ที่ สธ ๐๒๑๒/ ว ๑๔๐๓๙

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๔ มิถุนายน ๒๕๖๕

เรื่อง แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ฉบับที่ ๒

เรียน นายแพทย์สาธารณสุขจังหวัด/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง/ผู้อำนวยการสำนักงานเขตสุขภาพ ๑-๑๓/ สำนักงานรัฐมนตรี และหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ฉบับที่ ๒ จำนวน ๑ ชุด

ตามที่สำนักงานปลัดกระทรวงสาธารณสุข ได้แจ้งเวียนและเผยแพร่แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ฉบับที่ ๑ ผ่านเว็บไซต์ https://pdpa.moph.go.th เพื่อให้หน่วยงานในสังกัดได้นำไปปฏิบัติ พร้อมทั้งได้แจ้งให้หน่วยงานดำเนินการติดตามข้อมูลข่าวสารมาระยะหนึ่งแล้ว นั้น

สำนักงานปลัดกระทรวงสาธารณสุข ได้ร่วมกับผู้เชี่ยวชาญจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทบทวนและปรับปรุงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ให้มีความชัดเจนและหน่วยงานสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรมมากยิ่งขึ้น จึงขอแจ้งเวียนแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข ฉบับที่ ๒ รายละเอียดตามสิ่งที่ส่งมาด้วย ทั้งนี้ สำนักงานปลัดกระทรวงสาธารณสุข ขอเชิญเข้าร่วมคลินิกให้คำปรึกษาข้อมูลส่วนบุคคล (PDPA Clinic) ผ่านระบบออนไลน์ Zoom ทุกวันพฤหัสบดีสุดท้ายของเดือน เวลา ๑๗.๐๐ – ๑๘.๐๐ น. โดยเริ่มวันพฤหัสบดีที่ ๓๐ มิถุนายน ๒๕๖๕ เป็นครั้งแรก

จึงเรียนมาเพื่อโปรดทราบ และแจ้งเวียนให้เจ้าหน้าที่ถือปฏิบัติโดยเคร่งครัดต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายอนันต์ กนกศิลป์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ปฏิบัติหน้าที่ผู้บริหารข้อมูลระดับสูง (CDO)
ประจำสำนักงานปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการ
โทรศัพท์ ๐ ๒๕๙๐ ๑๒๑๓, ๐ ๒๕๙๐ ๒๑๘๐ ต่อ ๑๑๒, ๓๑๖
ไปรษณีย์อิเล็กทรอนิกส์ dpo@moph.go.th

PDPA Clinic ผ่านระบบ Zoom
Meeting ID: 916 1221 3861
Passcode: 591972
https://moph.cc/ih_E1sUR5

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุข จึงได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล 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
๗. สำนักสนับสนุนระบบสุขภาพปฐมภูมิ
๘. ศูนย์สันติวิธีสาธารณสุข

๙. ศูนย์บริหารจัดการเรื่องราวร้องทุกข์ กระทรวงสาธารณสุข
๑๐. ศูนย์อำนวยการป้องกันและปราบปรามยาเสพติด กระทรวงสาธารณสุข
๑๑. สำนักส่งเสริมและสนับสนุนอาหารปลอดภัย
๑๒. สำนักบริหารยุทธศาสตร์สุขภาพดีวิถีชีวิตไทย
๑๓. สำนักโครงการพระราชดำริ โครงการเฉลิมประเกียรติและกิจกรรมพิเศษ
๑๔. กลุ่มขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติและการสร้างความสามัคคีปรองดอง ประจำกระทรวงสาธารณสุข
๑๕. วิทยาลัยนักบริหารสาธารณสุข
๑๖. สถาบันกัญชาทางการแพทย์

๓. หน่วยงานส่วนภูมิภาค

- สำนักงานเขตสุขภาพ ๑๒ เขตสุขภาพ
- ราชการบริหารส่วนภูมิภาค ๒ สำนักงาน
  ๑. สำนักงานสาธารณสุขจังหวัด ๗๖ หน่วยงาน
  ๒. สำนักงานสาธารณสุขอำเภอ ๘๗๖ หน่วยงาน
- หน่วยบริการสุขภาพ
  ๑. โรงพยาบาลศูนย์ ๓๔ แห่ง
  ๒. โรงพยาบาลทั่วไป ๙๒ แห่ง
  ๓. โรงพยาบาลชุมชน ๗๗๔ แห่ง
  ๔. โรงพยาบาลส่งเสริมสุขภาพตำบล ๙,๗๖๕ แห่ง
  ๕. สถานีอนามัย ๔๑ แห่ง

มีผลบังคับใช้กับข้าราชการ พนักงาน ผู้ปฏิบัติงาน รวมถึงบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้สำนักงานปลัดกระทรวงสาธารณสุข

ส่วนที่ ๒. ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง

๒.๑ ข้อมูลส่วนบุคคลของบุคลากรหน่วยงานของกระทรวงสาธารณสุข

เป็นข้อมูลส่วนบุคคลของ ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างประจำ ลูกจ้างชั่วคราว ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข รวมถึง ผู้มาสมัครงาน ฝึกงาน หรือทดลองปฏิบัติงานในหน่วยงานสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

๒.๒ ข้อมูลส่วนบุคคลของผู้มาติดต่องาน

เป็นข้อมูลส่วนบุคลคล ของผู้มาติดต่องาน สมัครงาน การทำธุรกรรม เช่น การขอใบอนุญาตต่าง ๆ การส่งตรวจสิ่งส่งตรวจทางห้องปฏิบัติการ เป็นต้น การทำนิติกรรม เช่น การทำสัญญาว่าจ้าง สัญญาซื้อขาย รวมถึงข้อมูลส่วนบุคคลของพนักงานหรือลูกจ้างของหน่วยงานที่ทำสัญญา หรือทำงานให้กับสำนักงานปลัดกระทรวงสาธารณสุข

๒.๓ ข้อมูลส่วนบุคคลของผู้รับบริการ

เป็นข้อมูลส่วนบุคคลของผู้มาติดต่อเพื่อรับบริการทางการแพทย์และสาธารณสุข ที่หน่วยบริการสุขภาพของสำนักงานปลัดกระทรวงสาธารณสุข รวมถึงข้อมูลส่วนบุคคลของผู้รับบริการกรณีที่บุคลากรของหน่วยบริการสุขภาพของสำนักงานปลัดกระทรวงสาธารณสุขออกไปให้บริการนอกหน่วยบริการในพื้นที่ที่รับผิดชอบ และข้อมูลการใช้บริการสุขภาพทางดิจิทัล

ส่วนที่ ๓. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

สำนักงานปลัดกระทรวงสาธารณสุขจะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" สำหรับการให้บริการตามวัตถุประสงค์ในการดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุขอย่างเคร่งครัด เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่สำนักงานปลัดกระทรวงสาธารณสุข หรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข หรือประโยชน์สาธารณะที่สำคัญอื่น ๆ เป็นต้น โดยสำนักงานปลัดกระทรวงสาธารณสุขจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และจะทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐาน ของสำนักงานปลัดกระทรวงสาธารณสุข

ส่วนที่ ๔. วัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล

๔.๑ สำนักงานปลัดกระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล เพื่อการดำเนินงานในพันธกิจต่าง ๆ ของสำนักงานปลัดกระทรวงสาธารณสุข รวมทั้งเพื่อการศึกษาวิจัยหรือ การจัดทำสถิติที่เป็นไปตามวัตถุประสงค์การดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข หรือตามที่กฎหมายกำหนด

๔.๒ สำนักงานปลัดกระทรวงสาธารณสุข จะบันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูล สำนักงานปลัดกระทรวงสาธารณสุข จะจัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน หากมีการเปลี่ยนแปลงวัตถุประสงค์ตามที่เคยได้แจ้งไว้ สำนักงานปลัดกระทรวงสาธารณสุขจะแจ้งวัตถุประสงค์ใหม่นั้นให้กับเจ้าของข้อมูลส่วนบุคคลทราบตามที่กฎหมายกำหนด

ส่วนที่ ๕. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

๕.๑ สำนักงานปลัดกระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมายเก็บรวบรวมข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่นนอกเหนือวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เว้นแต่กรณีที่กฎหมายอนุญาตให้เปลี่ยนแปลงวัตถุประสงค์การใช้ข้อมูลได้

๕.๒ สำนักงานปลัดกระทรวงสาธารณสุข จะไม่เปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยไม่มีฐานการประมวลผลข้อมูลโดยชอบด้วยกฎหมาย แต่อาจเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลภายใต้หลักเกณฑ์ที่กฎหมายกำหนด เช่นการเปิดเผยต่อหน่วยงานราชการ หน่วยงานภาครัฐ หน่วยงานที่กำกับดูแล รวมถึงในกรณีที่มีการร้องขอให้เปิดเผยข้อมูลโดยอาศัยอำนาจตามกฎหมาย

๕.๓ สำนักงานปลัดกระทรวงสาธารณสุข อาจใช้เทคโนโลยีคุกกี้ (Cookies) เพื่อเก็บรวบรวมข้อมูลพฤติกรรมของเจ้าของข้อมูลส่วนบุคคล เกี่ยวกับการเข้าถึง การใช้งาน หรือการรับบริการผ่านเว็บไซต์และแอปพลิเคชันของสำนักงานปลัดกระทรวงสาธารณสุข เพื่อประโยชน์ในการอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึง การใช้งาน หรือการรับบริการผ่านเว็บไซต์และแอปพลิเคชัน ของสำนักงานปลัดกระทรวงสาธารณสุข

ส่วนที่ ๖. การใช้และเปิดเผยข้อมูลส่วนบุคคล

หลังจากที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลแล้ว สำนักงานปลัดกระทรวงสาธารณสุข อาจมีความจำเป็นต้องใช้หรือเปิดเผยข้อมูลไปยังบุคคลอื่นที่เกี่ยวข้อง ซึ่งการใช้หรือเปิดเผยข้อมูลนั้น จะเป็นการทำเพื่อให้บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลหรือการเปิดเผยที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว หรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานอื่นใด

๖.๑ แนวปฏิบัติในการใช้หรือเปิดเผยข้อมูลภายในประเทศ

โดยปกติภารกิจของสำนักงานปลัดกระทรวงสาธารณสุข มีความเชื่อมโยงเป็นเครือข่ายในการดูแลสุขภาพของประชาชนกับหน่วยงานในสังกัดและหน่วยงานอื่น จึงมีความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลระหว่างกันเพื่อวัตถุประสงค์ในการให้บริการสุขภาพแก่ประชาชนและการดูแลป้องกันโรคและภัยสุขภาพ การเบิกจ่ายค่ารักษาพยาบาล เป็นต้น ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขได้ทำการแจ้งรายละเอียดแก่เจ้าของข้อมูลส่วนบุคคลไว้ในหนังสือแจ้งการประมวลข้อมูลส่วนบุคคลแล้วนั้น

อย่างไรก็ดีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานใดหน่วยงานหนึ่ง ไม่ว่าจะอยู่ในสังกัดหรือนอกสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ในกรณีที่การใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไม่ได้เป็นการเกี่ยวข้องกับกิจกรรมในการให้บริการด้านสุขภาพแก่เจ้าของข้อมูลส่วนบุคคลโดยตรงหรือที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว รวมถึงการรวบรวมข้อมูลจากหลายๆหน่วยงานมาจัดทำเป็นคลังข้อมูล จำเป็นต้องมีการทำข้อตกลงในการใช้หรือเปิดเผยข้อมูลเพื่อ

๑. กำกับการใช้หรือเปิดเผยข้อมูลให้เป็นไปตามหลักการที่เหมาะสม ตาม ๕.๑ และ ๕.๒

๒. กำหนดขอบเขตความรับผิดชอบและผู้รับผิดชอบ

๓. จำกัดการเข้าถึงเพียงเฉพาะบุคคลหรือแผนกที่เกี่ยวข้อง

๔. ใช้หรือเปิดเผยเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ของการใช้หรือเปิดเผยข้อมูลนั้น

๕. มีมาตรการในการรักษาความปลอดภัย ป้องกันการเข้าถึง เปลี่ยนแปลง แก้ไขข้อมูลโดยมิชอบหรืออาจถูกนำไปใช้นอกเหนือจากวัตถุประสงค์

๖. มีการตรวจสอบ ติดตามผลการปฏิบัติ อย่างสม่ำเสมอ

หน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุขที่ต้องการดำเนินการ หรือร่วมมือกับโครงการที่มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ให้แจ้งขอความเห็นชอบในการดำเนินการมายังผู้บริหารข้อมูลระดับสูง(CDO) ประจำสำนักงานปลัดกระทรวงสาธารณสุข ทั้งที่ได้ดำเนินการไปแล้วและ/หรือที่กำลังจะดำเนินการ ทั้งนี้

การให้บริการด้านสุขภาพแก่เจ้าของข้อมูลส่วนบุคคลโดยตรง ได้แก่ การปรึกษาผู้เชี่ยวชาญ การรับ-ส่งต่อผู้ป่วย ระหว่างโรงพยาบาล การส่งสิ่งส่งตรวจทางห้องปฏิบัติการ การส่งตรวจเพื่อวินิจโรคหรือการตรวจเฉพาะทาง เช่น ส่งตรวจเอ็กซเรย์ อัลตราซาวด์ การส่งอ่านภาพเอ็กซเรย์ เป็นต้น การฟื้นฟูสุขภาพ การขอสนับสนุนบริการทางการแพทย์ เช่น ขอโลหิต ขอรับบริจาคอวัยวะ ขอเบิกยาพิเศษ เป็นต้น การใช้สิทธิสวัสดิการรักษาพยาบาล การเบิกจ่ายประกันสุขภาพ

การใช้หรือเปิดเผยที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว ได้แก่ การใช้หรือเปิดเผยเพื่อการควบคุมโรคและภัยสุขภาพ พัฒนากระบวนการรักษาโรค การศึกษาของบุคลากรวิชาชีพด้านสุขภาพ หรือกระบวนการอื่นใดตามหลักวิชาชีพที่เกี่ยวข้อง

๖.๒ การโอนข้อมูลไปต่างประเทศ

สำนักงานปลัดกระทรวงสาธารณสุข จะทำการเปิดเผยข้อมูลส่วนบุคคลต่อผู้รับข้อมูลในต่างประเทศ เฉพาะกรณีที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ทำได้เท่านั้น ทั้งนี้สำนักงานปลัดกระทรวงสาธารณสุข อาจปฏิบัติตามหลักเกณฑ์การโอนข้อมูลระหว่างประเทศ โดยเข้าทำข้อสัญญามาตรฐานหรือใช้กลไกอื่นที่พึงมีตามกฎหมายว่าด้วยการคุ้มครองข้อมูลที่ใช้บังคับ และ สำนักงานปลัดกระทรวงสาธารณสุข อาจอาศัยสัญญาการโอนข้อมูล หรือกลไกอื่นที่ได้รับการอนุมัติ เพื่อการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ส่วนที่ ๗. ระยะเวลาในการจัดเก็บข้อมูล

สำนักงานปลัดกระทรวงสาธารณสุข จะเก็บรักษาข้อมูลส่วนบุคคลของไว้เป็นระยะเวลา ตราบเท่าที่วัตถุประสงค์ของการนำข้อมูลดังกล่าวไปใช้ยังคงมีอยู่ หลังจากนั้น สำนักงานปลัดกระทรวงสาธารณสุขจะลบทำลายข้อมูล หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ เว้นแต่กรณีจำเป็นต้องเก็บ รักษาข้อมูลต่อไปตามที่กฎหมายที่เกี่ยวข้องกำหนด หรือเพื่อเป็นการคุ้มครองสิทธิประโยชน์ของสำนักงานปลัดกระทรวงสาธารณสุข หรือหากมีความจำเป็นเพื่อวัตถุประสงค์อื่น ๆ เช่น เพื่อความปลอดภัย เพื่อการป้องกันการละเมิดหรือการประพฤติมิชอบ หรือเพื่อการเก็บบันทึกทางการเงิน

ส่วนที่ ๘. การรักษาความมั่นคงปลอดภัย

สำนักงานปลัดกระทรวงสาธารณสุข จะใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกัน ด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) เพื่อป้องกันการเข้าถึงและเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และสอดคล้องกับการดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข และมาตรฐานที่รับรองโดยทั่วไป เพื่อให้บรรลุตามวัตถุประสงค์ ๓ ประการ ดังนี้

๑) การธำรงไว้ซึ่งความลับ (confidentiality)

๒) ความถูกต้องครบถ้วน (integrity)

๓) สภาพพร้อมใช้งาน (availability)

ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ประกอบด้วยการดำเนินการตามมาตรการดังต่อไปนี้

ข้อ ๑. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

๑.๑ มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออกมีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง

ทั้งนี้ ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๑.๒ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

ข้อ ๒. มาตรการป้องกันด้านเทคนิค (technical safeguard)

๒.๑ การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

ข้อ ๓. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๓.๑ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๓.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

โดยสำนักงานปลัดกระทรวงสาธารณสุข กำหนดให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุขเข้ารับการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของข้อมูล

การจัดจ้างผู้ให้บริการภายนอก สำนักงานปลัดกระทรวงสาธารณสุขจะมีการสอบทานและปรับปรุงมาตรการต่าง ๆ เพื่อให้แน่ใจว่า ผู้ให้บริการภายนอกที่ สำนักงานปลัดกระทรวงสาธารณสุขทำการว่าจ้างจะมีการใช้มาตรการในการ เก็บรวบรวม ประมวลผล โอนย้าย จัดการ และรักษาความมั่นคงปลอดภัย ของข้อมูลอย่างเพียงพอในการให้บริการภายใต้วัตถุประสงค์ของสำนักงานปลัดกระทรวงสาธารณสุขเป็นไปตามมาตรฐานต่าง ๆ ของประเทศ และกฎระเบียบที่เกี่ยวข้อง

สำนักงานปลัดกระทรวงสาธารณสุข จัดทำนโยบาย แนวปฏิบัติและขั้นตอนวิธีการต่าง ๆ เพื่อการจัดการข้อมูลอย่างปลอดภัย และป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาตโดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- กำหนดนโยบายและขั้นตอนวิธีการต่าง ๆ เพื่อจัดการข้อมูลอย่างปลอดภัย และอาจกำหนดเพิ่มเติมในสัญญาระหว่างสำนักงานปลัดกระทรวงสาธารณสุขกับคู่สัญญาแต่ละราย
- มีการบริหารจัดการสิทธิของพนักงานและลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคล อย่างเหมาะสม
- ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูล การตรวจสอบตัวตนและเทคโนโลยีการตรวจจับไวรัส ตามความจำเป็น รวมถึงจัดให้มีช่องทางการสื่อสารแบบปลอดภัยสำหรับข้อมูลดังกล่าวด้วยการเข้ารหัสลับข้อมูลดังกล่าว เช่น จัดให้มีการใช้ Secure Socket Layer (SSL) protocol เป็นต้น
- บริหารจัดการให้ ผู้ให้บริการภายนอกที่สำนักงานปลัดกระทรวงสาธารณสุขทำการว่าจ้างต้องปฏิบัติตามหลักเกณฑ์ ตามกฎหมาย และระเบียบต่าง ๆ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

• มีติดตามตรวจสอบเว็บไซต์และระบบออนไลน์ ของสำนักงานปลัดกระทรวงสาธารณสุข ผ่านหน่วยงาน ที่มีความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย

• จัดให้มีการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุข

• ประเมินผลแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การจัดการข้อมูล และการรักษาความมั่นคงปลอดภัยของข้อมูลของสำนักงานปลัดกระทรวงสาธารณสุข เป็นประจำ

ส่วนที่ ๙. การลบหรือทำลายข้อมูลส่วนบุคคล

สำนักงานปลัดกระทรวงสาธารณสุข จะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอหรือเจ้าของข้อมูลส่วนบุคคลได้เพิกถอนความยินยอมในกรณีที่มีการขอความยินยอมไว้ เว้นแต่การเก็บรักษาข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนดซึ่งโดยปกติสำนักงานปลัดกระทรวงสาธารณสุขไม่ได้ใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ส่วนที่ ๑๐.การมีส่วนร่วมของเจ้าของข้อมูล

สำนักงานปลัดกระทรวงสาธารณสุข จะเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรงเท่านั้น และต้อง “ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือระหว่างเก็บรวบรวมข้อมูลส่วนบุคคล” เว้นแต่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด หากสำนักงานปลัดกระทรวงสาธารณสุข จำเป็นต้อง “เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น” ที่ไม่ใช่เก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรง สำนักงานปลัดกระทรวงสาธารณสุข จะแจ้งเหตุผลความจำเป็นนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบ และขอความยินยอมในเวลาตามที่กำหนด เว้นแต่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

ส่วนที่ ๑๑.สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการ กับข้อมูลส่วนบุคคลของตนเอง ที่สำนักงานปลัดกระทรวงสาธารณสุขดูแล ดังต่อไปนี้

๑๑.๑ สิทธิในการขอรับข้อมูลส่วนบุคคลของตนเอง โดยเจ้าของข้อมูลมีสิทธิ ที่จะขอรับสำเนาข้อมูลส่วนบุคคลของตน และมีสิทธิที่จะร้องขอให้ เปิดเผยถึงการได้มาซึ่งข้อมูลของเจ้าของข้อมูล

๑๑.๒ สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

๑๑.๓ สิทธิขอให้ลบหรือทำลายข้อมูล โดยขอให้ สำนักงานปลัดงกระทรวงสาธารณสุข ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูล ส่วนบุคคลได้ด้วยเหตุบางประการได้ตามที่กฎหมายกำหนด

๑๑.๔ สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลโดยขอให้สำนักงานปลัดกระทรวงสาธารณสุขระงับการใช้ข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

๑๑.๕ สิทธิขอให้แก้ไขเปลี่ยนแปลง โดยขอให้ สำนักงานปลัดงกระทรวงสาธารณสุข ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ส่วนที่ ๑๒. การจ้างการประมวลผลหรือมอบหมายให้ประมวลผล

สำนักงานปลัดกระทรวงสาธารณสุขได้กำหนดแนวทางปฏิบัติในการทำสัญญาจ้างการประมวลผลข้อมูลส่วนบุคคล หรือมอบหมายให้ผู้อื่นประมวลผลข้อมูลส่วนบุคคลดังนี้

๑๒.๑ ก่อนทำการจ้างหรือมอบหมายผู้ประมวลผลข้อมูล ต้องประเมินระบบ สอบทานและปรับปรุงมาตรการต่างๆในการคุ้มครองข้อมูลส่วนบุคคลของผู้รับจ้างหรือผู้ถูกมอบหมาย เพื่อให้แน่ใจว่าระบบการรักษาความมั่นคงปลอดภัยข้อมูลมีความเหมาะสม เพียงพอ รวมถึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในส่วนของผู้รับจ้างหรือผู้รับมอบหมาย

๑๒.๒ ในสัญญาจ้างหรือข้อตกลงการประมวลผล ต้องระบุวัตถุประสงค์ วิธีการเก็บข้อมูล การแจ้งเจ้าของข้อมูลส่วนบุคคล การใช้ การส่งและโอนข้อมูล และการกำจัดข้อมูล

๑๒.๓ คู่สัญญาต้องลงนามในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามที่สำนักงานปลัดกระทรวงสาธารณสุขกำหนด

๑๒.๔ เมื่อมีการจ้างหรือมอบหมายให้มีการประมวลผลข้อมูล ต้องทำการควบคุมการประมวลผลและควบคุมการปฏิบัติให้เป็นไปตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานปลัดกระทรวงกำหนด

๑๒.๕ เมื่อครบกำหนดการเก็บรักษาข้อมูล ต้องควบคุมให้ผู้รับประมวลผลทำลายข้อมูลตามกำหนด

ส่วนที่ ๑๓. การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้

สำนักงานปลัดกระทรวงสาธารณสุข กำหนดให้ทุกหน่วยงานภายใต้สังกัด ดำเนินการตรวจสอบแยกแยะ ข้อมูลส่วนบุคคล ที่ถูกเก็บรวมรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้ ว่ายังเป็นข้อมูลส่วนบุคคลที่ยังมีความจำเป็นต้องเก็บไว้หรือไม่ หากหมดความจำเป็นที่จะต้องเก็บรักษาไว้ ก็ให้ดำเนินการลบทำลาย

ส่วนข้อมูลที่ยังมีความจำเป็นต้องเก็บรักษาไว้เพื่อใช้งานต่อไป ให้พิจารณาว่า เป็นข้อมูลที่ต้องขอความยินยอมก่อนการรวบรวมหรือไม่ (รายละเอียดในการพิจารณาขอให้ศึกษาในคู่มือปฏิบัติของข้อมูลส่วนบุคคลแต่ละประเภท) หากต้องขอความยินยอมให้ประสานงานกับเจ้าของข้อมูลและถ้าเจ้าของข้อมูลส่วนบุคคลไม่ประสงค์ ให้สำนักงานปลัดกระทรวงสาธารณสุขเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ดังกล่าว ก็ให้ดำเนินการยกเลิกความยินยอมได้ตามประสงค์

ส่วนที่ ๑๔. แนวทางการดำเนินการลบทำลายข้อมูลส่วนบุคคล

ให้หน่วยงานที่มีความประสงค์จะลบทำลายข้อมูลรวบรวมบัญชีข้อมูลส่วนบุคคลที่เกี่ยวข้องเสนอขอความเห็นชอบมาที่สำนักปลัดกระทรวงสาธารณสุข โดยเสนอผ่านเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อนำเข้าสู่กระบวนการพิจารณาให้ความเห็นชอบ

ส่วนที่ ๑๕. แนวทางการปฏิบัติเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล

เหตุละเมิดข้อมูลส่วนบุคคล หมายถึง การที่ข้อมูลส่วนบุคคลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผยหรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น ไม่ว่าจะเกิดจากการทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

ในกรณีที่มีเหตุละเมิดข้อมูลส่วนบุคคลเกิดขึ้นภายในหน่วยงาน ผู้ที่ทราบเหตุจะต้องแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการละเมิดข้อมูลส่วนบุคคลส่วนบุคคล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลส่วนบุคคลและ/หรือ สำนักงานคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า รวมทั้งออกมาตรการเยียวยาเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกเหตุการณ์การการละเมิดข้อมูลส่วนบุคคลและประเมินความเสี่ยง เมื่อเกิดการละเมิดข้อมูลส่วนบุคคลขึ้นในการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคลนั้น อาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ถ้าหากพิจารณาแล้วว่า ไม่ได้มีผลกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลหรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การละเมิดที่เกิดขึ้น แต่หากผลการประเมินแสดงให้เห็นว่าการละเมิดข้อมูลอาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งแนวทางในการเยียวยา อีกทั้งแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา ๗๒ ชั่วโมง นับจากทราบเหตุการณ์การละเมิดข้อมูลส่วนบุคคล

หน่วยงานควรมีการจัดทำแบบฟอร์มบันทึกการละเมิดข้อมูลส่วนบุคคลขึ้น เพื่อเป็นแนวทางในการจดบันทึกอย่างถูกต้องและครบถ้วน สำหรับหน้าที่ในการจดบันทึกควรกำหนดให้เป็นหน้าที่ของเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคลหรืออาจให้พนักงานผู้พบเหตุการณ์เป็นผู้ทำการบันทึกแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้แล้วแต่กรณี และแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การละเมิดข้อมูลที่เกิดขึ้นโดยเร็ว เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการหาสาเหตุและมาตรการเยียวยา รวมถึงติดตามผลการดำเนินการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล โดยมีรายละเอียดการบันทึกหลักๆดังนี้

- วันเวลา ข้อมูล ที่บ่งชี้ถึงเหตุการณ์ละเมิดข้อมูลที่ทราบ
- ประเมินจำนวนรายการของข้อมูลที่ถูกละเมิด/รั่วไหลหรือจำนวนของผู้ที่คาดว่าจะได้รับผลกระทบ
- ระบุประเภทของข้อมูลที่รั่วไหลเช่น ชื่อนามสกุล หมายเลขโทรศัพท์ อีเมล ข้อมูลด้านการเงิน อื่นๆ
- ระบุแนวทางการแก้ไขปัญหา หรือเยียวยาผู้ที่ได้รับผลกระทบ
- ระบุช่องทางการติดต่อ ผู้ที่รับผิดชอบเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑๖. การขอความยินยอมและการถอนความยินยอม

การใช้ฐานความยินยอมในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นฐานในการประมวลผลที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะจัดการกับข้อมูลส่วนบุคคลของตนเองได้อย่างเต็มที่ ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ยกเว้น กรณีการประมวลผลข้อมูลส่วนบุคคล ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

ภารกิจโดยส่วนใหญ่เกือบทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข เป็นการดำเนินการโดยใช้ฐานอำนาจตามกฎหมาย เนื่องจากมีความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่สำนักงานปลัดกระทรวงสาธารณสุข หรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข หรือประโยชน์สาธารณะที่สำคัญอื่น ๆ เป็นต้น และไม่ต้องขอความยินยอม

๑๖.๑ การเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องขอความยินยอม ให้หน่วยงานที่ต้องการดำเนินการดังกล่าวประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ก่อนเริ่มดำเนินการเพื่อพิจารณาให้ความเห็นชอบแนวทางปฏิบัติทั้งการขอความยินยอมและการถอนความยินยอม เว้นแต่เป็นการดำเนินการตามที่คู่มือปฏิบัติได้กำหนดไว้

๑๖.๒ หน่วยงานควรเลือกใช้ฐานในการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเนื่องจากฐานความยินยอมไม่สามารถใช้ได้ทุกกรณี เว้นแต่กรณีที่ต้องขอความยินยอม ตามข้อกำหนดของกฎหมายอื่น ฐานความยินยอมจะเหมาะสมเมื่อการประมวลผลข้อมูลไม่ได้มีความจำเป็นตามเงื่อนไขสัญญา นอกจากนั้นการให้ความยินยอมจะต้องเป็นสิ่งที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกได้ว่าจะให้หรือปฏิเสธก็ได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา การขอความยินยอมจะต้องอาศัยหลักการกระทำโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness, and Transparency) โดยหน่วยงานจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์และจะต้องคำนึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการตัดสินใจให้ความยินยอม โดยการให้ความยินยอมจะต้องเป็นการสมัครใจ ดังนั้นการขอความยินยอมจะต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด

๑๖.๓ เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผย ข้อมูลนั้นๆได้
- เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้
- การใช้ฐานความยินยอมนั้นจะต้องให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้ความยินยอมได้
- การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้นหน่วยงานจึงควรออกแบบแบบฟอร์มการขอความยินยอม ที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเห็นได้อย่างชัดเจนว่า หน่วยงานขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง
- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคลในการ ให้ความยินยอม ทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms& Conditions) หรือข้อความในสัญญา
- การขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

๑๖.๔ หน่วยงาน ต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกันต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาก็ควรระบุอยู่ในสัญญา ซึ่งการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) เนื่องจากการกระทำดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดว่าหากไม่ให้ความยินยอมล้วจะไม่ได้รับบริการหรือมีผลต่อการใช้ผลิตภัณฑ์หรือบริการของหน่วยงาน

๑๖.๕ การใช้ฐานความยินยอมอาจเหมาะสมในสถานการณ์ที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เฉพาะเจาะจงมากกว่า และหน่วยงานไม่สามารถประมวลผลข้อมูลตามวัตถุประสงค์ที่เพิ่มเติมขึ้นมาใหม่เองได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หน่วยงานจะต้องขอความยินยอมใหม่หากต้องการประมวลผลข้อมูลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว เว้นแต่หากพิจารณาแล้วว่าการประมวลผลเพื่อวัตถุประสงค์นั้นสามารถทำได้ภายใต้ฐานกฎหมายฐานอื่น

๑๖.๖ การขอความยินยอมสามารถทำได้หลายวิธีเช่น

- การยินยอมจากการเลือกยินยอม (Opt-in Consent) ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจนเป็นลายลักษณ์อักษร หน่วยงานควรออกแบบให้เจ้าของข้อมูลส่วนบุคคลต้องมีการกระทำให้ความยินยอมอย่างชัดเจน (Clear Affirmative Action) เช่น การทำเป็นช่องเช็คถูก (CheckBox) โดยให้เจ้าของข้อมูลส่วนบุคคล กด/เขียน/เช็คเองได้ (Signatures or Ticks Indicating Consent)

● การขอความยินยอมในรูปแบบวาจา (Verbal Consent) สำหรับรูปแบบการขอความยินยอมนี้ ใช้ในกรณีที่มีการบันทึกความยินยอมในรูปแบบเสียง (Voice Record) ด้วยระบบดิจิทัล เช่น บันทึกผ่านการติดต่อกับเจ้าของข้อมูลส่วนบุคคลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลส่วนบุคคลกดปุ่มยืนยันการให้ความยินยอม เป็นต้น ซึ่งหน่วยงานจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลส่วนบุคคลจริง นอกจากนั้นหน่วยงานควรให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคล อย่างเพียงพอต่อการตัดสินใจมีทางเลือกและเนื้อหาชัดเจนไม่ก่อให้เกิดความ เข้าใจผิด และให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมหรือไม่ให้ความยินยอมก็ได้โดยสมัครใจไม่เป็นการบังคับ

๑๖.๗ การถอนความยินยอม (Withdraw of Consent)

ในกรณีที่ท่านได้ให้ความยินยอมไว้ ท่านมีสิทธิที่จะขอเพิกถอนความยินยอม ที่ให้ไว้กับหน่วยงานในการเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และหน่วยงานจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้

หากหน่วยงานไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวมใช้หรือเปิดเผยต่อไป ให้หน่วยงานดำเนินการลบข้อมูลออก

การใช้สิทธิถอนความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

ส่วนที่ ๑๗. การตรวจสอบและปรับปรุงระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

สำนักงานปลัดกระทรวงสาธารณสุข มอบหมายให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และผู้ประสานงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในสังกัด ตรวจสอบระบบการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามนโยบาย แนวปฏิบัติ และคู่มือการปฏิบัติ รายงานให้ผู้บริหารทราบ และทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล โดยบุคลากรที่มีส่วนเกี่ยวข้องสามารถเสนอการปรับปรุงแก้ไขคู่มือ ประกาศ ข้อกำหนด หรือ แบบฟอร์มต่างๆ เพื่อให้ระบบบริหารจัดการมีประสิทธิภาพมากขึ้นโดยเสนอต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อดำเนินการต่อไป

ส่วนที่ ๑๘. การพัฒนาบุคคลากรผู้ที่มีส่วนเกี่ยวข้อง

เพื่อให้บุคลากรทุกคนของสำนักงานปลัดกระทรวงสาธารณสุขได้รับข้อมูลความรู้ และความเข้าใจที่เพียงพอ สำนักงานปลัดกระทรวงสาธารณสุขจะดำเนินการตามที่จำเป็นเพื่อให้บุคลากรได้รับทราบและตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคล

บุคลากรที่มีหน้าที่เกี่ยวข้องกับการประมวลผลข้อมูล จะต้องได้รับการอบรม เพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลส่วนบุคคลตามที่สำนักงานปลัดกระทรวงสาธารณสุขกำหนด

ส่วนที่ ๑๙. การควบคุมเอกสาร

สำนักงานปลัดกระทรวงสาธารณสุข มีการควบคุมเอกสาร แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและคู่มือปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล เอกสารที่เกี่ยวข้อง เพื่อให้ทุกหน่วยงานในสังกัดถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและมีประสิทธิภาพ

ส่วนที่ ๒๐. การปรับปรุงทบทวนหรือแก้ไขคู่มือปฏิบัติ

สำนักงานปลัดกระทรวงสาธารณสุข อาจดำเนินการปรับปรุง ทบทวน หรือ แก้ไข คู่มือปฏิบัติฉบับนี้ ไม่ว่าบางส่วนหรือทั้งหมด หรือเป็นครั้งคราว เพื่อให้สอดคล้องกับนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุข กฎหมาย กฎเกณฑ์ของหน่วยงานทางราชการที่มีอำนาจ

ส่วนที่ ๒๑. กฎหมายที่ใช้บังคับและเขตอำนาจศาล

นโยบาย และแนวปฏิบัติตามคู่มือการคุ้มครองข้อมูลส่วนบุคคลนี้อยู่ภายใต้การบังคับและตีความตามกฎหมายไทย และให้ศาลไทยเป็นผู้มีอำนาจในการพิจารณาข้อพิพาทใดที่อาจเกิดขึ้น

ส่วนที่ ๒๒. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติและนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

๒๒.๑ สำนักงานปลัดกระทรวงสาธารณสุข มีการดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กระทรวงสาธารณสุข โดยจะเผยแพร่ผ่านทางเว็บไซต์ https://pdpa.moph.go.th รวมทั้งหากมีการปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็จะดำเนินการเผยแพร่ผ่านช่องทางดังกล่าว รวมทั้งผ่านสื่อที่ กระทรวงสาธารณสุขใช้เพื่อการประชาสัมพันธ์ตามความเหมาะสมด้วย

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

ส่วนที่ ๒๓. แนวทางการคุ้มครองข้อมูลส่วนบุคคล

สำนักงานปลัดกระทรวงสาธารณสุข ได้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อการประสานงานในการคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลและสิทธิประโยชน์ของสำนักงานปลัดกระทรวงสาธารณสุข ช่วยให้สามารถบริหารความเสี่ยงและจัดการข้อมูลส่วนบุคคล ได้อย่างมีประสิทธิภาพและประสิทธิผล ในกรณีที่เจ้าของข้อมูลต้องการใช้สิทธิ หรือมีคำถามเกี่ยวกับการใช้ สิทธิของตน หรือความยินยอมที่เจ้าของข้อมูลได้ให้ไว้ สามารถติดต่อได้ที่

ส่งถึง : เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข
อาคาร ๒ ชั้น ๑ เลขที่ ๘๘/๒๐ หมู่ ๔ ถนนติวานนท์
ตำบลตลาดขวัญ อำเภอเมือง จังหวัดนนทบุรี ๑๑๐๐๐
อีเมล : dpo@moph.go.th
โทรศัพท์ ๐ ๒๕๙๐ ๑๒๑๓ ,๐ ๒๕๙๐ ๒๑๘๐ ต่อ ๑๑๒,๓๑๖

สำนักงานปลัดกระทรวงสาธารณสุข