัย เลิศวิไลรัตนพงศ์)
รองปลัดกระทรวงสาธารณสุข
หัวหน้ากลุ่มภารกิจด้านพัฒนาการสาธารณสุข
ปฏิบัติราชการแทน ปลัดกระทรวงสาธารณสุข

ดำเนินการแล้ว : ✓คำสั่ง สป.สธ. ที่ 1189/2565
เรื่องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สั่ง ณ วันที่ 25 พ.ค.65

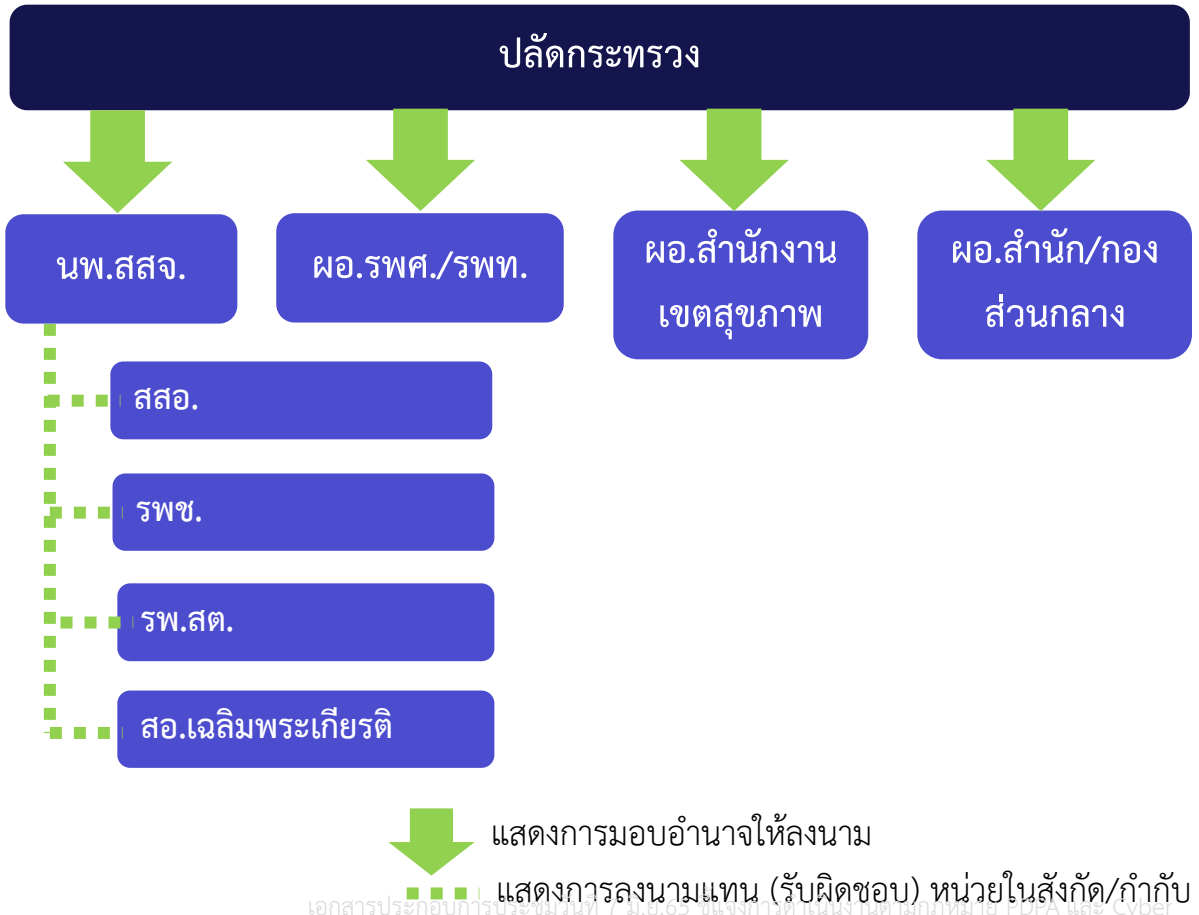
แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกระทรวงสาธารณสุข

ประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกระทรวงสาธารณสุข ครั้งที่ 2/2565 เมื่อวันที่ 18 พ.ค. 65 มีมติดังนี้

3) การมอบอำนาจให้หัวหน้าหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข **ลงนามในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล** (DPA: Data Processing Agreement)

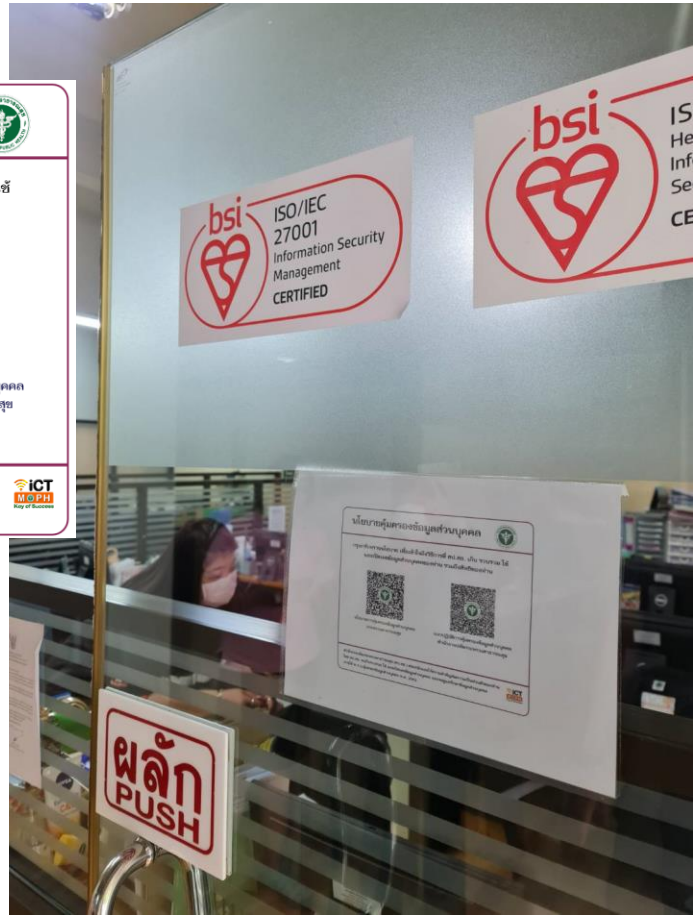
<u>มอบ</u> กองกฎหมายดำเนินการ

แผนภาพการมอบอำนาจให้แก่หน่วยงาน
ในการลงนามในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

ตัวอย่างการประกาศ เผยแพร่ นโยบายฯ และการแจ้งการเก็บข้อมูลผ่านกล้องวงจรปิด CCTV



ขอบคุณภาพ จาก Facebook ของ ดร.ศักดิ์ เสกขุนทด

นโยบายคุ้มครองข้อมูลส่วนบุคคล

กรุณารับทราบนโยบาย เพื่อเข้าใจถึงวิธีการที่ สป.สธ. เก็บ รวบรวม ใช้
และเปิดเผยข้อมูลส่วนบุคคลของท่าน รวมถึงสิทธิของท่าน

นโยบายการคุ้มครองข้อมูลส่วนบุคคล
กระทรวงสาธารณสุข

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
สำนักงานปลัดกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข (สป.สธ.) ตระหนักและให้ความสำคัญต่อความเป็นส่วนตัวของท่าน
โดย สป.สธ. จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล และจะดูแลรักษาข้อมูลส่วนบุคคล
ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

แนวทางดำเนินงานตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
สำหรับกระทรวงสาธารณสุข

สป.สธ. มีระบบรักษาความปลอดภัย ด้วยกล้องวงจรปิดภายในสำนักงาน ตลอด 24 ชั่วโมง

CCTV กล้องวงจรปิด กำลังทำงาน เพื่อการรักษาความปลอดภัย

สำนักงานปลัดกระทรวงสาธารณสุข (สป.สธ.) ตระหนักและให้ความสำคัญต่อความเป็นส่วนตัวของท่าน โดย สป.สธ. จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล และจะดูแลรักษาข้อมูลส่วนบุคคล ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข

เอกสารประกอบการประชุมวันที่ 7 มิ.ย.65 ชี้แจงการดำเนินงานตามกฎหมาย PDPA และ Cyber และแผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud สำหรับหน่วยงานสำนักงานปลัดกระทรวงสาธารณสุข

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565

ประกาศกระทรวงสาธารณสุข
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ กระทรวงสาธารณสุขจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๗ วรรคหนึ่ง แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ปลัดกระทรวงสาธารณสุขโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกระทรวงสาธารณสุข ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดกระทรวงสาธารณสุข และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกระทรวงสาธารณสุข ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของกระทรวงสาธารณสุขในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕. นโยบาย...

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบ...

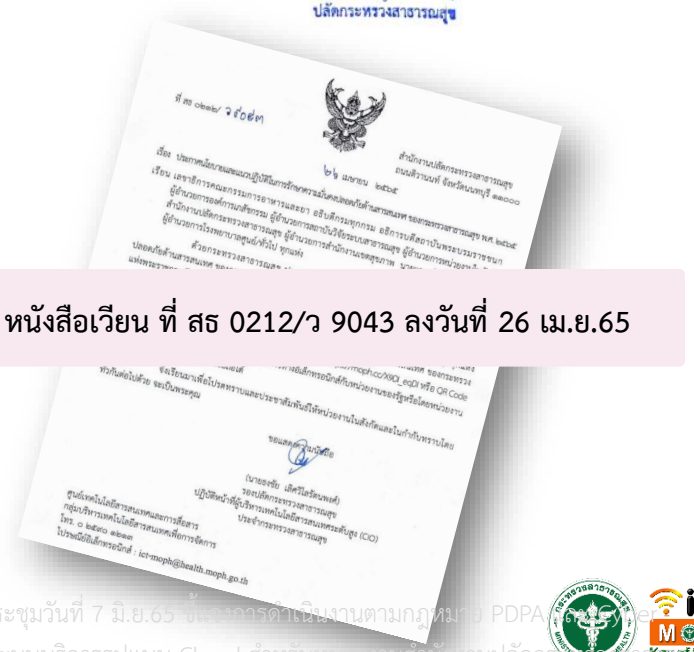
๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๖๕

(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข



หนังสือเวียน ที่ สธ 0212/ว 9043 ลงวันที่ 26 เม.ย.65

คำสั่งมอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขและระบบสุขภาพดิจิทัล

คำสั่งกระทรวงสาธารณสุข
ที่ ๓๗๘ /๒๕๖๕
เรื่อง มอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ มีผลบังคับใช้เมื่อ ๒๔ สิงหาคม พ.ศ. ๒๕๖๔ กำหนดให้สำนักงานปลัดกระทรวงสาธารณสุข เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านสาธารณสุข สำหรับหน่วยงานที่มีลักษณะการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล จึงควรให้มีหน่วยงานขับเคลื่อนการดำเนินงานตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในนามของสำนักงานปลัดกระทรวงสาธารณสุข และมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๓๘ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ปลัดกระทรวงสาธารณสุข จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข โดยมีหน้าที่และอำนาจ ดังนี้

ข้อ ๑. รับผิดชอบหลักเกี่ยวกับงานควบคุมและกำกับดูแล (Main Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ก. ปฏิบัติหน้าที่ที่เกี่ยวข้องกับงานควบคุมและกำกับดูแล ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข. เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) มีลักษณะ หน้าที่และความรับผิดชอบ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔ ฉบับลงวันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔

ค. เฝ้าระวังความเสี่ยง เตรียมพร้อมรับมือและแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ง. ประสาน...

ง. ประสานดำเนินงานร่วมกับหน่วยงานควบคุมและกำกับดูแลเกี่ยวกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขที่ให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา

จ. ประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ศปช.สกมช.) (National CERT)

ฉ. รายงานผลเบื้องต้นต่อผู้บังคับบัญชา เพื่อนำเสนอผู้บริหารระดับสูงด้านความปลอดภัยสารสนเทศ (CISO) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ช. ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับเทคโนโลยีสารสนเทศดิจิทัลด้านสุขภาพ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารด้านธุรกรรมทางอิเล็กทรอนิกส์ด้านสุขภาพ

ข้อ ๒. รับผิดชอบหลักเกี่ยวกับงานควบคุมและกำกับดูแล (Regulator) หน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขที่ให้บริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

ก. จัดทำข้อเสนอแนะที่เกี่ยวข้องกับมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการพัฒนาบริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

ข. จัดทำข้อเสนอแนะเกี่ยวกับมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการพัฒนาบริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

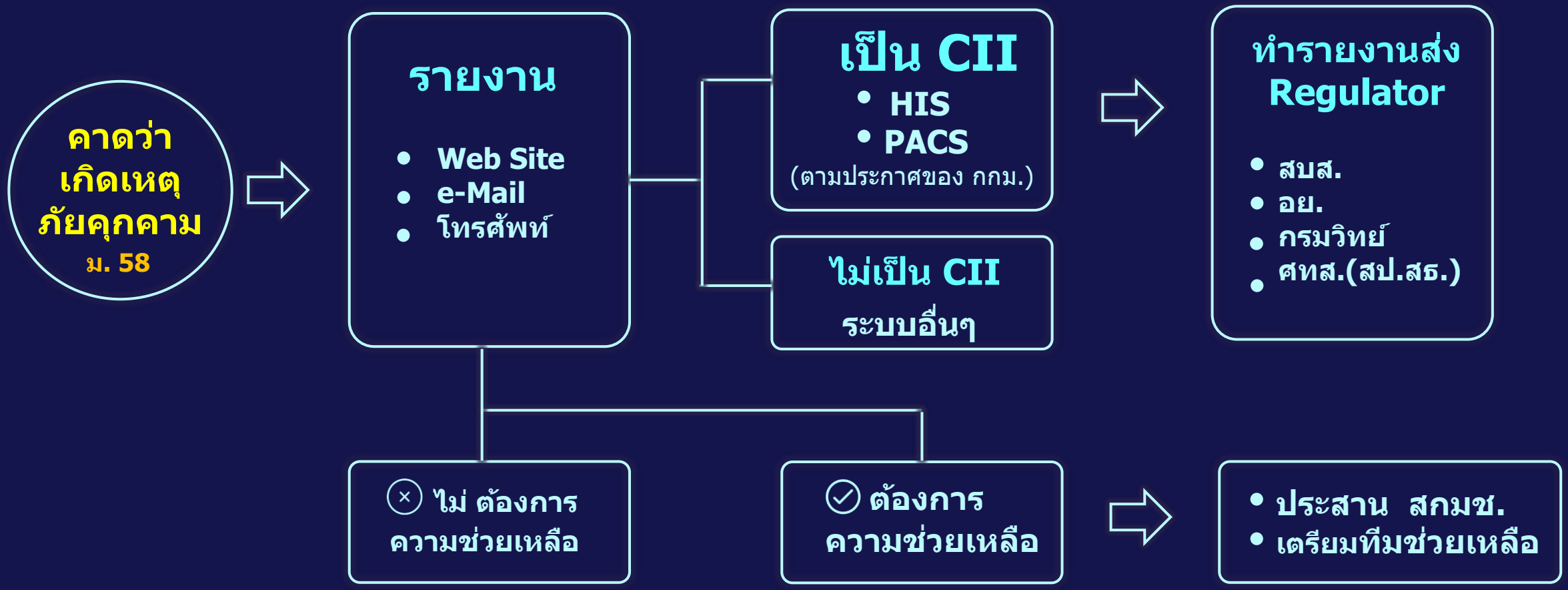
ข้อ ๓. ในการปฏิบัติตามคำสั่งนี้ หากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจำเป็นต้องออกระเบียบ ประกาศ คำสั่ง แนวทางปฏิบัติ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการจัดทำระเบียบ ประกาศ คำสั่ง แนวทางปฏิบัติเสร็จแล้วให้เสนอผู้มีอำนาจเพื่อพิจารณาลงนามใช้บังคับต่อไป

ทั้งนี้ ตั้งแต่บัดนี้ เป็นต้นไป

สั่ง ณ วันที่ ๒๘ มีนาคม พ.ศ. ๒๕๖๕

(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข

Cyber Attack Incident Report Center



- มีผู้รับผิดชอบ 24 ชม. x 7 วัน
- เว็บไซต์ https://health-cirt.moph.go.th
- โทร: 083-064-9867
- โทรสาร : 02-590-1215

- e-mail: health-cirt@moph.go.th
- Line Official : @health-cirt
- LINE Open Chat ให้ความรู้ : Moph IT Community

การตรวจพบภัยคุกคามทางไซเบอร์ด้านสาธารณสุข (ม.ค. – พ.ค. 2565)

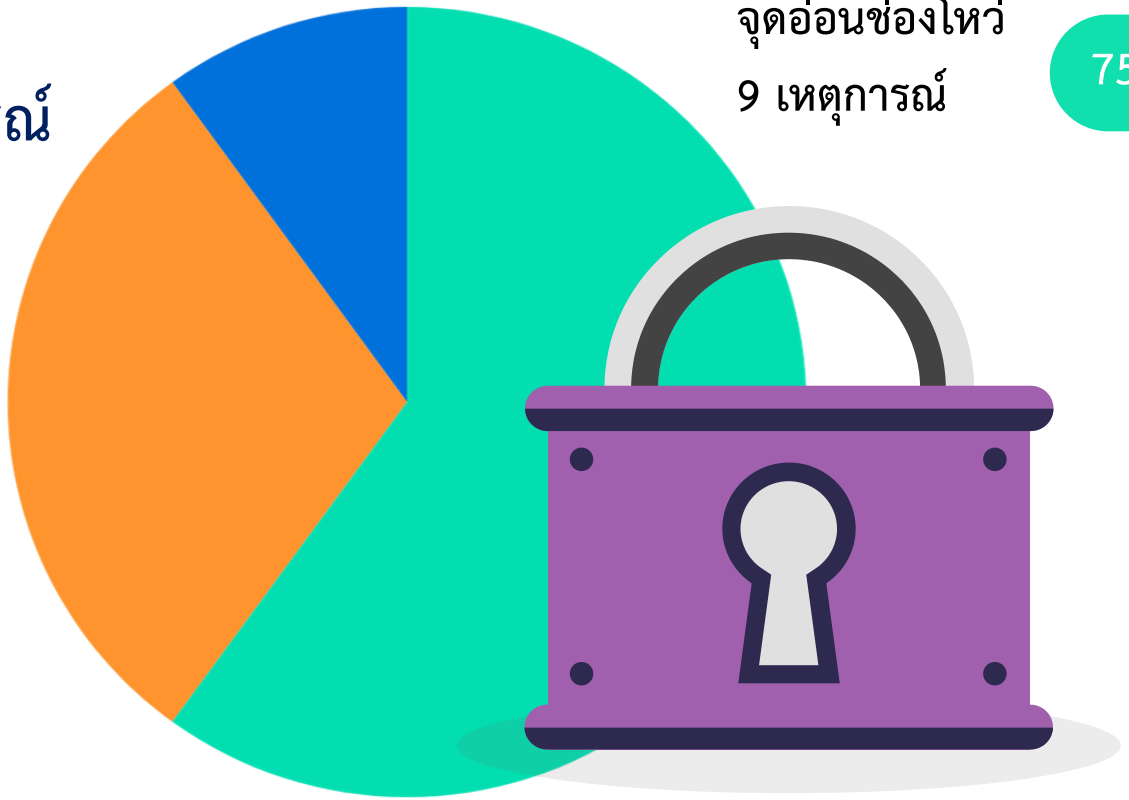
โดย HealthCIRT

ตรวจพบทั้งหมด 12 เหตุการณ์

Website Defacement
1 เหตุการณ์
20%

จุดอ่อนช่องโหว่
9 เหตุการณ์
75%

Misconfiguration
2 เหตุการณ์
20%



*** ตรวจสอบในรูปแบบ internal pentest โดยมุ่งเน้นไปที่การเข้าถึงฐานข้อมูลเป็นหลัก ***

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับโรงพยาบาล

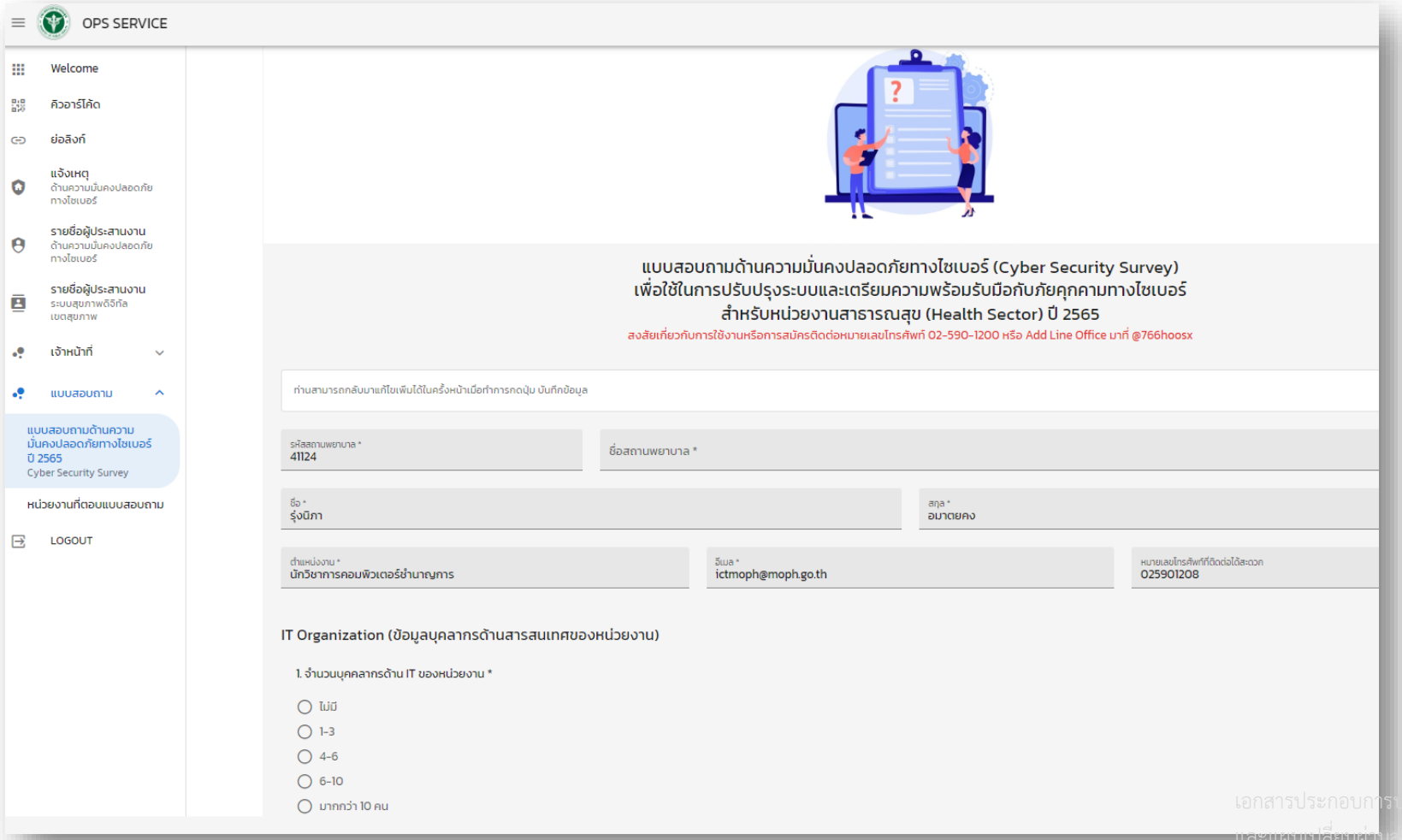
จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) เพื่อป้องกันการเข้าถึงและเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ประกอบด้วย

- มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)
- มาตรการป้องกันด้านเทคนิค (Technical Safeguard)
- มาตรการป้องกันทางกายภาพ (Physical Safeguard)

โดยที่**มาตรการดังกล่าวเป็นไปตามวัตถุประสงค์ 3 ประการ ของการรักษาความมั่นคงปลอดภัยไซเบอร์** ได้แก่

1) การธำรงไว้ซึ่งความลับ (**Confidentiality**)
2) ความถูกต้องครบถ้วน (**Integrity**) และ
3) สภาพพร้อมใช้งาน (**Availability**)

แบบสอบถามด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Survey) เพื่อใช้ในการปรับปรุงระบบและเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ สำหรับหน่วยงานสาธารณสุข (Health Sector) ปี 2565



ขณะนี้มีตอบมาทั้งสิ้น 288 หน่วย

** ขอให้ รพช. รพท. รพศ. สสจ. ทุกหน่วย ช่วยตอบแบบสอบถามให้ครบด้วย

หากมีข้อสงสัยสอบถามได้ที่

กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ.

โทร 025901200 หรือ

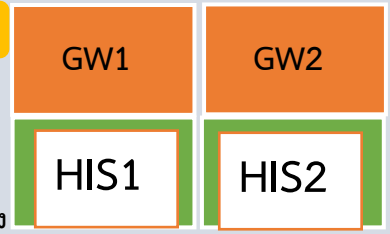
ictmoph@moph.go.th หรือ

Line OA : @ictmoph

1 On Premise

หน่วยบริการสุขภาพ

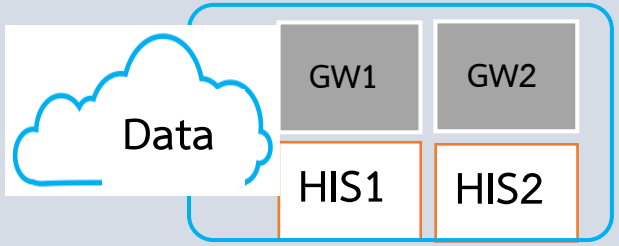
- รพศ. 34 แห่ง
- รพท. 92 แห่ง
- รพช. 775 แห่ง
- รพ.สต. 9,765 แห่ง
- สถานีอนามัย 41 แห่ง



1.HIS 1,000x10 ลบ. = 10,000 ลบ.
ค่าใช้จ่าย Cyber Security
2.ISO 1,000x10 ลบ. = 10,000 ลบ.
3.จ้างคน 1,000x10 คน = 10,000 คน
4.ค่าจ้างคน 10,000x200,000 บ./ปี
total 22,000 ลบ. ในปีแรก

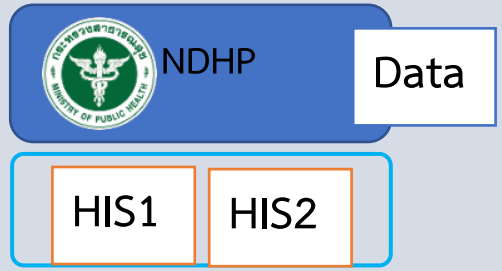
เฉพาะ รพ

2 On Cloud



1.HIS 1,000x10 ลบ. = 10,000 ลบ.
ค่าใช้จ่าย Cyber Security
2.Cloud 1000x 0.5 ลบ.=500 ลบ./ปี
2.ISO 1,000x0 ลบ. = 0 ลบ.
3.จ้างคน 1,000x0 คน = 0 คน
total 10,500 ลบ. ในปีแรก

3 as a Service



1.HIS 1,000x1 ลบ./ปี = 1,000 ลบ./ปี
2.ISO 1,000x0 ลบ. = 0 ลบ.
3.จ้างคน 1,000x0 คน = 0 คน
total 1,000 ลบ./ปี

พบเซิร์ฟเวอร์ MySQL 3.6 ล้านเครื่องเชื่อมต่ออินเทอร์เน็ตโดยตรง ไทยมีราว 1 หมื่นเครื่อง

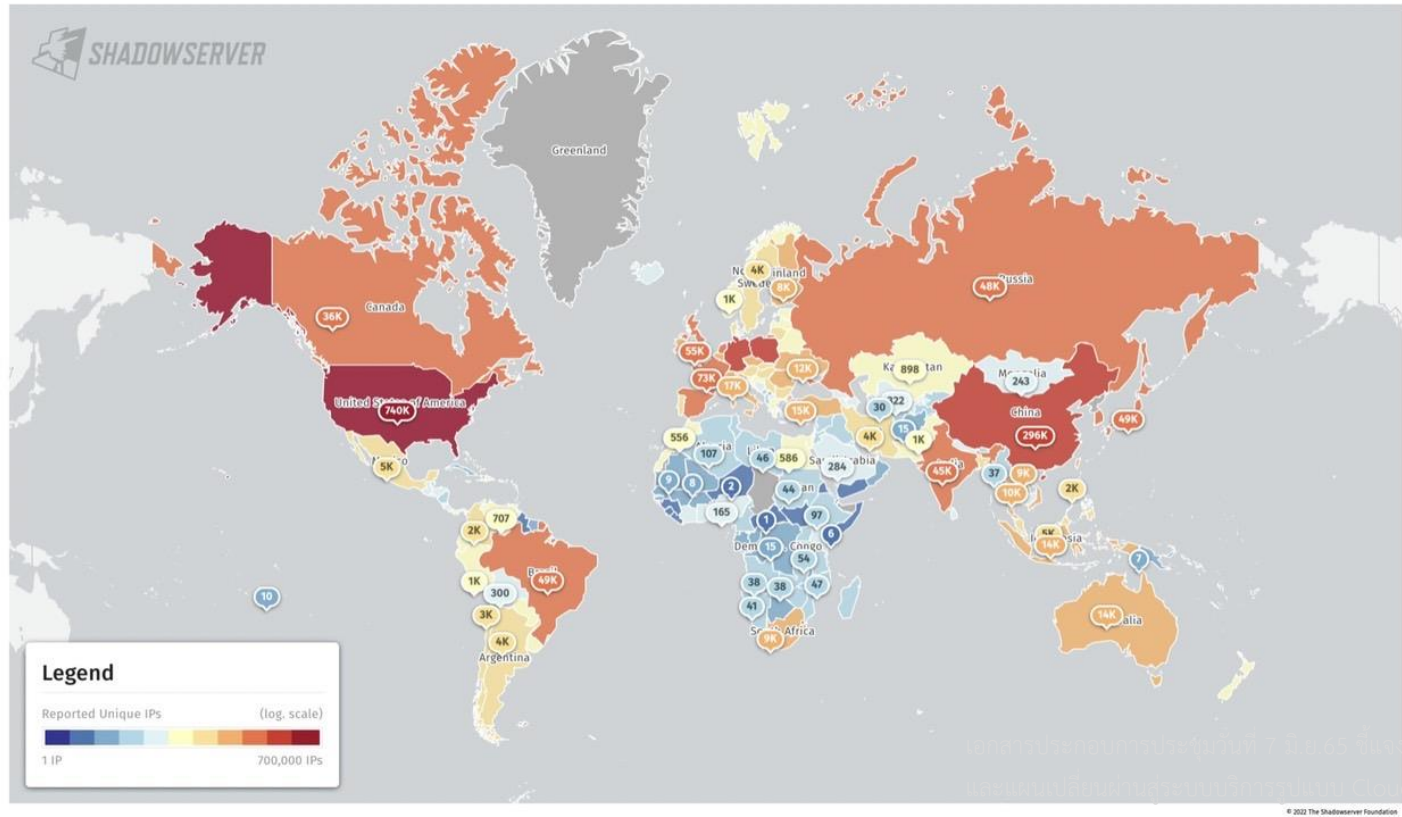
By: mk on 2 June 2022 - 20:19 Tags: MySQL Security Database

Shadowserver Foundation หน่วยงานไม่หวังผลกำไรด้านความปลอดภัยไซเบอร์ ทดลองสแกนพอร์ต MySQL ของทั้งโลก (ตรวจสอบเฉพาะพอร์ต 3306/TCP ที่เป็นค่าดีฟอลต์) และพบว่ามีเซิร์ฟเวอร์ MySQL ที่สามารถเข้าถึงได้ (accessible คือตอบสถานะกลับมา แต่ไม่ได้ลองล็อกอิน) จำนวน 3.6 ล้านเครื่อง แบ่งเป็น IPv4 2.3 ล้านเครื่อง และ IPv6 อีก 1.3 ล้านเครื่อง

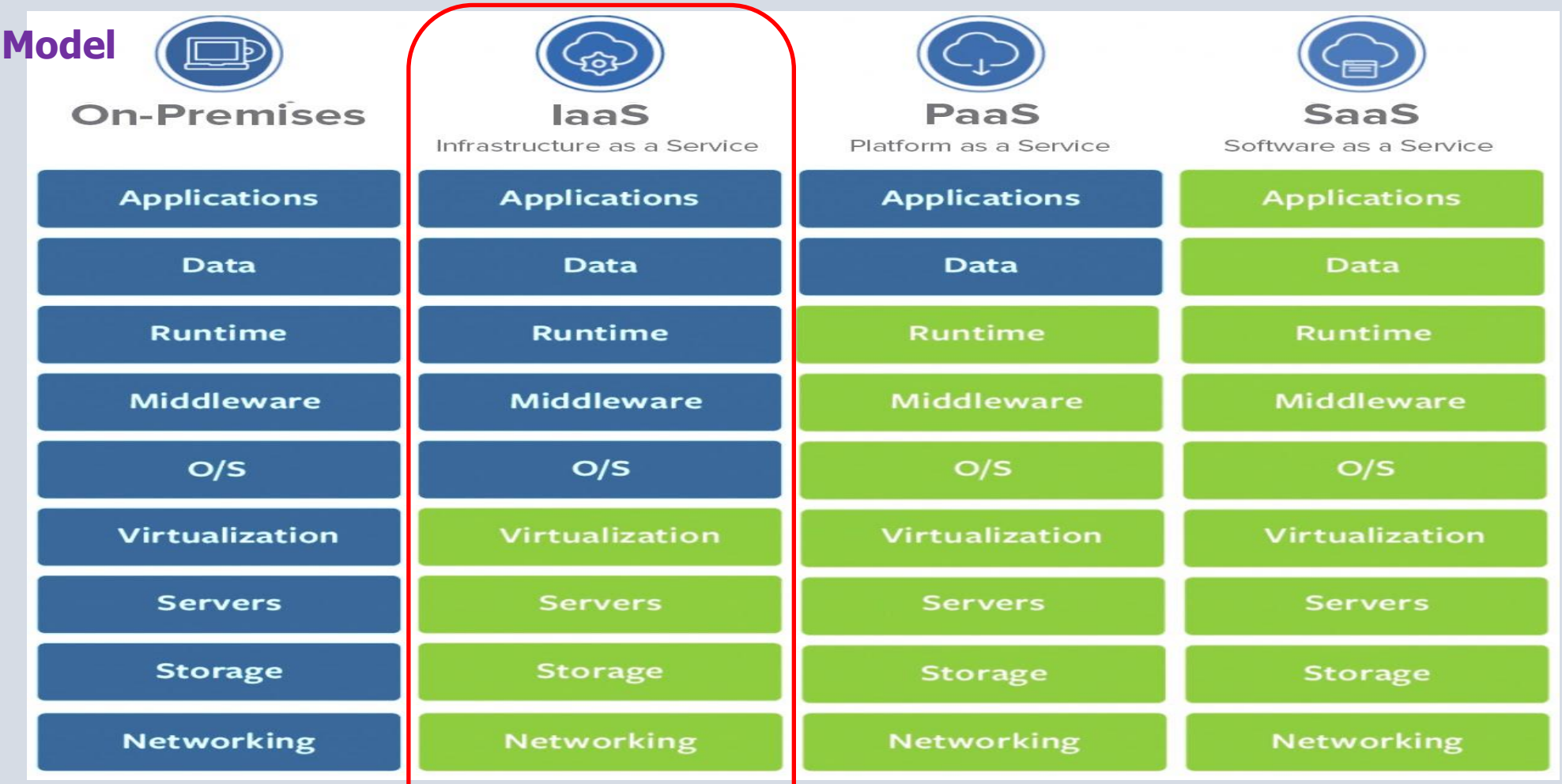
หากดูตัวเลขแยกรายประเทศ เอาเฉพาะ IPv4 สหรัฐอเมริกามีเซิร์ฟเวอร์ MySQL ถูกเข้าถึงได้มากที่สุด 7.4 แสนเครื่อง ตามด้วยจีน 2.96 แสนเครื่อง ส่วนประเทศไทยก็อยู่ในอันดับต้นๆ คือมี 1 หมื่นเครื่อง ถ้าดูของ IPv6 สหรัฐอเมริกามี 4.6 แสนเครื่อง เนเธอร์แลนด์ 2.96 แสนเครื่อง และสิงคโปร์ 2.18 แสนเครื่อง (ไทยมี 136 เครื่อง IPv6)

Shadowserver Foundation บอกว่าตามปกติแล้วคงไม่ค่อยมีใครตั้งเซิร์ฟเวอร์ MySQL เพื่อรอการเชื่อมต่อจากอินเทอร์เน็ตโดยตรง แปลว่าเครื่องจำนวน 3.6 ล้านเครื่องนี้ถูกละเลยเครื่องความปลอดภัย และมีความเสี่ยงสูงที่จะถูกโจมตีได้ ทางมูลนิธิจึงแนะนำให้แอดมิน MySQL เร่งเพิ่มมาตรการความปลอดภัย เช่น คัดกรองทราฟฟิกที่เข้าถึงได้ หรือเพิ่มระบบยืนยันตัวตนที่แข็งแกร่งขึ้น

ที่มา - Shadowserver Foundation



Clouds Model



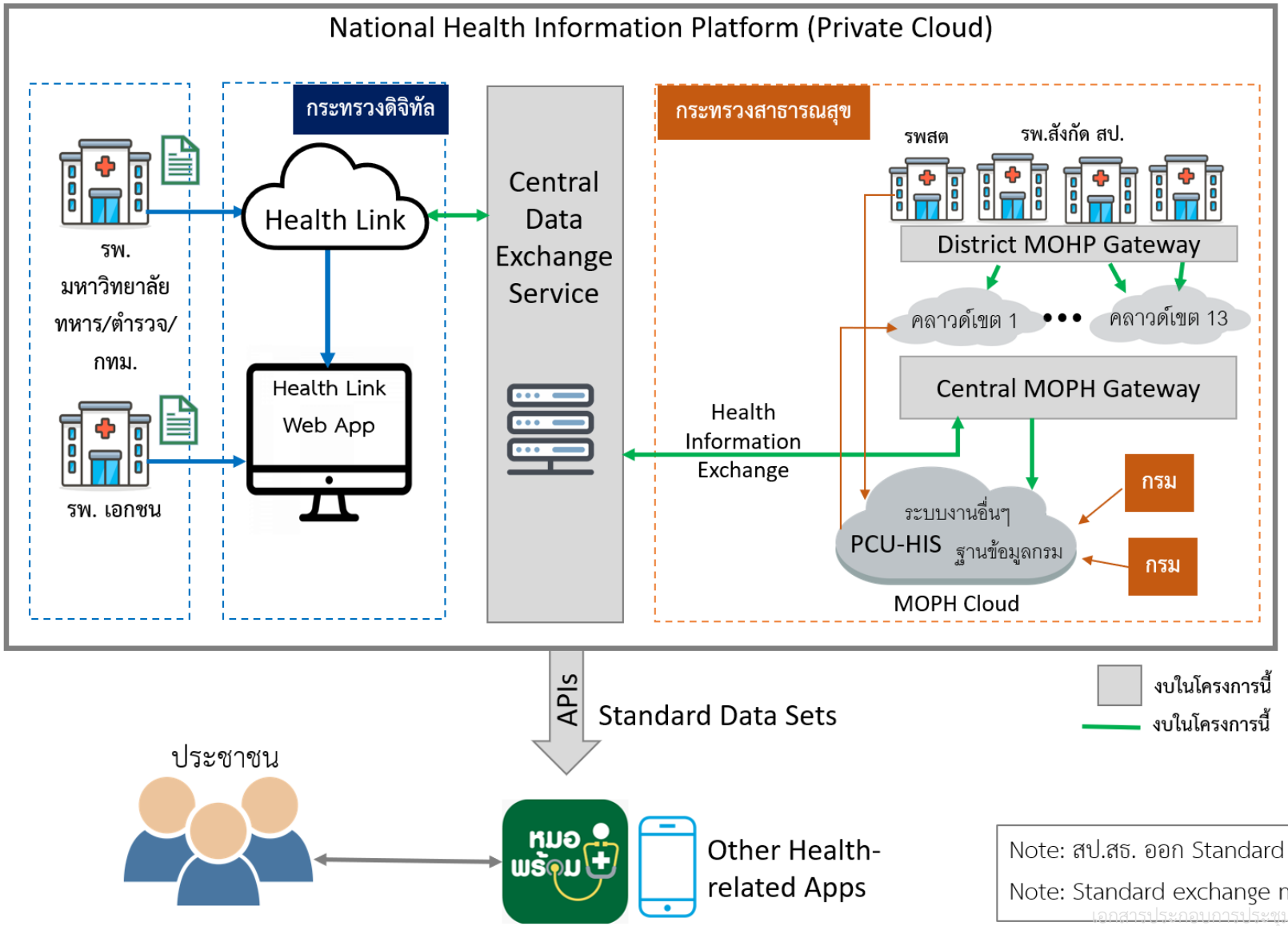
- ผู้ใช้งาน
- ผู้ดูแลฐานข้อมูล
- ทีมพัฒนาระบบ
- จนท. ไอทีซัพพอร์ต
- จนท. Helpdesk
- วิศวกรระบบ
- วิศวกรเครือข่าย
- จนท. ปลอดภัยทางไซเบอร์

- ผู้ใช้งาน
- ผู้ดูแลฐานข้อมูล
- ทีมพัฒนาระบบ
- จนท. ไอทีซัพพอร์ต
- จนท. Helpdesk
- วิศวกรระบบ
- จนท. ปลอดภัยทางไซเบอร์

- ผู้ใช้งาน
- ผู้ดูแลฐานข้อมูล
- ทีมพัฒนาระบบ
- จนท. ไอทีซัพพอร์ต
- จนท. Helpdesk

- ผู้ใช้งาน

แผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud



งบประมาณ

1. Cloud สำหรับ

- MOPH Gateway ทั้งระบบ
- คลาวด์เขตสุขภาพ ทั้ง 13 เขต
- Ministry Cloud ของ ก.สธ (รวมระบบ PCU-HIS)

2. พัฒนา/จัดหา Software

- MOPH Gateway (ระดับเขต และส่วนกลาง)
- ระบบแลกเปลี่ยนข้อมูลกลาง และการเชื่อมต่อจาก MOPH / Health Link

3. ค่า Migration

- ระบบของศูนย์เทคฯ ที่เกี่ยวข้อง

4. Security ในทุกระดับ

Note: สป.สธ. ออก Standard Data Set สำหรับประวัติคนไข้

Note: Standard exchange mechanism for standard data set

แผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud

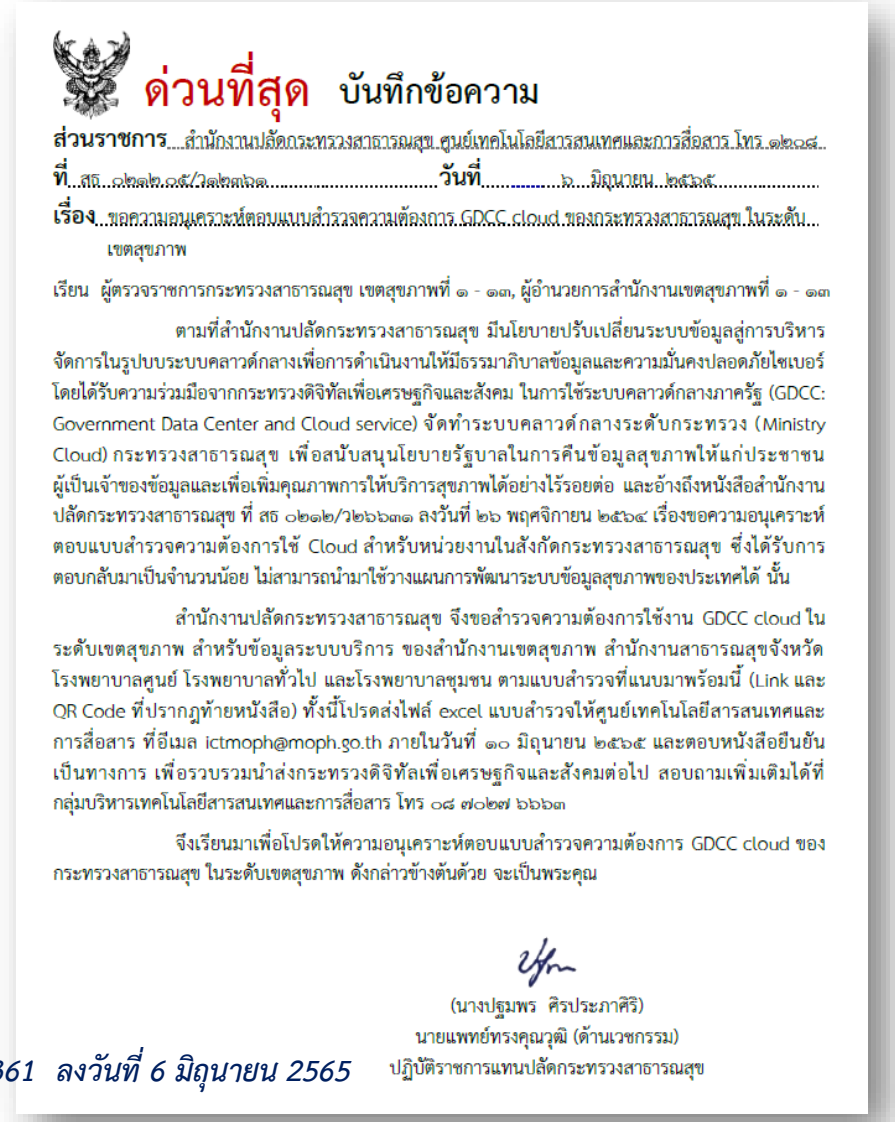
การสนับสนุน cloud ให้เขตสุขภาพทั้ง 13 เขต โดยกระทรวงดิจิทัลฯ จะของบกลางเพื่อพัฒนา cloud ให้ สป.สธ. สนับสนุนนโยบายรัฐบาลในการคืนข้อมูลสุขภาพให้ประชาชน และการให้บริการแบบไร้รอยต่อ

สิ่งที่เขตสุขภาพจะได้รับ :-

1) มีระบบรักษาความปลอดภัยของข้อมูลสุขภาพส่วนบุคคลที่ดีขึ้น จากการลงทุน Cyber Security จากศูนย์กลาง
2) สร้างระบบเชื่อมโยงแลกเปลี่ยนข้อมูลสุขภาพ เพื่อการส่งต่อ ภายใน Cloud ของเขตสุขภาพ ได้ตามที่เขตออกแบบ และแลกเปลี่ยนข้ามเขตที่ Cloud กลางของ สป.สธ. และ แลกเปลี่ยนข้ามสังกัด ที่ Cloud กลางของ DE (Health Link)
3) คืนข้อมูลสุขภาพจากทุก รพ. ให้แก่ประชาชนผู้เป็นเจ้าของข้อมูลได้สะดวก รวดเร็วและปลอดภัย ใน Application เดียว

สิ่งที่เขตและจังหวัดต้องดำเนินการ :-

1) **สำคัญเร่งด่วน** - ตอบแบบสำรวจความต้องการ GDCC cloud ส่งให้ ศทส.สป.สธ. รวบรวมภายในวันที่ 10 มิ.ย.65 เพื่อส่งกระทรวงดิจิทัลฯ ให้ทันต่อการเสนอของบกลาง ปี 2565
2) สำคัญ - ร่างแผนการย้ายข้อมูลขึ้น cloud หลังจากที่ทราบปริมาณ cloud ที่ได้รับจัดสรร
3) สำคัญ - ส่งข้อมูลจำเป็นสำหรับการคืนข้อมูล PHR และการส่งต่อ ตามรรายการ รูปแบบ และ API ที่ สป.สธ. จะประกาศต่อไป



ด่วนที่สุด บันทึกข้อความ

ส่วนราชการ สำนักงานปลัดกระทรวงสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร ๑๒๑๘

ที่ สธ ๐๒๑๒.๐๕/ว๑๒๓๖๑ **วันที่** ๖ มิถุนายน ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ตอบแบบสำรวจความต้องการ GDCC cloud ของกระทรวงสาธารณสุข ในระดับเขตสุขภาพ

เรียน ผู้ตรวจราชการกระทรวงสาธารณสุข เขตสุขภาพที่ ๑ - ๑๓, ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ - ๑๓

ตามที่สำนักงานปลัดกระทรวงสาธารณสุข มีนโยบายปรับเปลี่ยนระบบข้อมูลสู่การบริหารจัดการในรูปบบระบบคลาวด์กลางเพื่อการดำเนินงานให้มีธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยไซเบอร์ โดยได้รับความร่วมมือจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในการใช้ระบบคลาวด์กลางภาครัฐ (GDCC: Government Data Center and Cloud service) จัดทำระบบคลาวด์กลางระดับกระทรวง (Ministry Cloud) กระทรวงสาธารณสุข เพื่อสนับสนุนโยบายรัฐบาลในการคืนข้อมูลสุขภาพให้แก่ประชาชนผู้เป็นเจ้าของข้อมูลและเพื่อเพิ่มคุณภาพการให้บริการสุขภาพได้อย่างไร้รอยต่อ และอ้างถึงหนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/ว๒๖๖๓๑ ลงวันที่ ๒๖ พฤศจิกายน ๒๕๖๔ เรื่องขอความอนุเคราะห์ตอบแบบสำรวจความต้องการใช้ Cloud สำหรับหน่วยงานในสังกัดกระทรวงสาธารณสุข ซึ่งได้รับการตอบกลับมาเป็นจำนวนน้อย ไม่สามารถนำมาใช้วางแผนการพัฒนาระบบข้อมูลสุขภาพของประเทศได้ นั้น

สำนักงานปลัดกระทรวงสาธารณสุข จึงขอสำรวจความต้องการใช้งาน GDCC cloud ในระดับเขตสุขภาพ สำหรับข้อมูลระบบบริการ ของสำนักงานเขตสุขภาพ สำนักงานสาธารณสุขจังหวัด โรงพยาบาลศูนย์ โรงพยาบาลทั่วไป และโรงพยาบาลชุมชน ตามแบบสำรวจที่แนบมาพร้อมนี้ (Link และ QR Code ที่ปรากฏท้ายหนังสือ) ทั้งนี้โปรดส่งไฟล์ excel แบบสำรวจให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่อีเมล ictmoph@moph.go.th ภายในวันที่ ๑๐ มิถุนายน ๒๕๖๕ และตอบหนังสือยืนยันเป็นทางการ เพื่อรวบรวมนำส่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมต่อไป สอบถามเพิ่มเติมได้ที่ กลุ่มบริหารเทคโนโลยีสารสนเทศและการสื่อสาร โทร ๐๘ ๗๐๒๗ ๖๖๖๓

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ตอบแบบสำรวจความต้องการ GDCC cloud ของกระทรวงสาธารณสุข ในระดับเขตสุขภาพ ดังกล่าวข้างต้นด้วย จะเป็นพระคุณ

(นางปฐมพร ศิรประภาศิริ)
นายแพทย์ทรงคุณวุฒิ (ด้านเวชกรรม)
ปฏิบัติราชการแทนปลัดกระทรวงสาธารณสุข

หนังสือเวียนที่ สธ 0212.05/ว12361 ลงวันที่ 6 มิถุนายน 2565

แผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud

ตารางสำรวจความต้องการ GDCC cloud ของกระทรวงสาธารณสุข ของ รพช. รพท. รพศ. และ สสจ. (ระดับจังหวัด)
ทั้งนี้ให้แจ้งความพร้อม/ศักยภาพในการถ่ายโอนข้อมูล ไปยัง GDCC cloud ภายในปีงบประมาณ พ.ศ. 2566-2567
(เมื่อได้รับจัดสรรแล้วจะมีการติดตามประเมินผลการโอนข้อมูลไปยัง GDCC cloud โดยกระทรวงสาธารณสุขร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)

ประมาณการความต้องการ Cloud เพื่อเก็บข้อมูลย้อนหลัง 10 ปี ในช่วงที่ของบประมาณ (ปีปฏิทิน พ.ศ.2556-2567)			ความต้องการ cloud สำหรับฐานข้อมูลการบริการสุขภาพบุคคล ที่เกี่ยวข้องกับการคืน PHR และการส่งต่อ ของหน่วยบริการระดับ รพช. รพท. รพศ.										กรณีไม่สามารถแยกรายการได้ ให้ประมาณการผลรวมเฉพาะฐานข้อมูลที่กำหนด หาก รพ. ไม่สามารถตอบได้ ให้จังหวัดประมาณการแทน	
			HIS		LIS (ยังไม่โอนข้อมูลในปี 66-67 ใส่ 0)		PACS (ยังไม่โอนข้อมูลในปี 66-67 ใส่ 0)		16 แฟ้มส่ง สป.สช. (ไม่แยกฐานจากHIS ใส่ 0)		43+แฟ้ม (ไม่แยกฐานจากHIS ใส่ 0)			
			ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67
1	รพ ตัวอย่าง	VM	12	8	4	0	12	0	4	4	0	0		
		CPU (core)	48	32	16	0	48	0	16	16	0	0		
		RAM (GB)	144	112	48	0	144	0	48	48	0	0		
		Storage (GB)	6000	4000	2000	0	6000	0	2000	2000	0	0		
2	รพ...	VM												
		CPU (core)												
		RAM (GB)												
		Storage (GB)												
3	สสจ	VM									4	4		
		CPU (core)									16	16		
		RAM (GB)									48	48		
		Storage (GB)									2000	2000		

หมายเหตุ 1. การสำรวจไม่รวม รพ.สต. เนื่องจากจะมีการจัดสรร cloud รพ.สต. แยกไปอีก 1 ส่วน เพื่อรองรับการรองรับการกระจายอำนาจ
2. รพช. ที่ไม่สามารถตอบข้อมูลได้ใส่ NA เพื่อให้ IT ของจังหวัดประมาณการให้ หรือประสานบริษัทเจ้าของ HIS
3. โปรดระบุรหัสหน่วย 5 หลัก และชื่อ รพ. , ชื่อจังหวัด , ชื่อเขตสุขภาพ
4. สสจ. รวบรวมจากทุก รพ. ในจังหวัด และสรุปรวมจำนวนระดับจังหวัด

แบบสำรวจสำหรับ สสจ.
รวบรวมจาก รพศ. รพท. รพช.
แล้วจัดส่งให้ สำนักงานเขตสุขภาพ

ใช้ excel ในการบันทึกข้อมูลแบบสำรวจ

Download ได้ที่

https://moph.cc/7VYmsiXif

แผนเปลี่ยนผ่านสู่ระบบบริการรูปแบบ Cloud

ตารางสรุปสำรวจความต้องการ GDCC cloud ของกระทรวงสาธารณสุข ในระดับเขตบริการสุขภาพ
เพื่อนำส่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในการขอรับจัดสรร GDCC cloud สำหรับเขตสุขภาพ ในปีงบประมาณ พ.ศ. 2566-2567

**การส่งข้อมูลระดับเขตสุขภาพ ให้บันทึกสรุปจำนวนความต้องการระดับจังหวัดและระดับเขต
จัดส่งไฟล์ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ. ภายใน วันที่ 10 มิ.ย.65 ที่ email ictmoph@moph.go.th และส่งหนังสือแจ้งเป็นทางการ**

ประมาณการความต้องการ Cloud เพื่อเก็บข้อมูลย้อนหลัง 10 ปี ในช่วงที่ของบประมาณ (ปีปฏิทิน พ.ศ. 2556-2567)			ความต้องการ cloud สำหรับฐานข้อมูลการบริการสุขภาพบุคคล ที่เกี่ยวข้องกับการคืน PHR และการส่งต่อ ของหน่วยบริการระดับ รพช. รพท. รพศ.										กรณีไม่สามารถแยกรายการได้ ให้ประมาณการผลรวมเฉพาะฐานข้อมูลที่กำหนด หากจังหวัดส่งข้อมูลไม่ทันกำหนด ให้ ITเขตประมาณการแทน	
			HIS		LIS		PACS		16 แฟ้มส่ง สป.สช. (ไม่แยกฐานจากHIS ใส่ 0)		43+แฟ้ม (ไม่แยกฐานจากHIS ใส่ 0)			
			ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67	ความต้องการ	โอนย้ายข้อมูลปี 66-67
1	จังหวัด	VM												
		CPU (core)												
		RAM (GB)												
		Storage (GB)												
2	จังหวัด	VM												
		CPU (core)												
		RAM (GB)												
		Storage (GB)												
3	สำนักงานเขต	VM												
		CPU (core)												
		RAM (GB)												
		Storage (GB)												

หมายเหตุ 1. การสำรวจไม่รวม รพ.สต. เนื่องจากจะมีการจัดสรร cloud รพ.สต. แยกไปอีก 1 ส่วน เพื่อรองรับการรองรับการกระจายอำนาจ
2. รพช. ที่ไม่สามารถตอบข้อมูลได้ใส่ NA เพื่อให้ IT ของจังหวัดประมาณการให้ หรือประสานบริษัทเจ้าของ HIS
3. โปรดระบุรหัสหน่วย 5 หลัก และชื่อจังหวัด , ชื่อเขตสุขภาพ
4. สสจ. รวบรวมจากทุก รพ. ในจังหวัด และสรุปรวมจำนวนระดับจังหวัด
5. สำนักงานเขตสุขภาพ รวบรวมจากทุก สสจ. ในเขต และสรุปรวมจำนวนระดับเขตสุขภาพ

แบบสำรวจสำหรับ สำนักงานเขตสุขภาพ รวบรวมจาก สสจ.
แล้วจัดส่งให้ ศทส.สป.สธ.
ภายในวันที่ 10 มิ.ย.65
อีเมล ictmoph@moph.go.th

ใช้ excel ในการบันทึกข้อมูลแบบสำรวจ
Download ได้ที่
https://moph.cc/7VYmsiXif

Thank you!