ร่าง

แนวปฏิบัติ

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและรายงาน

ของหน่วยงานสำนักงานปลัดกระทรวงสาธารณสุข

โดย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

รหัสเอกสาร : W–PA–CL–02.00Rev.00

สารบัญ

บทนำ 3

วัตถุประสงค์ 3

ขอบเขต 3

คำนิยาม 4

แผนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล 6

การประเมินความเสี่ยงเหตุละเมิดบุคคล 7

การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์ 10

กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล 11

การรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล 16

ภาคผนวก 17

1 การพิจารณาปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับความเสี่ยงตามเกณฑ์ดังต่อไปนี้ 17

2 แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล 19

บทนำ

สำนักงานปลัดกระทรวงสาธารณสุข (“สป.”) เล็งเห็นถึงความสำคัญของข้อมูลส่วนบุคคลที่ สป. จัดเก็บ รวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติให้เป็นไปตามหลักเกณฑ์และวิธีการที่กฎหมายกำหนด อย่างไรก็ตาม การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีรายละเอียดค่อนข้างมากและมีหลายประเด็นที่เป็นเรื่องใหม่สำหรับการขับเคลื่อนเศรษฐกิจและยกระดับการคุ้มครองสิทธิของสังคมไทย

สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตระหนักว่าในช่วงเวลาการประมวลผลข้อมูลส่วนบุคคล มีโอกาสที่จะเกิดเหตุการละเมินข้อมูลส่วนบุคคล ประกอบกับ มาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม แจ้งเหตุการละเมินข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ดังนั้น สป. มีการกำหนดกระบวนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลและแบบฟอร์มรายงานเหตุละเมินข้อมูลส่วนบุคคลเพื่อแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล เพื่อใช้เป็นแนวทางในการปฏิบัติเมื่อเกิดเหตุต้องมีการตอบสนองต่อเหตุละเมิดข้อมูลส่วนบุคคลที่เหมาะสม และสร้างความเชื่อมั่นต่อเจ้าของข้อมูลส่วนบุคคลที่ สป. มีการนำข้อมูลส่วนบุคคลมาประมวลผล

วัตถุประสงค์

แนวปฏิบัติฉบับนี้จัดทำเพื่อเป็นขั้นตอนและกระบวนการปฏิบัติการจัดการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลในการแก้ไขและลดผลกระทบต่อเจ้าของข้อมูลที่เกิดการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าเจ้าของข้อมูลจะได้รับผลกระทบจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลน้อยที่สุด และการรายงานเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล

ขอบเขต

กระบวนการปฏิบัติงานที่กำหนดไว้ในแนวปฏิบัติฉบับนี้ใช้กับการจัดการและการรายงานเหตุละเมิดข้อมูลส่วนบุคคลประกอบไปด้วย ช่องทางการเฝ้าระวังและตรวจสอบ กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคลการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุละเมิดข้อมูลส่วนบุคลลต่อสำนักงานปลัดกระทรวงสาธารณสุขภายใน 24 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ หากเป็นกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล พร้อมแนวทางการเยียวยาเจ้าของข้อมูลส่วนบุคคลในการแจ้งเหตุละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าด้วย ทั้งนี้ สป. จะดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

สำนักงานปลัดกระทรวงสาธารณสุขอาจแก้ไขเพิ่มเติมแนวทางนี้เป็นครั้งคราว โดย สป. จะแจ้งให้ผู้ปฏิบัติงานให้ สป. ทราบตามความเหมาะสม

คำนิยาม

คำศัพท์	ความหมาย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะเช่น ชื่อ นามสกุลที่อยู่ หมายเลขโทรศัพท์ เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษีเลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) ทะเบียนรถยนต์ IP Address, Cookies, Log File เป็นต้น
การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data)	การดำเนินการใดๆ กับข้อมูลส่วนบุคคล (อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในลักษณะใดลักษณะหนึ่งได้) เช่น การจัดเก็บ รวบรวมการบันทึก การจัดระบบจัดโครงสร้างการปรับปรุงหรือการแก้ไขข้อมูลการดึงข้อมูล การให้คำปรึกษาที่ต้องใช้ข้อมูลในการให้คำปรึกษา การใช้ข้อมูล การเปิดเผยด้วยการส่งต่อ การเผยแพร่ หรือการกระทำใด ๆ เพื่อให้ข้อมูลสามารถเข้าถึงหรือใช้งานได้ การรวมข้อมูลเข้าด้วยกัน การดำเนินการเพื่อให้ข้อมูลสอดคล้องกัน การจำกัดการใช้งาน การลบ หรือการทำลายข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่สามารถระบุตัวตนได้จากข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำ การแทนคนเสมือนไร้ความสามารถรวมตลอดทั้งผู้ที่ถือว่าเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ปลัดกระทรวงสาธารณสุข (บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล)
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือองค์กรใดที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลส่วนบุคคล
เหตุละเมิดข้อมูลส่วนบุคคล	การละเมิดความปลอดภัยของข้อมูลส่วนบุคคลที่ที่มีการเก็บรวบรวมใช้ หรือเผยแพร่ ซึ่งนำไปสู่ผลกระทบของเจ้าของข้อมูลส่วนบุคคล ความเสียหาย และความไม่ชอบด้วยกฎหมาย เช่น • การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • การแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • การลบข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • ข้อมูลส่วนบุคคลสูญหาย หรือถูกโจรกรรม • การประมวลผลข้อมูลส่วนบุคคลผิดพลาด/ไม่ถูกต้อง

	• การประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ที่กำหนดไว้
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หรือ DPO	เป็นเจ้าหน้าที่จะเข้ามาดูแลและให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลทั้งในองค์กร ไม่ว่าจะเป็นข้อมูลภายในขององค์กร หรือจะเป็นข้อมูลภายนอก โดย DPO ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล และตรวจสอบการใช้ข้อมูลส่วนบุคคล
เจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล	เป็นเจ้าหน้าที่สนับสนุนและประสานงานภายในหน่วยงาน (ตามคำสั่ง สำนักงานปลัดกระทรวงสาธารณสุข ที่ 1480/ 2565 สั่ง ณ วันที่ 30 มิถุนายน 2565)มีหน้าที่ ดังนี้ (๑) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุข (๒) ในกรณีพบเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล ถูกละเมิด ให้แจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุขโดยไม่ชักช้า ภายใน ๒๔ ชั่วโมง นับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เนื่องจากต้องแจ้งต่อไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง (๓) รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาในการปฏิบัติหน้าที่ (๔) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุขในการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของเจ้าข้อมูลส่วนบุคคลหรือข้อร้องเรียนใด ๆ ตามกฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคลในกรณีที่หน่วยงานเป็นผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (๕) ติดต่อประสานงานภายในหน่วยงาน ให้มีการดำเนินงานที่ถูกต้องตามกฎหมายว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล รวมทั้งให้คำแนะนำแก่หน่วยงาน ลูกจ้างหรือผู้รับจ้างเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ (๖) ทบทวนกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานให้ถูกต้องและเป็นปัจจุบัน (๗) ศึกษาและทำความเข้าใจกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
สคส.	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
คทง. BCM	คณะทำงานดำเนินการตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Management : BCM) หรืออาจเรียกชื่ออื่น
แผน BCP	แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan : BCP)
แผน DRP	แผนการกอบกู้ระบบหรือ DRP (Disaster Recovery Plan)
สป.สธ.	สำนักงานปลัดกระทรวงสาธารณสุข
หน่วยงาน	หน่วยงานภายใต้สังกัดสำนักงานปลัดกระทรวงสาธารณสุข ส่วนกลางและ ส่วนภูมิภาค รวมทั้งหน่วยงานตามภารกิจเฉพาะ

แผนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

เมื่อหน่วยงานได้รับแจ้งข้อมูลเบื้องต้นว่าเกิดเหตุการณ์ไม่ปกติ เข้าข่ายเป็นเหตุการละเมิดข้อมูลส่วนบุคคล จำต้องดำเนินการตาม 5 ขั้นตอน ดังต่อไปนี้

(1) ประเมินความน่าเชื่อถือของข้อมูลการละเมิดที่ได้รับแจ้ง และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถทำได้

หน่วยงานจะต้องดำเนินการประเมินว่าข้อมูลการละเมิดที่ได้รับแจ้งเบื้องต้นนั้น มีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลจริงหรือไม่ โดยหน่วยงานควรดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

- มาตรการเชิงองค์กร (organizational measures) เช่น นโยบายความมั่นคงปลอดภัยของข้อมูล การประเมินความเสี่ยง การสร้างความตระหนักและการอบรมความรู้แก่บุคลากรภายในองค์กร เป็นต้น
- มาตรการเชิงเทคนิค (technical measures) เช่น ระบบการเข้ารหัสข้อมูล (encryption) การทำข้อมูลแฝง (pseudonymisation) เป็นต้น และ
- มาตรการทางกายภาพ (physical measures) เช่น การมีระบบความปลอดภัย กล้องวงจรปิดสอดส่องดูแลบริเวณที่มีการเก็บเซิร์ฟเวอร์ของหน่วยงาน เป็นต้น ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

ทั้งนี้ หน่วยงานจะต้องดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับหน่วยงานเอง เพื่อยืนยันว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เพื่อประกอบพิจารณาในการดำเนินการขั้นตอนต่อไป

(2) ป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที

หน่วยงานได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด รวมทั้งประเมินความเสี่ยงของเหตุการละเมิดข้อมูลส่วนบุคคลแล้ว พบว่าเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้หน่วยงานดำเนินการใช้มาตรการในการป้องกัน ระงับ หรือแก้ไขให้เหตุการณ์ละเมิดนั้นสิ้นสุดลง หรือทุเลาลงเท่าที่สามารถกระทำได้โดยทันที

(3) แจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่ามีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง

- ให้หน่วยงานจะต้องแจ้งในสำนักงานปลัดกรทะรวงสาธารณสุขทราบภายใน 24 นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้
- หากเหตุการละเมิดดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานไม่สามารถแจ้งเหตุละเมิดดังกล่าวได้ จะต้องดำเนินการชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องกับการแจ้งเหตุล่าช้าแก่สำนักงานปลัดกระทรวงสาธารณสุขเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่ สป.โดยเร็วไม่เกินสิบวันนับแต่ทราบเหตุ

สำนักงานปลัดกระทรวงสาธารณสุขจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ กรณีมีเหตุจำเป็นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถแจ้งเหตุละเมิดที่ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลต้องโดยรายงานโดยไม่ชักช้าแต่ไม่เกินสิบห้าวันนับแต่ทราบเหตุ โดย สคส. จะพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าตามที่เห็นสมควร

(4) แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงนั้นให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดดังกล่าวโดยไม่ชักช้า พร้อมกับแจ้งแนวทางในการเยียวยาผลกระทบที่เกิดจากเหตุละเมิดดังกล่าวไปด้วยให้สำนักงานปลัดกระทรวงสาธารณสุขพร้อมรายงานตาม (3) เพื่อพิจารณาด้วย

วิธีการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล หนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หากโดยสภาพหน่วยงานไม่สามารถดำเนินการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล เนื่องจากไม่มีวิธีการติดต่อหรือโดยเหตุจำเป็นอื่นใด หน่วยงานอาจแจ้งเหตุการละเมิดเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคม ออนไลน์หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ หรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ เช่น เว็บไซต์ที่ให้บริการ แก่ผู้รับบริการ เป็นต้น ทั้งนี้ การแจ้งในลักษณะดังกล่าวจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

(5) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว

หน่วยงานจะต้องดำเนินการป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

การประเมินความเสี่ยงเหตุละเมิดบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้วางหลักการให้ สป.สธ. ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

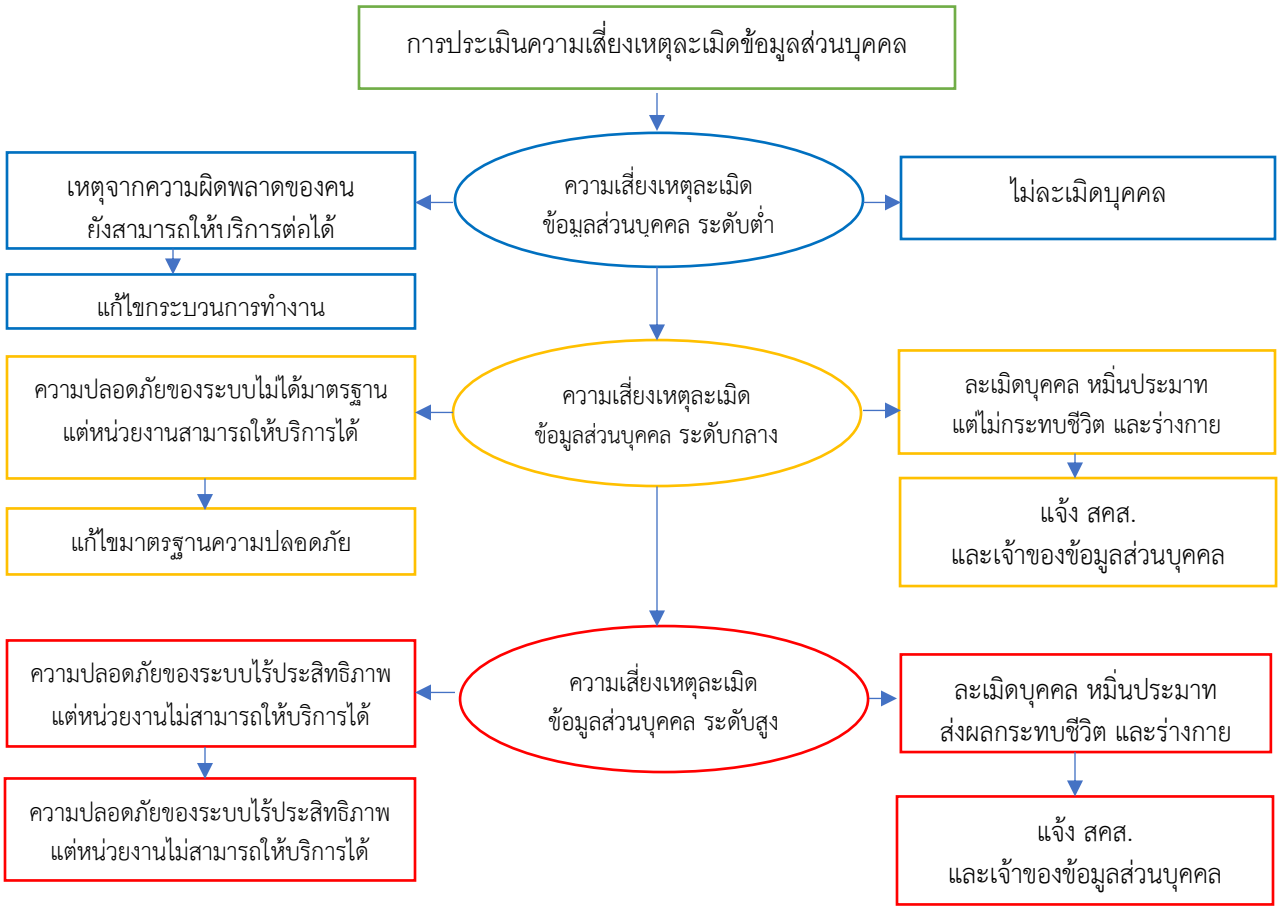
ทั้งยังวางหลักให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ สคส. โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

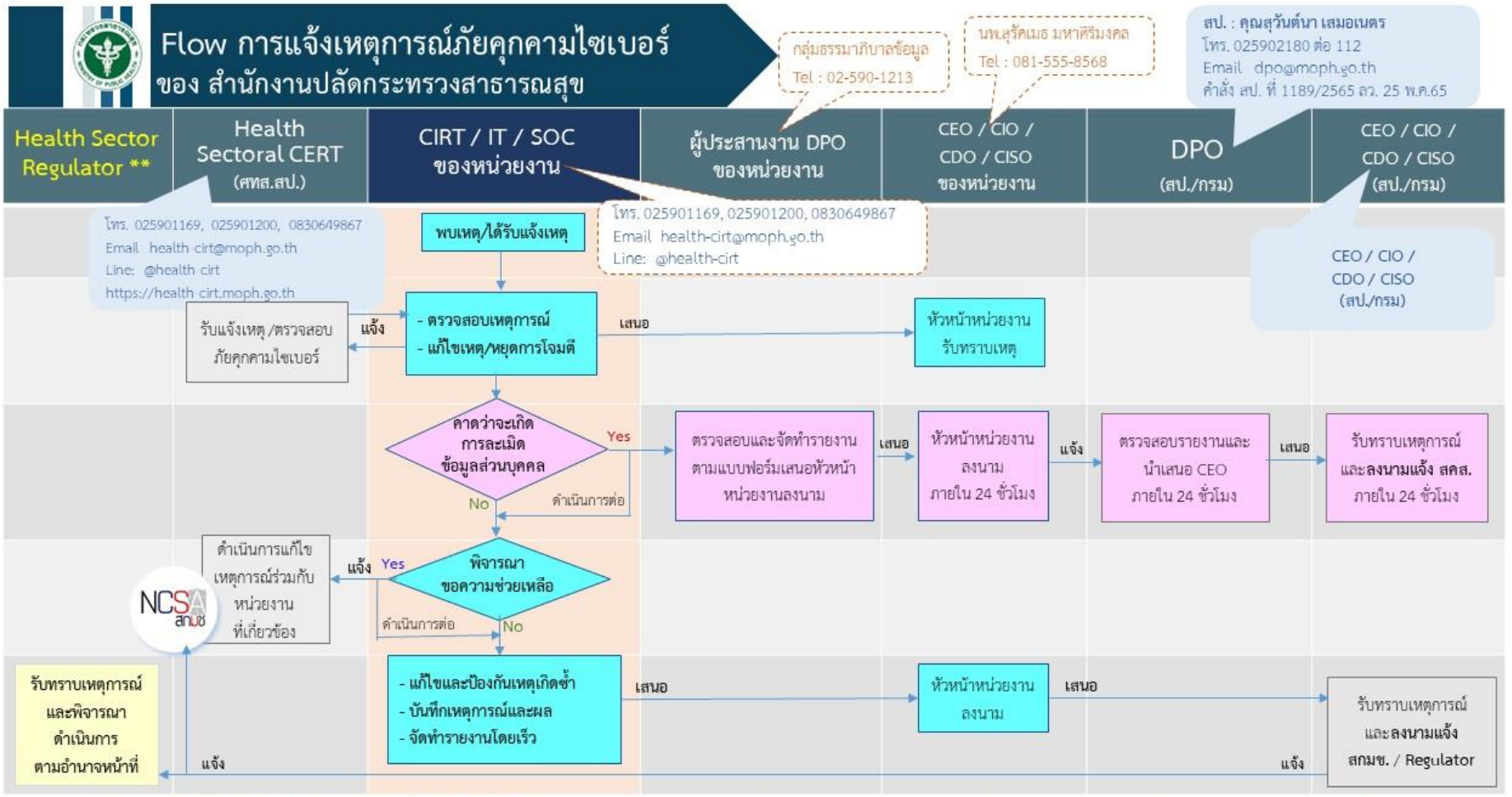
ดังนั้น การประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล จึงแยกประเมินเป็นเหตุละเมิด และเหตุจากระบบการรักษาความมั่นคงปลอดภัยของข้อมูล ดังนี้

1 การประเมินความเสี่ยงเหตุละเมิดบุคคล ต้องประเมินจากผลกระทบที่อาจเกิดความร้ายแรง ละเมิดต่อเจ้าของข้อมูลส่วนบุคคล เช่น ถูกนำไปประจาน ดูถูก ดูหมิ่นเกลียดชัง ถูกหมิ่นประมาท ถูกเลือกปฏิบัติ ถูกสะกดรอยตาม ถูกทำร้ายร่างกาย การแบล็คเมล์เรียกค่าไถ่ ถูกสวมรอยบุคคล ขโมยรหัสผ่านหรือเข้าถึงข้อมูลอื่น ๆ ต่อไป

2 การประเมินความเสี่ยงหตุการรักษาความมั่นคงปลอดภัย ต้องประเมินจากความร้ายแรงของผลกระทบ (Impact Levels) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ประกอบกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

ทั้งนี้ สำนักงานปลัดกระทรวงสาธารณสุขได้จัดทำปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับความเสี่ยง รายละเอียดตามภาคผนวก





** Regulator ของ หน่วยบริการสุขภาพ (รพ. ,คลินิก) คือ กรมสนับสนุนบริการสุขภาพ (สบส.)
Regulator ของ หน่วยงานที่ดำเนินการเกี่ยวกับผลิตภัณฑ์สุขภาพ (ยา, เวชภัณฑ์, เครื่องมือแพทย์) คือ อย.
Regulator ของ หน่วยงานที่มีการดำเนินการกับข้อมูลสุขภาพ (Digital health) ยกเว้นหน่วยบริการสุขภาพ คือ สป.(ศทส.)

- คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (ประสาน DPO ระดับจังหวัด/หน่วยงาน)
- แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th/

การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนจากการตรวจสอบ หรือทดสอบ หรือเกิดจุดอ่อนของระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

1) ให้ผู้รับผิดชอบเทคโนโลยีสารสนเทศ (CERT / IT / SOC)

1.1 ดำเนินการตรวจสอบยับยั้งการโจมตี หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

1.2 เสนอ ผู้บริหารของหน่วยงาน และแจ้ง Health Sectoral CERT ช่วยดำเนินการตรวจสอบ

1.3 กรณีที่มีการรั่วไหลหรือคาดว่าจะเกิดเหตุละเมิดข้อมูลส่วนบุคคลให้รีบแจ้งเจ้าหน้าที่ประสานงาน DPO หรือเจ้าหน้าที่คุ้มครองข้อมูล (DPO) ให้จัดทำรายงานฯ สรุปในเบื้องต้น นำเสนอให้ปลัดกระทรวง ภายใน 24 ชั่วโมงนับตั้งแต่เมื่อทราบเหตุละเมิด เพื่อ สป. จัดสรุปผลเสนอ สคส. ภายใน 72 ชั่วโมง

1.4 เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอ สป. เพื่อ สป. ส่งสรุปการดำเนินงานให้ สกมช. และ สคส. ต่อไป

2) ให้หัวหน้าหน่วยงาน

2.1 หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทางวินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง

2.2 หากเป็นบุคคลภายนอก ให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่เกี่ยวข้อง

2.3 ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

2.4 สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

แบบบันทึกรายงานภัย คุกคามทางไซเบอร์ (สำหรับหน่วยงานที่เกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ ตามบ สกมช.)
รหัสเอกสาร : F–PA–IM-01.01Rev00 ได้ที่ https://pdpa.moph.go.th/pdpa/index.php

กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล

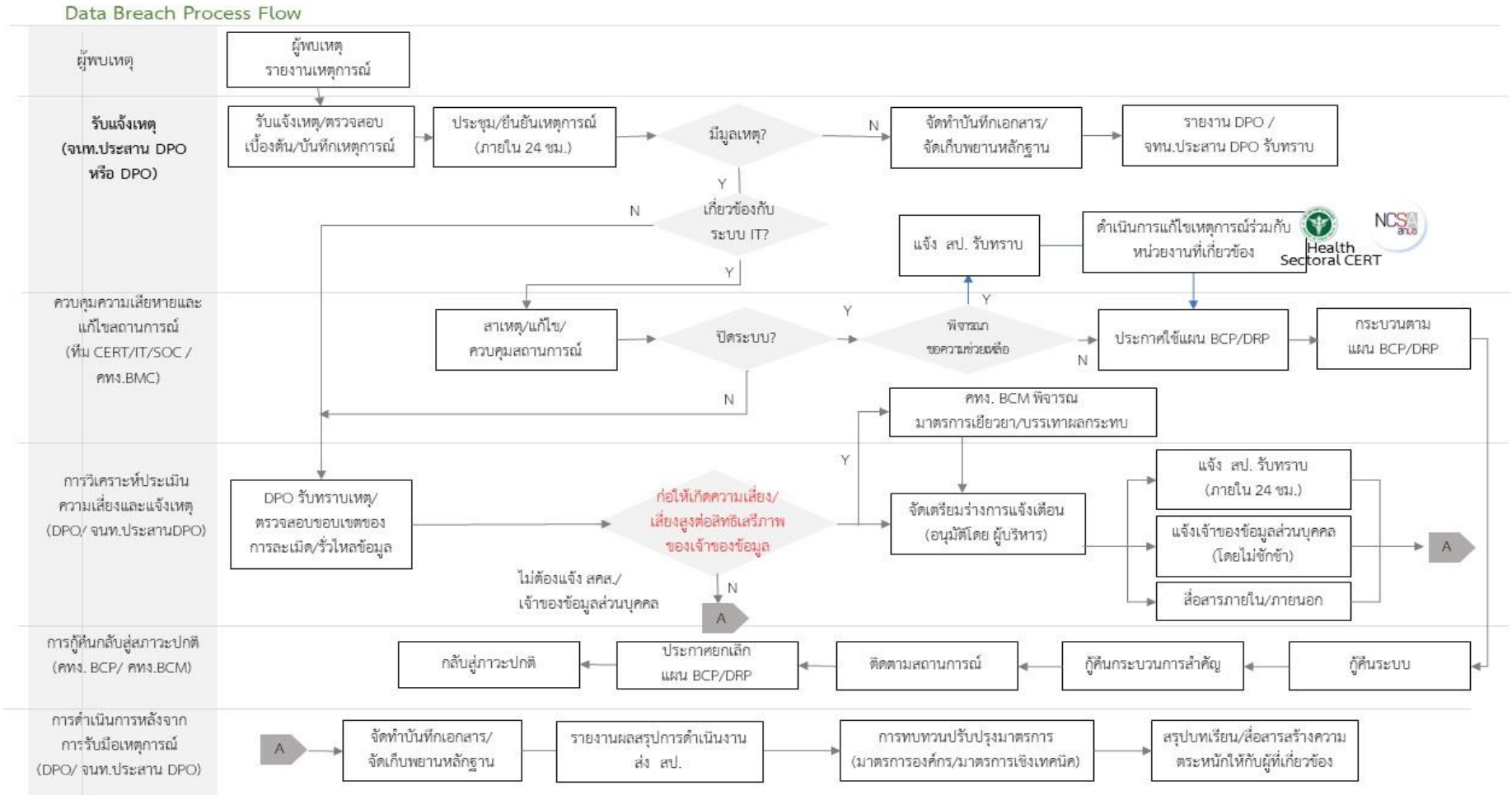
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 วรรค 1 และ วรรค 4 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า สำหนังานปลัดกระทรวงสาธารณสุขจึงได้กำหนดกระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล ดั้งนี้

1.การยับยั้งการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนที่อาจทำให้ข้อมูลรั่วไหลจากการตรวจสอบ หรือทดสอบหรือเกิดจุดอ่อนของระบบ

1) ให้ผู้รับผิดชอบของหน่วยงาน (CERT / IT / SOC)
   - 1.1 ดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง
   - 1.2 ให้แจ้งเจ้าหน้าที่ประสานงาน DPO ของหน่วยงาน เสนอหัวหน้าหน่วยงาน เพื่อหน่วยงานเตรียมร่าง
     - 1.2.1 จัดทำรายงานในเบื้องต้นเสนอปลัดกระทรวง ให้ภายใน 24 ชั่วโมงนับตั้งแต่เมื่อทราบเหตุละเมิด เพื่อ สป. จัดสรุปผลเสนอ สคส. ภายใน 72 ชั่วโมง
     - 1.2.2 แจ้งเจ้าข้อมูลข้อมูลส่วนบุคคล
     - 1.2.3 ทำการสื่อสารเกี่ยวกับเหตุการณ์ทั้งภายในและภายนอก
   - 1.3 เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอ สป. เพื่อ สป. ส่งสรุปการดำเนินงานให้ สกมช. และ สคส. ต่อไป
2) ให้หัวหน้าหน่วยงาน
   - 2.1 หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทางวินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง
   - 2.2 หากเป็นบุคคลภายนอก ให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่เกี่ยวข้อง
   - 2.3 ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)
   - 2.4 สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

2. การแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล



ข้อ 1 รับแจ้งเหตุรายงานเหตุการณ์ การควบคุมความเสียหายและการแก้ไขสถานการณ์

1) ผู้พบเหตุรายงานเหตุการณ์ พบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจให้รีบแจ้งเจ้าหน้าที่ประสานงาน DPO ทราบโดยทันที

2) เจ้าหน้าที่ประสานงาน DPO รับแจ้งเหตุและตรวจสอบข้อมูลเบื้องต้นพร้อมบันทึกเหตุการณ์

3) เจ้าหน้าที่ประสานงาน DPO ประชุมและหรือยืนยันเหตุการณ์ (ภายใน 24 ชม.) เจ้าหน้าที่ประสานงาน DPO จะต้องประเมินเหตุการณ์ ดังนี้

(ก) กรณีที่ไม่พบต้นเหตุการณ์การละเมิด

(1) เจ้าหน้าที่ประสานงาน DPO จัดทำบันทึกเอกสาร

(2) เจ้าหน้าที่ประสานงาน DPO จะรายงานข้อมูลให้ผู้บริหารและสำเนา DPO รับทราบ

(ข) กรณีที่มีพบต้นเหตุการณ์การละเมิด

เจ้าหน้าที่ประสานงาน DPO จะต้องพิจารณาว่าเหตุการณ์ ดังนี้

(1) กรณีที่เกี่ยวข้องระบบ IT

ทีม CERT/IT/SOC/เจ้าหน้าที่ประสานงาน DPO ทำการหาสาเหตุ แก้ไข และควบคุมสถานการณ์ พร้อมทั้งวิเคราะห์ว่าเหตุการณ์นั้นว่าจำเป็นต้องปิดระบบ IT หรือไม่

(1.1) กรณีที่ปิดระบบแล้ว

(1.1.1) แจ้ง คทง. BCM

(1.1.2) ทีม CERT/IT/SOC/เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

1) ดำเนินการประกาศใช้แผน BCP/DRP

2) กระบวนการตามแผน BCP/DRP

3) กู้คืนระบบ (DR-Site)

4) กู้คืนกระบวนการสำคัญ

5) ติดตามสถานการณ์

6) ประกาศยกเลิกแผน BCP/DRP

(1.1.3) กลับสู่ภาวะปกติ

(1.1.4) **ดำเนินการตามข้อ 2 ต่อไป**

(1.2) กรณีที่ไม่ปิดระบบแล้ว

(1.2.1) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO ตรวจสอบขอบเขตของการละเมิดหรือการรั่วไหลข้อมูล

(1.2.2) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO พิจารณาว่าความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อ สิทธิเสรีภาพของเจ้าของข้อมูล

(1.2.3) **ดำเนินการตามข้อ 2 ต่อไป**

(2) กรณีที่ไม่เกี่ยวข้องกับระบบ IT

(2.1) เจ้าหน้าที่ประสานงาน DPO รับทราบเหตุ ต้องดำเนินการ

1) ตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล
2) พิจารณาว่าระดับความเสี่ยงที่มีผลต่อสิทธิเสรีภาพของเจ้าของข้อมูล

(2.2) **ดำเนินการตามข้อ 2 ต่อไป**

ข้อ 2 การวิเคราะห์ประเมินความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล

ทีมทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPOตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล

ก. กรณีการละเมิดหรือรั่วไหลข้อมูลไม่ใช่ข้อมูลส่วนบุคคล

1) เจ้าหน้าที่ประสานงาน DPO จะรายงานข้อมูลให้ผู้บริหารและสำเนา DPO รับทราบ
2) ไม่ต้องแจ้งสคส. และหรือเจ้าขอข้อมูลส่วนบุคคล
3) ทีม CERT/IT/SOC ต้องจัดทำรายงานแจ้ง Health Sectoral Cert กระทรวงสาธารณสุข

ข. กรณีการละเมิดหรือรั่วไหลข้อมูลเป็นข้อมูลส่วนบุคคล

1) คทง. BCM พิจารณามาตรการเยียวยาและบรรเทาผลกระทบ
2) ทีม CERT/IT/SOC ต้องจัดทำรายงานแจ้ง Health Cert กระทรวงสาธารณสุข
3) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO จัดเตรียมร่างการแจ้งเตือน (อนุมัติโดยผู้บริหาร)
4) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO ดำเนินการวิเคราะห์ระดับความเสี่ยง

4.1) กรณีมีระดับความเสี่ยงสูงต่อสิทธิของเจ้าของข้อมูล (ระดับความเสี่ยงสูง)

4.1.1) เจ้าหน้าที่ประสานงาน DPO จัดทำรายงานและแนวทางเยี่ยวยา แจ้งให้ผู้บริหารหน่วยงานและ DPOเพื่อเสนอให้ปลัดกระทรวงและส่ง สคส.รับทราบ (ภายใน 72 ชม.) ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลาให้หน่วยงานอาจพิจารณานำเสนอรายงานเบื้องต้นต่อ สคส.และปลัดกระทรวงพร้อมกันได้

4.1.2) สป. และหน่วยงานแจ้งสาเหตุและแนวทางเยี่ยวยาต่อเจ้าของข้อมูลส่วนบุคคล

4.1.3) สป. และหน่วยงานดำเนินการสื่อสารภายในและภายนอก

4.1.4) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินงาน

(1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน
(2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)
(3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

4.2) กรณีมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล(ระดับความเสี่ยงน้อย หรือปานกลาง)

4.2.1) เจ้าหน้าที่ประสานงาน DPO แจ้งให้ผู้บริหารและ DPO เพื่อเสนอปลัดกระทรวงและส่ง สคส.รับทราบ (ภายใน 72 ชม.) ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลาหน่วยงานนำเสนอรายงานต่อ สคส.กับ CDC พร้อมกันได้

4.2.2) หน่วยงานดำเนินการสื่อสารภายในและภายนอก

4.2.3) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

(1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

(2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

(3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

4.3) กรณีไม่มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล

4.3.1) เจ้าหน้าที่ประสานงาน DPO แจ้งให้ ผู้บริหารและ DPO เพื่อเสนอ CDO รับทราบ

4.3.2) หน่วยงานดำเนินการสื่อสารภายใน

4.3.3) ทีม CERT/IT/SOC /เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

(1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

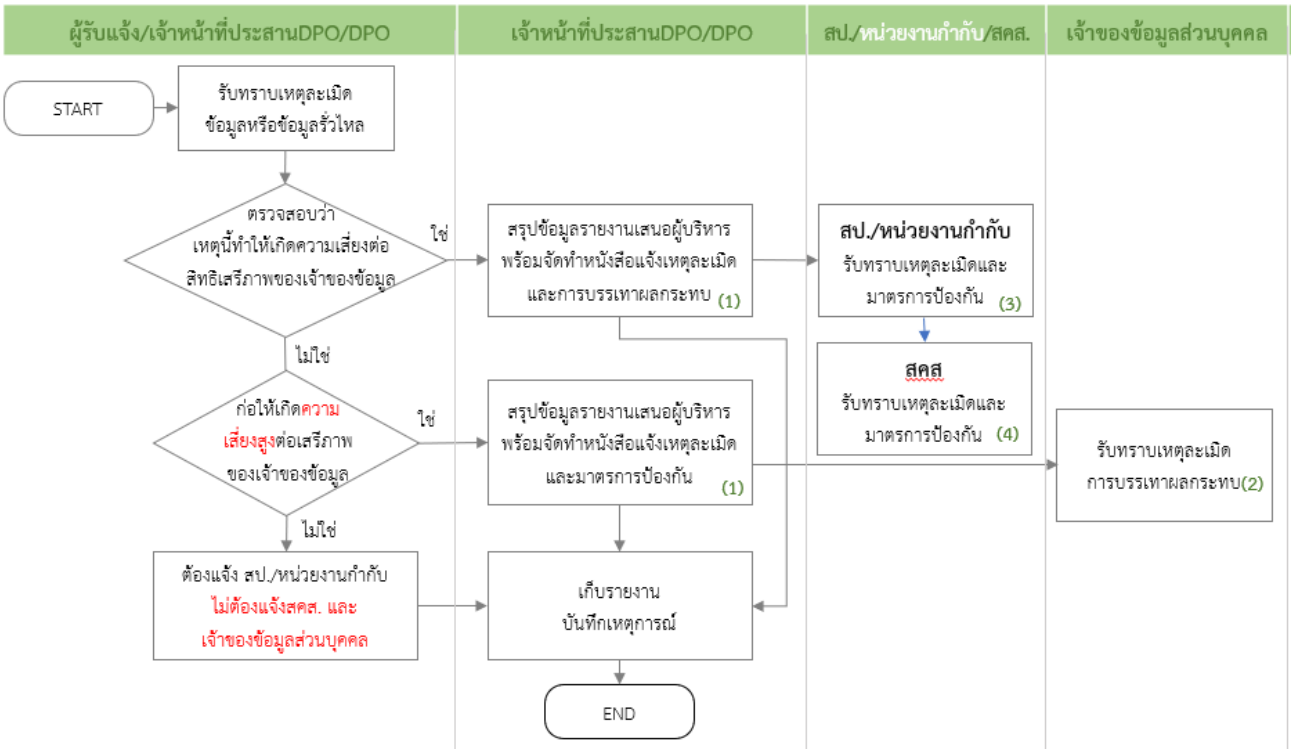
(2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

(3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

การรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลและคณะทำงานข้อมูลส่วนบุคคลประเมินผลกระทบของเหตุการณ์การละเมิดข้อมูลส่วนบุคคล ผลการพิจารณาระดับความรุนแรงมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลระดับ ต่ำ, ปานกลาง, สูง ให้ดำเนินการรายงานเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขั้นตอนการดำเนินงาน กรณีมีการละเมิดข้อมูลหรือข้อมูลรั่วไหล



ภาคผนวก: ประกอบด้วย

- การพิจารณาปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับความเสี่ยงตามเกณฑ์
- 1 : แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (สำหรับหน่วยงานที่เกิดเหตุการละเมิดข้อมูลส่วนบุคคล)
- 2 : ตัวอย่างการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล
- 3 : ตัวอย่างหนังสือการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อปลัดกระทรวงสาธารณสุข
- 4. ตัวอย่างการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาคผนวก

1 **การพิจารณาปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับความเสี่ยงตามเกณฑ์ดังต่อไปนี้**

คะแนนสำหรับระดับความเสี่ยง	ระดับความเสี่ยง
0	ไม่มีความเสี่ยง
1-7	ความเสี่ยงน้อย
8-14	ความเสี่ยงปานกลาง
15-21	ความเสี่ยงสูง

หัวข้อประเมิน ปัจจัยความเสี่ยง	คะแนนความเสี่ยง			
	0	1	2	3
1. จำนวนเจ้าของข้อมูลที่อาจได้รับผลกระทบ	ไม่มีเจ้าของข้อมูลที่ได้รับผลกระทบ เช่น จำนวนข้อมูลที่รั่วไหลเป็นจำนวนสถิติ หรือข้อมูลที่ได้รับการแปลงแล้ว	ทราบจำนวนเจ้าของข้อมูลแน่นอนซึ่งไม่เกิน 50 คน	คาดหมายว่าอาจมีเจ้าของข้อมูลที่ได้รับผลกระทบไม่เกิน 100 คน	มากกว่า 100 คน หรือไม่สามารถระบุจำนวนเจ้าของข้อมูลได้
2. ลักษณะของข้อมูลที่รั่วไหล	ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น ข้อมูลนิรนามและข้อมูลภาพรวมเชิงสถิติ เป็นต้น และข้อมูลทั่วไปที่สามารถระบุตัวบุคคลได้ แต่เป็นข้อมูลที่	ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ทันที (โดยไม่รวมถึงข้อมูลอ่อนไหว) ต้องประกอบกับข้อมูลอื่น เช่น รหัสพนักงาน ที่อยู่ หมายเลขโทรศัพท์เป็นต้น	ข้อมูลส่วนบุคคล ที่สามารถระบุตัวเจ้าของข้อมูลได้ทันที เช่น ชื่อของเจ้าของข้อมูล ภาพถ่าย วิดีโอ เป็นต้น	ข้อมูลอ่อนไหว (Sensitive Data) เช่นเชื้อชาติ ความ เห็นทางการเมืองศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลชีวภาพ เป็นต้น
3. ระยะเวลาการพบการรั่วไหล	ทราบเหตุทันทีที่เกิดการรั่วไหล	ทราบเหตุภายใน 24 ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายหลัง 24 ชั่วโมง แต่ไม่เกิน 72 ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายหลัง 72 ชั่วโมง นับแต่การรั่วไหล
4. การเข้าถึงข้อมูลของบุคลากรของหน่วยงานเมื่อถูกโจรกรรมข้อมูล	บุคลากรสามารถเข้าถึงข้อมูลได้ปกติ	บุคลากรไม่สามารถเข้าถึงข้อมูลบาง ส่วนเป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมดเป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมดเป็นการถาวร

หัวข้อประเมิน ปัจจัยความเสี่ยง	คะแนนความเสี่ยง			
	0	1	2	3
5. ความเสียหายต่อข้อมูลเมื่อถูกโจรกรรมข้อมูลหรือถูกเข้าโดย ไม่ได้รับอนุญาต หรือเกิดจากความผิดพลาดของบุคลากรที่เกี่ยวข้อง	ข้อมูลไม่ได้ถูกแก้ไข/เสียหายประการใด	ข้อมูลถูกแก้ไข แต่ยังไม่ถูกนำไปใช้งาน ซึ่งหน่วยงานคงมีข้อมูลสำรอง และสามารถใช้ข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งานโดยไม่ทราบว่ามีการแก้ไขข้อมูล ทั้งนี้ หน่วยงานยังคงมีข้อมูลสำรองและสามารถใช้ข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งานโดยไม่ทราบว่ามีการแก้ไขข้อมูล ซึ่งหน่วยงานไม่มีข้อมูลสำรอง
6. ขอบเขตในการรั่วไหลของข้อมูล	ข้อมูลไม่ได้ถูกเปิดเผยหรือถูกเข้าถึงโดยมิชอบโดยบุคคลที่ไม่ได้รับอนุญาต	ข้อมูลที่รั่วไหลอาจถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตภายในหน่วยงาน แต่ยังไม่พบหลักฐานว่าบุคคลที่ไม่ได้รับอนุญาตดังกล่าว มีการประมวลผลโดยมิชอบเช่น เอกสารหายภายในอาคารหน่วยงาน หรืออุปกรณ์อิเล็กทรอนิกส์ถูกเลิกใช้งานโดยไม่ลบทำลายข้อมูล	ข้อมูลถูกเปิดเผยต่อหรือเข้าถึงโดยบุคคลภายนอก โดยทราบุคคลภายนอกดังกล่าว เช่น การส่งอีเมลผิดให้ผู้อื่น พร้อมเอกสารแนบซึ่งเป็นข้อมูลส่วนบุคคล แต่ผู้รับข้อมูลไม่สามารถเปิด หรืออ่านข้อมูลได้ต้องใช้มาตรการทางเทคนิคจึงจะเข้าถึงข้อมูลได้	ข้อมูลถูกเปิดเผย หรือเข้าถึงโดยบุคคลภายนอกที่ไม่เกี่ยวข้องโดยไม่ทราบจำนวน เช่น ถูกเปิดเผยสาธารณะ หรือ มีการขายข้อมูลลูกค้า/ผู้ใช้บริการให้บุคคลภายนอก
7. ผลกระทบทีอาจเกิดขึ้นต่อเจ้าของข้อมูลจากการรั่วไหล	ไม่มีผลกระทบต่อเจ้าของข้อมูลเนื่องจากเป็นข้อมูลที่เป็นสาธารณะอยู่ก่อนการรั่วไหล หรือ ฝ่ายงานสามารถป้องกันเหตุที่อาจเกิดขึ้นแล้ว	คาดว่าจะไม่เกิดผลกระทบต่อเจ้าของข้อมูล แต่อาก่อให้เกิดความรำคาญต่อเจ้าของข้อมูล เช่น ต้องกรอกข้อมูลในระบบใหม่ หรือลักษณะของข้อมูลที่รั่วไหลไม่สามารถกระทบต่อการดำรงชีวิตของเจ้าของข้อมูลได้	อาจก่อให้เกิดผลกระทบโดยอ้อม ต่อสิทธิ ทรัพย์สิน และร่างกาย เช่น เกิดความกลัว หรือความกังวล	อาจก่อให้เกิดผล กระทบโดยตรงที่ไม่อาจแก้ไขได้โดยง่าย เช่น ได้รับความเสียหายต่อทรัพย์สิน ถูกเลิกจ้าง การถูกปฏิเสธในการรับบริการถูกดำเนินคดี เสียสุขภาพ หรือเจ็บป่วยรุนแรง หรือระยะยาวหรือเสียชีวิต

2 **แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล** (https://pdpa.moph.go.th/pdpa/index.php)

สำนักงานปลัดกระทรวงสาธารณสุข OFFICE OF THE PERMANENT SECRETARY MINISTRY OF PUBLIC HEALTH	**ชื่องาน :แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล** (สำหรับหน่วยงานที่เกิดเหตุการละเมิดข้อมูลส่วนบุคคล)		**เริ่มใช้** 1เม.ย66
	ชั้นความลับ :ใช้ภายนอก	**รหัสเอกสาร :**F–PA–CL-02.01Rev01	**หน้าที่**19**ของ**26

เลขที่.....(ส่วนหน่วยงานผู้แจ้ง/รับแจ้ง)	**วันที่แจ้ง/รับแจ้ง**.....

แบบฟอร์มฉบับนี้ใช้สำหรับหน่วยงานที่เกิดเหตุการละเมิดข้อมูลส่วนบุคคลและต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**ขอความกรุณาอย่ากรอกข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับเหตุการละเมิดข้อมูลส่วนบุคคลในแบบฟอร์มฉบับนี้** เช่น ห้ามใส่ชื่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล หาก สป.สธ. และ สคส. ต้องการข้อมูลดังกล่าว จะทำการติดต่อท่านไปในภายหลัง

หน่วยงานควรตรวจสอบให้แน่ใจว่าข้อมูลที่ให้นั้นถูกต้องที่สุดและมีรายละเอียดครบถ้วนมากที่สุดเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

กรุณาตอบคำถามต่อไปนี้เพื่อช่วยให้ สป.สธ. และ สคส. ดำเนินการเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลของท่านอย่างมีประสิทธิภาพและเพื่อทำความเข้าใจหน่วยงานของท่านได้ดียิ่งขึ้น

ส่วนที่ 1 ผู้แจ้ง/ผู้รับแจ้งเหตุการณ์

ชื่อ-นามสกุล:	ตำแหน่ง: .....
หน่วยงาน:	
เบอร์โทร:	เบอร์โทรสาร: .....
อีเมล: ..... หน่วยงาน/ผู้ประสานงานสำหรับติดต่อ	
ที่อยู่เพื่อการติดต่อ	
.....	

ส่วนที่ 2 รายละเอียดเหตุการณ์

วันที่พบเหตุการณ์ละเมิด :	เวลาที่พบเหตุการณ์ละเมิด : ..... นาฬิกา
วันที่เกิดเหตุการณ์ละเมิดขึ้น :	เวลาที่เกิดเหตุการละเมิดขึ้น:..... นาฬิกา
กิจกรรม/ระบบที่เกิดเหตุ:.....	
.....	
.....	
.....	
รายละเอียดเหตุการณ์:	
(1) กรุณาอธิบายเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น	
.....	

(2) กรุณาอธิบายว่าเหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นได้อย่างไร

.....

(3) หน่วยงานพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลได้อย่างไร เช่น พบเหตุจากกระบวนการตรวจสอบภายใน

.....

(4) หน่วยงานมีมาตรการป้องกันอะไรบ้าง

.....

(5) ประเภทของการละเมิด

☐ รูปแบบเอกสาร ☐ รูปแบบอิเล็กทรอนิกส์ ☐ระบบงาน

(6) เหตุการละเมิดข้อมูลส่วนบุคคลเกิดจากสาเหตุทางไซเบอร์หรือไม่

☐ ใช่ ☐ไม่ใช่ ☐ไม่ทราบ

ส่วนที่ 3 ผลกระทบ(ทำเครื่องหมายทุกข้อที่เกี่ยวข้อง ได้มากกว่า 1 ข้อ)

ประเภทของข้อมูลที่ถูกละเมิด:	☐ข้อมูลเจ้าหน้าที่และผู้บริหาร ☐ข้อมูลผู้มารับบริการ เช่น ผู้ป่วย ผู้มาติดต่อ ☐ข้อมูลผู้สมัครงาน ☐ข้อมูลผู้เข้าร่วมฝึกอบรมภายในหน่วยงาน ☐ที่ปรึกษา และบุคคลที่เกี่ยวข้อง ☐ลูกจ้างตามสัญญาจ้าง หรือผู้ที่ทำงาน หรือปฏิบัติงาน ☐กรรมการ และผู้บริหาร ☐ข้อมูลอื่นๆ (ระบุ)..... ☐ข้อมูลอื่นๆ (ระบุ)..... ☐ข้อมูลอื่นๆ (ระบุ)..... ☐ไม่สามารถระบุได้ในขณะนี้
ข้อมูลที่ถูกละเมิด:	**ข้อมูลส่วนบุคคลทั่วไป** ☐ ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล วันเดือนปีเกิด การศึกษา ข้อมูลติดต่อUsername Password เป็นต้น ☐ ประวัติการทำงานเช่นสถานะวิชาชีพตำแหน่งงาน ผลการประเมินผลการปฏิบัติงาน ☐ข้อมูลเอกสารราชการบัตรประจำตัวประชาชนหนังสือเดินทาง ใบขับขี่ บัตรข้าราชการ ☐ข้อมูลด้านการเงิน เช่น ธุรกรรมทางการเงิน ข้อมูลภาษี เลขที่บัญชี เลขบัตรเครดิต ☐ ข้อมูลภาพวิดีทัศน์กล้องวงจรปิด

	☐ข้อมูลที่เกี่ยวเนื่องกับบุคคล เช่น IP address บทสนทนา และการสื่อสารทางโทรศัพท์ หรืออุปกรณ์อิเล็กทรอนิกส์ ☐ข้อมูลอื่นๆ (โปรดระบุ)..... ☐ไม่สามารถระบุได้ในขณะนี้ **ข้อมูลส่วนบุคคลที่มีความอ่อนไหว** ☐ ข้อมูลเกี่ยวกับเชื้อชาติ ☐ ข้อมูลเกี่ยวกับศาสนา ☐ ข้อมูลด้านความคิดเห็นทางการเมือง ☐ ประวัติอาชญากรรม ☐ ข้อมูลสุขภาพ/สุขภาพจิต ☐ ข้อมูลสหภาพแรงงาน ☐ ข้อมูลพันธุกรรม ☐ ข้อมูลเกี่ยวกับชีวิตทางด้านเพศ ☐ ข้อมูลเกี่ยวกับรสนิยมทางเพศ ☐ ข้อมูลการแปลงเพศ ☐ ข้อมูลตำแหน่ง เช่น พิกัด ☐ ข้อมูลชีวมิติ (อาทิ ภาพสแกนใบหน้า/ม่านตา ลายนิ้วมือ ฟิล์มเอกซเรย์ เสียง) ☐ข้อมูลอื่นๆ (โปรดระบุ)..... ☐ไม่สามารถระบุได้ในขณะนี้
ปริมาณของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ	☐ จำนวน.....คน/record ☐ ไม่สามารถระบุจำนวนได้ในขณะนี้
ลักษณะเหตุการละเมิดอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล	☐ กลุ่มของข้อมูลที่มีความเฉพาะข้อมูลที่เป็นความลับหรือข้อมูลที่มีความเสี่ยงสูงเมื่อเกิดเหตุละเมิดเช่นข้อมูลทางการเงินประวัติสุขภาพเป็นต้น ☐ จำนวนความหลากหลายของข้อมูลส่วนบุคคลเช่นกลุ่มของข้อมูลที่รั่วไหลประกอบด้วยชื่อที่อยู่อาชีพประวัติการศึกษาอายุ ☐ ความยากง่ายในการระบุถึงตัวบุคคลเช่นข้อมูลที่ถูกละเมิดไม่ได้เป็นข้อมูลแฝงหรือเป็นข้อมูลที่เข้ารหัส ☐ ข้อมูลส่วนบุคคลของผู้ที่มีความเสี่ยงต่อการล่วงละเมิดหรืออาชญากรรมเช่นข้อมูลของพยานในคดีข้อมูลของเหยื่อผู้ถูกล่วงละเมิด ☐ การรั่วไหลที่มีสาเหตุมาจากการโจมตีโดยผู้ไม่ประสงค์ดีที่มุ่งเน้นในการเข้าถึงข้อมูลที่เป็นความลับ ☐ข้อมูลอื่นๆ (โปรดระบุ).....

รายละเอียดของลกระทบที่อาจจะเกิด หรือเกิดไปแล้วต่อเจ้าของข้อมูลส่วนบุคคล:	....
รายละเอียดของผลกระทบที่น่าจะเกิดจากการละเมิด:	....
การประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล(ตามเกณฑ์ภาคผนวก	☐สูง - ส่งผลกระทบต่อสุขภาพ เสรีภาพ และชีวิตของเจ้าของข้อมูล ☐ปานกลาง - ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของเจ้าของข้อมูล ☐ต่ำ – ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลต่ำ ☐ไม่มีความเสี่ยง - เป็นข้อมูลส่วนบุคคลที่เข้าถึงได้สาธารณะอยู่ก่อนแล้ว

ส่วนที่ 4 การตอบสนองเพื่อระงับเหตุการณ์

การตอบสนองเพื่อระงับเหตุการณ์(ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ข้อ ๕(๕)	....
แนวทางเยียวยาเจ้าของข้อมูล (กรณีผลกระทบสูง) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ประกาศ สคส. ข้อ ๖(๔)	(โปรดระบุมาตรการการแก้ไขปัญหา เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น) สาเหตุของปัญหา..... ..... การแก้ไขระยะสั้น..... ..... การแก้ไขระยะยาว..... .....

ส่วนที่ 5 การวิเคราะห์สาเหตุ และป้องกันการเกิดซ้ำ

สาเหตุ	(โปรดอธิบาย เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด) .....
การป้องกัน/การขจัดสาเหตุ	(โปรดระบุแผนงาน และการป้องกัน การเกิดเหตุการณ์ซ้ำ) ....

หน่วยงานที่รับผิดชอบ	(โปรดระบุหน่วยงาน/กลุ่ม/ฝ่าย/งาน ที่รับผิดชอบในการดำเนินการตามแผนข้างต้น) 1..... เบอร์โทร:.....e-Mail :..... 2..... เบอร์โทร:.....e-Mail :.....

ส่วนที่ 6 การแจ้งต่อหน่วยงานที่เกี่ยวข้อง

1. แจ้งต่อผู้คุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวง ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง
2. แจ้งต่อผู้บริหารของหน่วยงาน ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง
3. แจ้งความ / ลงบันทึกประจำวันต่อเจ้าหน้าที่ตำรวจ ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง
4. แจ้งต่อเจ้าของข้อมูลส่วนบุคคล*
   - ☐ ดำเนินการแจ้งเจ้าของข้อมูลเรียบร้อยแล้ว วันที่..... ช่องที่ใช้ในการแจ้ง.....
   - ☐ อยู่ระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล
   - ☐ สำนักงานปลัดกระทรวงสาธารณสุข และ/หรือ หน่วยงาน ตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล
   - ☐ อยู่ระหว่างการพิจารณาของสำนักงานปลัดกระทรวงสาธารณสุข และ/หรือ หน่วยงาน
   - ☐ อื่นๆ (โปรดระบุ) _____

* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง

ผู้รายงาน (หัวหน้าหน่วยงานที่ถูกละเมิด)

ชื่อ-นามสกุล:	ตำแหน่ง:
ส่วนราชการ:	เบอร์โทร:
e-Mail :	

ส่วนที่ 7 แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPO เป็นผู้บันทึกข้อมูล)

5. แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล*

☐ แจ้งเรียบร้อยแล้ว ☐ไม่ต้องแจ้งเพราะการละเมิดไม่ใช่ข้อมูลส่วนบุคคล หรือไม่มีข้อมูลรั่วไหล

☐ ยังไม่แจ้ง เนื่องจาก .....

* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง

ผู้รายงาน (ผู้ควบคุมข้อมูลส่วนบุคคล)

ชื่อ-นามสกุล:	ตำแหน่ง: ปลัดกระทรวงสาธารณสุข
ส่วนราชการ: สำนักงานปลัดกระทรวงสาธารณสุข	เบอร์โทร: 02 5902180 ต่อ 112
e-Mail :dpo@moph.go.th https : pdpa.moph.go.th	

ตัวอย่าง หนังสือการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของหน่วยงานต่อปลัดกระทรวงสาธารณสุข

เรื่อง รายงานเหตุละเมิดข้อมูลส่วนบุคคล

เรียน ปลัดกระทรวงสาธารณสุข

สิ่งส่งมาด้วย:แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล จำนวน ๑ ชุด

ด้วย....ชื่อหน่วยงาน..... ได้ตรวจพบเหตุละเมิดข้อมูลส่วนบุคคลที่....ชื่อหน่วยงาน..... ทำการเก็บรักษาอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่ง....ชื่อหน่วยงาน..... พิจารณาว่าเหตุดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตามความของมาตรา 37(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒....ชื่อหน่วยงาน.....สำนักงานปลัดกระทรวงสาธารณสุข ขอรายงานเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังเอกสารแนบ

ทั้งนี้ ....ชื่อหน่วยงาน..... ยินดีให้ความร่วมมือในการสอบสวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้ โดยสามารถติดต่อ....ชื่อหน่วยงาน..... ได้ที่.....โทร..... อีเมล.....

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไปด้วย จักเป็นพระคุณ

(ลงชื่อ).....

ตำแหน่ง.....

ตัวอย่าง หนังสือการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุขต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง รายงานเหตุละเมิดข้อมูลส่วนบุคคล
เรียน เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เอกสารแนบ แบบฟอร์มรายงานเหตุละเมิดข้อมูลส่วนบุคคล

ด้วย สำนักงานปลัดกระทรวงสาธารณสุข ได้ตรวจพบเหตุละเมิดข้อมูลส่วนบุคคลที่....ชื่อหน่วยงาน..... ทำการเก็บรักษาอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งสำนักงานปลัดกระทรวงสาธารณสุข จารณาว่าเหตุดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตามความของมาตรา ๓๗(๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒สำนักงานปลัดกระทรวงสาธารณสุข ขอรายงานเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังเอกสารแนบ

ทั้งนี้ สำนักงานปลัดกระทรวงสาธารณสุข ยินดีให้ความร่วมมือในการสอบสวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้ โดยสามารถติดต่อ....ชื่อหน่วยงาน..... ได้ที่.....โทร.....

อีเมล.....

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไปด้วย จักเป็นพระคุณ

(ลงชื่อ).....

ตำแหน่ง.....ปลัดกกระทรวงสาธารณสุข.....

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลและคณะทำงานข้อมูลส่วนบุคคลประเมินผลกระทบของเหตุการณ์การละเมิดข้อมูลส่วนบุคคล ผลการพิจารณาระดับความรุนแรงระดับ ต่ำ, ปานกลาง, สูง ถ้าเหตุละเมิดข้อมูลส่วนบุคคลที่มีผลการพิจารณาระดับความรุนแรงระดับปานกลางหรือสูงต่อเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งเจ้าของข้อมูล

ตัวอย่างการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

เรื่อง รายงานเหตุละเมิดข้อมูลส่วนบุคคล ....ชื่อหน่วยงาน.....

เรียน คุณ.....

จากการที่ สำนักงานปลัดกระทรวงสาธารณสุข โดย....ชื่อหน่วยงาน..... ได้ทำการเก็บรักษาข้อมูลส่วนบุคคลของท่านภายใต้*มาตรการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมาตรการในการตรวจสอบการละเมิดข้อมูลส่วนบุคคลอย่างต่อเนื่อง* พบว่ามีเหตุละเมิดข้อมูลส่วนบุคคลที่....ชื่อหน่วยงาน..... ทำการเก็บรักษาอยู่ โดยเหตุการณ์ที่ตรวจพบคือ.....ตรวจพบเมื่อวันที่.....เหตุเกิดเมื่อวันที่ ..... ประเภทของการละเมิด..ข้อมูลส่วนบุคคล/ข้อมูลอ่อนไหว.....ข้อมูลที่ถูกละเมิด..... ความรุนแรงของผลกระทบ..... ซึ่งส่งผล (อาจส่งผล) ให้.....

....ชื่อหน่วยงาน..... ได้ดำเนินการระงับเหตุการณ์ดังกล่าว และวิเคราะห์หาสาเหตุ รวมถึงดำเนินการเพื่อป้องการการเกิดขึ้นซ้ำ

....ชื่อหน่วยงาน..... ขอแนะนำให้ท่านดำเนินการ ดังนี้

๑. .....

๒. .....

ทั้งนี้ ....ชื่อหน่วยงาน..... มีมาตรการเยียวยาสำหรับเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ดังนี้

๑. .....

๒. .....

หากท่านต้องการข้อมูลเพิ่มเติม สามารถติดต่อ ได้ที่:

เจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล โทร..... อีเมล.....

เจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ โทร..... อีเมล.....

ขออภัยเป็นอย่างสูง

(ลงชื่อ).....

ตำแหน่ง.....