

**แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

        สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กระทรวงสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุข จึงได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ไว้ดังต่อไปนี้

**ส่วนที่ ๑. ผู้มีหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล**

หน่วยงานภายใต้สำนักงานปลัดกระทรวงสาธารณสุขซึ่งประกอบ หน่วยงานในส่วนกลางและส่วนภูมิภาค ดังนี้

**๑. ราชการบริหารส่วนกลาง ๑๕ หน่วยงาน**

1. กองการพยาบาล
2. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
3. กองยุทธศาสตร์และแผนงาน
4. กองตรวจราชการ
5. กองบริหารการสาธารณสุข
6. กองกลาง
7. กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ
8. กองบริหารการคลัง
9. กองบริหารทรัพยากรบุคคล
10. กองการต่างประเทศ
11. กองกฎหมาย
12. กองสาธารณสุขฉุกเฉิน
13. ศูนย์ปฏิบัติการต่อต้านการทุจริต
14. กลุ่มพัฒนาระบบบริหาร
15. กลุ่มตรวจสอบภายใน

**๒. หน่วยงานตามภารกิจเฉพาะ ๑๖ หน่วยงาน**

1. สำนักตรวจราชการ กระทรวงสาธารณสุข
2. สำนักวิชาการสาธารณสุข
3. สำนักงานรัฐมนตรี
4. กลุ่มเสริมสร้างวินัยและระบบคุณธรรม
5. สำนักสารนิเทศ
6. สำนักงานบริหารโครงการร่วมผลิตแพทย์เพิ่มเพื่อชาวชนบท
7. สำนักสนับสนุนระบบสุขภาพปฐมภูมิ
8. ศูนย์สันติวิธีสาธารณสุข
9. ศูนย์บริหารจัดการเรื่องราวร้องทุกข์ กระทรวงสาธารณสุข
10. ศูนย์อำนวยการป้องกันและปราบปรามยาเสพติด กระทรวงสาธารณสุข
11. สำนักส่งเสริมและสนับสนุนอาหารปลอดภัย
12. สำนักบริหารยุทธศาสตร์สุขภาพดีวิถีชีวิตไทย
13. สำนักโครงการพระราชดำริ โครงการเฉลิมประเกียรติและกิจกรรมพิเศษ
14. กลุ่มขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติและการสร้างความสามัคคีปรองดอง ประจำกระทรวงสาธารณสุข
15. วิทยาลัยนักบริหารสาธารณสุข
16. สถาบันกัญชาทางการแพทย์

**๓. หน่วยงานส่วนภูมิภาค**

* สำนักงานเขตสุขภาพ ๑๒ เขตสุขภาพ
* ราชการบริหารส่วนภูมิภาค ๒ สำนักงาน

๑. สำนักงานสาธารณสุขจังหวัด ๗๖ หน่วยงาน

๒. สำนักงานสาธารณสุขอำเภอ ๘๗๖ หน่วยงาน

* หน่วยบริการสุขภาพ
1. โรงพยาบาลศูนย์ ๓๔ แห่ง
2. โรงพยาบาลทั่วไป ๙๒ แห่ง
3. โรงพยาบาลชุมชน ๗๗๔ แห่ง
4. โรงพยาบาลส่งเสริมสุขภาพตำบล ๙,๗๖๕ แห่ง
5. 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 หรือทำงานให้กับสำนักงานปลัด กระทรวงสาธารณสุข

 **๒.๓ ข้อมูลส่วนบุคคลของผู้รับบริการ**

 เป็นข้อมูลส่วนบุคคลของผู้มาติดต่อเพื่อรับบริการทางการแพทย์และสาธารณสุข ที่หน่วยบริการสุขภาพ ของสำนักงานปลัดกระทรวงสาธารณสุข รวมถึงข้อมูลส่วนบุคคลของผู้รับบริการกรณีที่บุคลากรของหน่วยบริการสุขภาพของสำนักงานปลัดกระทรวงสาธารณสุขออกไปให้บริการนอกหน่วยบริการในพื้นที่ที่รับผิดชอบ และข้อมูลการใช้บริการสุขภาพทางดิจิทัล

**ส่วนที่ ๓. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด**

            สำนักงานปลัดกระทรวงสาธารณสุขจะเก็บรวบรวมข้อมูลส่วนบุคคล “เท่าที่จำเป็น” สำหรับการให้บริการตามวัตถุประสงค์ในการดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุขอย่างเคร่งครัด เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่สำนักงานปลัดกระทรวงสาธารณสุข หรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะ ด้านการสาธารณสุข หรือประโยชน์สาธารณะที่สำคัญอื่น ๆ เป็นต้น โดยสำนักงานปลัดกระทรวงสาธารณสุข จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และจะทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย ที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐาน ของสำนักงานปลัดกระทรวงสาธารณสุข

**ส่วนที่ ๔. วัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล**

        ๔.๑  สำนักงานปลัดกระทรวงสาธารณสุข จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ของเจ้าของข้อมูลส่วนบุคคล เพื่อการดำเนินงานในพันธกิจต่าง ๆ ของสำนักงานปลัดกระทรวงสาธารณสุข รวมทั้งเพื่อการศึกษาวิจัยหรือ การจัดทำสถิติที่เป็นไปตามวัตถุประสงค์การดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข หรือตามที่กฎหมายกำหนด

            ๔.๒  สำนักงานปลัดกระทรวงสาธารณสุข จะบันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูล สำนักงานปลัดกระทรวงสาธารณสุข จะจัดทำบันทึกแก้ไขเพิ่มเติม ไว้เป็นหลักฐาน หากมีการเปลี่ยนแปลงวัตถุประสงค์ตามที่เคยได้แจ้งไว้ สำนักงานปลัดกระทรวงสาธารณสุข จะแจ้งวัตถุประสงค์ใหม่นั้นให้กับเจ้าของข้อมูลส่วนบุคคลทราบตามที่กฎหมายกำหนด

**ส่วนที่ ๕. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล**

            ๕.๑  สำนักงานปลัดกระทรวงสาธารณสุข จะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมาย เก็บรวบรวมข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เว้นแต่กรณีที่กฎหมายอนุญาต ให้เปลี่ยนแปลงวัตถุประสงค์การใช้ข้อมูลได้

            ๕.๒  สำนักงานปลัดกระทรวงสาธารณสุข จะไม่เปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยไม่มีฐานการประมวลผลข้อมูลโดยชอบด้วยกฎหมาย แต่อาจเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล ภายใต้หลักเกณฑ์ที่กฎหมายกำหนด เช่นการเปิดเผยต่อหน่วยงานราชการ หน่วยงานภาครัฐ หน่วยงาน ที่กำกับดูแล รวมถึงในกรณีที่มีการร้องขอให้เปิดเผยข้อมูลโดยอาศัยอำนาจตามกฎหมาย

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

๕.๔ สำนักงานปลัดกระทรวงสาธารณสุข อาจทำการเก็บข้อมูลส่วนบุคคลไว้ในระบบประมวลผล แบบคลาวด์ (Cloud Computing) โดยใช้บริการจากบุคคลที่สามไม่ว่าตั้งอยู่ในประเทศไทยหรือต่างประเทศ หรือ ผู้ให้บริการเซิร์ฟเวอร์ สำหรับเว็บไซต์ การวิเคราะห์ข้อมูล การประมวลผลการจ่ายและรับชำระเงิน การทำคำสั่งซื้อ การให้บริการโครงสร้างพื้นฐานเกี่ยวกับเทคโนโลยีสารสนเทศ เป็นต้น

ในกรณีที่สำนักงานปลัดกระทรวงสาธารณสุข จำเป็นต้องส่งข้อมูลส่วนบุคคลให้แก่บุคคลภายนอก สำนักงานปลัดกระทรวงสาธารณสุขจะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อให้มั่นใจว่า บุคคลภายนอกจะดูแลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ไม่ให้เกิด การสูญหาย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้ การดัดแปลง การเปิดเผย หรือการใช้งานที่ไม่ถูกต้อง

**ส่วนที่ ๖. การใช้และเปิดเผยข้อมูลส่วนบุคคล**

หลังจากที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลแล้ว สำนักงานปลัด กระทรวงสาธารณสุข อาจมีความจำเป็นต้องใช้หรือเปิดเผยข้อมูลไปยังบุคคลอื่นที่เกี่ยวข้อง ซึ่งการใช้หรือเปิดเผยข้อมูลนั้น จะเป็นการทำเพื่อให้บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลหรือการเปิดเผยที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว หรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานอื่นใด

 **๖.๑ แนวปฏิบัติในการใช้หรือเปิดเผยข้อมูลภายในประเทศ**

 โดยปกติภารกิจของสำนักงานปลัดกระทรวงสาธารณสุข มีความเชื่อมโยงเป็นเครือข่าย ในการดูแลสุขภาพของประชาชนกับหน่วยงานในสังกัดและหน่วยงานอื่น จึงมีความจำเป็นในการเปิดเผย ข้อมูลส่วนบุคคลระหว่างกันเพื่อวัตถุประสงค์ในการให้บริการสุขภาพแก่ประชาชนและการดูแลป้องกัน โรคและภัยสุขภาพ การเบิกจ่ายค่ารักษาพยาบาล เป็นต้น ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขได้ทำการแจ้งรายละเอียดแก่เจ้าของข้อมูลส่วนบุคคลไว้ในหนังสือแจ้งการประมวลข้อมูลส่วนบุคคลแล้วนั้น

 อย่างไรก็ดีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานใดหน่วยงานหนึ่ง ไม่ว่าจะอยู่ ในสังกัดหรือนอกสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ในกรณีที่การใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไม่ได้เป็นการเกี่ยวข้องกับกิจกรรมในการให้บริการด้านสุขภาพแก่เจ้าของข้อมูลส่วนบุคคลโดยตรงหรือ ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว รวมถึงการรวบรวมข้อมูลจากหลายๆหน่วยงานมาจัดทำเป็นคลังข้อมูล จำเป็นต้องมีการทำข้อตกลงในการใช้หรือเปิดเผยข้อมูลเพื่อ

1. กำกับการใช้หรือเปิดเผยข้อมูลให้เป็นไปตามหลักการที่เหมาะสม ตาม ๕.๑ และ ๕.๒
2. กำหนดขอบเขตความรับผิดชอบและผู้รับผิดชอบ
3. จำกัดการเข้าถึงเพียงเฉพาะบุคคลหรือแผนกที่เกี่ยวข้อง
4. ใช้หรือเปิดเผยเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ของการใช้หรือเปิดเผยข้อมูลนั้น
5. มีมาตรการในการรักษาความปลอดภัย ป้องกันการเข้าถึง เปลี่ยนแปลง แก้ไขข้อมูลโดยมิชอบ หรืออาจถูกนำไปใช้นอกเหนือจากวัตถุประสงค์
6. มีการตรวจสอบ ติดตามผลการปฏิบัติ อย่างสม่ำเสมอ

 หน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุขที่ต้องการดำเนินการ หรือร่วมมือกับโครงการที่มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ให้แจ้งขอความเห็นชอบในการดำเนินการมายังผู้บริหารข้อมูลระดับสูง(CDO) ประจำสำนักงานปลัดกระทรวงสาธารณสุข ทั้งที่ได้ดำเนินการไปแล้วและ/หรือที่กำลังจะดำเนินการ ทั้งนี้

 การให้บริการด้านสุขภาพแก่เจ้าของข้อมูลส่วนบุคคลโดยตรง ได้แก่ การปรึกษาผู้เชี่ยวชาญ การรับ-ส่งต่อผู้ป่วย ระหว่างโรงพยาบาล การส่งสิ่งส่งตรวจทางห้องปฏิบัติการ การส่งตรวจเพื่อวินิจโรคหรือการตรวจ เฉพาะทาง 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. ข้อมูลที่เกี่ยวกับบุคคลภายนอก**

 หากเจ้าของข้อมูลให้ข้อมูลส่วนบุคคลของบุคคลอื่นใด นอกเหนือจากตนเอง เช่น คู่สมรส บุตร บิดา มารดา บุคคลในครอบครัว ผู้รับผลประโยชน์ บุคคลที่สามารถติดต่อได้ในกรณีฉุกเฉิน บุคคลอ้างอิง หรือบุคคลอื่นที่เกี่ยวข้อง สำนักงานปลัดกระทรวงสาธารณสุขจะถือว่าเจ้าของข้อมูลรับรองว่าตนเอง มีอำนาจที่จะให้ข้อมูลส่วนบุคคลของบุคคลดังกล่าว และมีหน้าที่แจ้งให้บุคคลดังกล่าวทราบและอนุญาตให้สำนักงานปลัดกระทรวงสาธารณสุข ใช้ข้อมูลส่วนบุคคล ตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ได้

**ส่วนที่ 8.ระยะเวลาในการจัดเก็บข้อมูล**

สำนักงานปลัดกระทรวงสาธารณสุข จะเก็บรักษาข้อมูลส่วนบุคคลของไว้เป็นระยะเวลา ตราบเท่าที่วัตถุประสงค์ของการนำข้อมูลดังกล่าวไปใช้ยังคงมีอยู่ หลังจากนั้น สำนักงานปลัดกระทรวงสาธารณสุขจะลบ ทำลายข้อมูล หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ เว้นแต่กรณีจำเป็นต้องเก็บ รักษาข้อมูลต่อไปตามที่กฎหมายที่เกี่ยวข้องกำหนด หรือเพื่อเป็นการคุ้มครองสิทธิประโยชน์ของสำนักงานปลัดกระทรวงสาธารณสุข หรือหากมีความจำเป็นเพื่อวัตถุประสงค์อื่น ๆ เช่น เพื่อความปลอดภัย เพื่อการป้องกันการละเมิดหรือ การประพฤติมิชอบ หรือเพื่อการเก็บบันทึกทางการเงิน

**ส่วนที่ 9. การรักษาความมั่นคงปลอดภัย**

            สำนักงานปลัดกระทรวงสาธารณสุข จะใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกัน ด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุม การใช้งานข้อมูลส่วนบุคคล (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 หรือเปิดเผย ข้อมูลส่วนบุคคลโดยมิชอบ ประกอบด้วยการดำเนินการตามมาตรการดังต่อไปนี้

1. **มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)**
	1. มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออกมีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง

ทั้งนี้ ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

* 1. มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย
1. **มาตรการป้องกันด้านเทคนิค (technical safeguard)**
	1. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
	2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุม การเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย
	3. จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง
2. **มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)**
	1. มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ
	2. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

โดยสำนักงานปลัดกระทรวงสาธารณสุข กำหนดให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุขเข้ารับการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของข้อมูล

 การจัดจ้างผู้ให้บริการภายนอก สำนักงานปลัดกระทรวงสาธารณสุขจะมีการสอบทาน และปรับปรุงมาตรการต่าง ๆ เพื่อให้แน่ใจว่า ผู้ให้บริการภายนอกที่ สำนักงานปลัดกระทรวงสาธารณสุข ทำการว่าจ้างจะมีการใช้มาตรการในการ เก็บรวบรวม ประมวลผล โอนย้าย จัดการ และรักษาความมั่นคงปลอดภัย ของข้อมูลอย่างเพียงพอในการให้บริการภายใต้วัตถุประสงค์ของสำนักงานปลัดกระทรวงสาธารณสุข เป็นไปตามมาตรฐานต่าง 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 ผู้ให้บริการภายนอกที่สำนักงานปลัดกระทรวงสาธารณสุขทำการว่าจ้าง ต้องปฏิบัติตามหลักเกณฑ์ ตามกฎหมาย และระเบียบต่าง ๆ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
* มีติดตามตรวจสอบเว็บไซต์และระบบออนไลน์ ของสำนักงานปลัดกระทรวงสาธารณสุข ผ่านหน่วยงาน ที่มีความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย
* จัดให้มีการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุข
* ประเมินผลแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การจัดการข้อมูล และการรักษาความมั่นคงปลอดภัยของข้อมูลของสำนักงานปลัดกระทรวงสาธารณสุข เป็นประจำ

**ส่วนที่ 10. การลบหรือทำลายข้อมูลส่วนบุคคล**

 สำนักงานปลัดกระทรวงสาธารณสุข จะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บหรือหมดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือเมื่อเจ้าของข้อมูล ส่วนบุคคลร้องขอหรือเจ้าของข้อมูลส่วนบุคคลได้เพิกถอนความยินยอมในกรณีที่มีการขอความยินยอมไว้ เว้นแต่การเก็บรักษาข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนดซึ่งโดยปกติสำนักงานปลัดกระทรวงสาธารณสุขไม่ได้ใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

**ส่วนที่ ๑1.การมีส่วนร่วมของเจ้าของข้อมูล**

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

**ส่วนที่ ๑2.สิทธิของเจ้าของข้อมูลส่วนบุคคล**

 เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการดำเนินการ กับข้อมูลส่วนบุคคลของตนเอง ที่สำนักงานปลัด กระทรวงสาธารณสุขดูแลดังต่อไปนี้

 ๑2.๑  สิทธิในการขอรับข้อมูลส่วนบุคคลของตนเอง โดยเจ้าของข้อมูลมีสิทธิ ที่จะขอรับสำเนาข้อมูลส่วนบุคคลของตน และมีสิทธิที่จะร้องขอให้ เปิดเผยถึงการได้มาซึ่งข้อมูลของเจ้าของข้อมูล

 ๑2.๒  สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

 ๑2.๓  สิทธิขอให้ลบหรือทำลายข้อมูล โดยขอให้ สำนักงานปลัดงกระทรวงสาธารณสุข ดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูล ส่วนบุคคลได้ด้วยเหตุบางประการได้ตามที่กฎหมายกำหนด

 ๑2.๔  สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลโดยขอให้สำนักงานปลัดกระทรวงสาธารณสุขระงับ การใช้ข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

 ๑2.๕  สิทธิขอให้แก้ไขเปลี่ยนแปลง โดยขอให้ สำนักงานปลัดงกระทรวงสาธารณสุข ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

**ส่วนที่ ๑3. การจ้างการประมวลผลหรือมอบหมายให้ประมวลผล**

สำนักงานปลัดกระทรวงสาธารณสุขได้กำหนดแนวทางปฏิบัติในการทำสัญญาจ้างการประมวลผลข้อมูลส่วนบุคคล หรือมอบหมายให้ผู้อื่นประมวลผลข้อมูลส่วนบุคคลดังนี้

๑3.๑ ก่อนทำการจ้างหรือมอบหมายผู้ประมวลผลข้อมูล ต้องประเมินระบบ สอบทานและปรับปรุงมาตรการต่างๆในการคุ้มครองข้อมูลส่วนบุคคลของผู้รับจ้างหรือผู้ถูกมอบหมาย เพื่อให้แน่ใจว่า ระบบการรักษาความมั่นคงปลอดภัยข้อมูลมีความเหมาะสม เพียงพอ รวมถึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในส่วนของผู้รับจ้างหรือผู้รับมอบหมาย

๑3.๒ ในสัญญาจ้างหรือข้อตกลงการประมวลผล ต้องระบุวัตถุประสงค์ วิธีการเก็บข้อมูล การแจ้งเจ้าของข้อมูลส่วนบุคคล การใช้ การส่งและโอนข้อมูล และการกำจัดข้อมูล

๑3.๓ คู่สัญญาต้องลงนามในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม ที่สำนักงานปลัดกระทรวงสาธารณสุขกำหนด

๑3.๔ เมื่อมีการจ้างหรือมอบหมายให้มีการประมวลผลข้อมูล ต้องทำการควบคุมการประมวลผล และควบคุมการปฏิบัติให้เป็นไปตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานปลัดกระทรวงกำหนด

๑3.๕ เมื่อครบกำหนดการเก็บรักษาข้อมูล ต้องควบคุมให้ผู้รับประมวลผลทำลายข้อมูลตามกำหนด

**ส่วนที่ ๑4. การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้**

 สำนักงานปลัดกระทรวงสาธารณสุข กำหนดให้ทุกหน่วยงานภายใต้สังกัด ดำเนินการตรวจสอบ แยกแยะ ข้อมูลส่วนบุคคล ที่ถูกเก็บรวมรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้ ว่ายังเป็นข้อมูลส่วนบุคคล ที่ยังมีความจำเป็นต้องเก็บไว้หรือไม่ หากหมดความจำเป็นที่จะต้องเก็บรักษาไว้ ก็ให้ดำเนินการลบทำลาย

 ส่วนข้อมูลที่ยังมีความจำเป็นต้องเก็บรักษาไว้เพื่อใช้งานต่อไป ให้พิจารณาว่า เป็นข้อมูลที่ต้องขอ ความยินยอมก่อนการรวบรวมหรือไม่ (รายละเอียดในการพิจารณาขอให้ศึกษาในคู่มือปฏิบัติของข้อมูลส่วนบุคคลแต่ละประเภท) หากต้องขอความยินยอมให้ประสานงานกับเจ้าของข้อมูลและถ้าเจ้าของข้อมูลส่วนบุคคล ไม่ประสงค์ ให้สำนักงานปลัดกระทรวงสาธารณสุขเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ดังกล่าว ก็ให้ดำเนินการยกเลิกความยินยอมได้ตามประสงค์

**ส่วนที่ ๑5. แนวทางการดำเนินการลบทำลายข้อมูลส่วนบุคคล**

 ให้หน่วยงานที่มีความประสงค์จะลบทำลายข้อมูลรวบรวมบัญชีข้อมูลส่วนบุคคลที่เกี่ยวข้องเสนอขอความเห็นชอบมาที่สำนักปลัดกระทรวงสาธารณสุข โดยเสนอผ่านเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อนำเข้าสู่กระบวนการพิจารณาให้ความเห็นชอบ

**ส่วนที่ ๑6. แนวทางการปฏิบัติเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล**

 เหตุละเมิดข้อมูลส่วนบุคคล หมายถึง การที่ข้อมูลส่วนบุคคลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผยหรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น ไม่ว่าจะเกิดจาก การทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

 ในกรณีที่มีเหตุละเมิดข้อมูลส่วนบุคคลเกิดขึ้นภายในหน่วยงาน ผู้ที่ทราบเหตุจะต้องแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการละเมิดข้อมูลส่วนบุคคลส่วนบุคคล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลส่วนบุคคล และ/หรือ สำนักงานคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า รวมทั้งออกมาตรการเยียวยาเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกเหตุการณ์การการละเมิดข้อมูลส่วนบุคคล และประเมินความเสี่ยง เมื่อเกิดการละเมิดข้อมูลส่วนบุคคลขึ้นในการประเมินความเสี่ยงจากการละเมิด ข้อมูลส่วนบุคคลนั้น อาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ถ้าหากพิจารณาแล้วว่า ไม่ได้มีผลกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลหรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การละเมิดที่เกิดขึ้น แต่หากผลการประเมินแสดงให้เห็นว่าการละเมิดข้อมูลอาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้ง แก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งแนวทางในการเยียวยา อีกทั้งแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา ๗๒ ชั่วโมง นับจากทราบเหตุการณ์การละเมิดข้อมูล ส่วนบุคคล

 หน่วยงานควรมีการจัดทำแบบฟอร์มบันทึกการละเมิดข้อมูลส่วนบุคคลขึ้น เพื่อเป็นแนวทาง ในการจดบันทึกอย่างถูกต้องและครบถ้วน สำหรับหน้าที่ในการจดบันทึกควรกำหนดให้เป็นหน้าที่ ของเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคลหรืออาจให้พนักงานผู้พบเหตุการณ์เป็นผู้ทำการบันทึกแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้แล้วแต่กรณี และแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การละเมิดข้อมูลที่เกิดขึ้นโดยเร็ว เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการหาสาเหตุและมาตรการเยียวยา รวมถึงติดตามผลการดำเนินการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล โดยมีรายละเอียดการบันทึกหลักๆดังนี้

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

**ส่วนที่ ๑7. การขอความยินยอมและการถอนความยินยอม**

 การใช้ฐานความยินยอมในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นฐาน ในการประมวลผลที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะจัดการกับข้อมูลส่วนบุคคลของตนเองได้อย่างเต็มที่ ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ยกเว้น กรณีการประมวลผลข้อมูลส่วนบุคคล ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

 ภารกิจโดยส่วนใหญ่เกือบทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข เป็นการดำเนินการ โดยใช้ฐานอำนาจตามกฎหมาย เนื่องจากมีความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่สำนักงานปลัดกระทรวงสาธารณสุข หรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข หรือประโยชน์สาธารณะ ที่สำคัญอื่น ๆ เป็นต้น และไม่ต้องขอความยินยอม

 ๑7.๑ การเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องขอความยินยอม ให้หน่วยงานที่ต้องการดำเนินการดังกล่าวประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ก่อนเริ่มดำเนินการเพื่อพิจารณาให้ความเห็นชอบแนวทางปฏิบัติทั้งการขอความยินยอมและการถอนความยินยอม เว้นแต่เป็นการดำเนินการตามที่คู่มือปฏิบัติได้กำหนดไว้

 ๑7.๒ หน่วยงานควรเลือกใช้ฐานในการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเนื่องจากฐานความยินยอมไม่สามารถใช้ได้ทุกกรณี เว้นแต่กรณีที่ต้องขอความยินยอม ตามข้อกำหนดของกฎหมายอื่น ฐานความยินยอมจะเหมาะสมเมื่อการประมวลผลข้อมูลไม่ได้มี ความจำเป็นตามเงื่อนไขสัญญา นอกจากนั้นการให้ความยินยอมจะต้องเป็นสิ่งที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกได้ว่าจะให้หรือปฏิเสธก็ได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา การขอความยินยอมจะต้องอาศัยหลักการกระทำโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness, and Transparency) โดยหน่วยงานจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์และจะต้องคำนึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลใน การตัดสินใจให้ความยินยอม โดยการให้ความยินยอมจะต้องเป็นการสมัครใจ ดังนั้นการขอความยินยอมจะต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด

 ๑7.๓ เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

* ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผย ข้อมูลนั้นๆได้
* เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้
* การใช้ฐานความยินยอมนั้นจะต้องให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้ความยินยอมได้
* การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้นหน่วยงานจึงควรออกแบบแบบฟอร์มการขอความยินยอม ที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเห็นได้อย่างชัดเจนว่า หน่วยงานขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง
* ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคลในการ ให้ความยินยอมทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไข การให้บริการ (Terms& Conditions ) หรือข้อความในสัญญา
* การขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

 ๑7.๔ หน่วยงาน ต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกันต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาก็ควรระบุอยู่ในสัญญา ซึ่งการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) เนื่องจาก การกระทำดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดว่าหากไม่ให้ความยินยอมล้วจะไม่ได้รับบริการหรือมีผลต่อการใช้ผลิตภัณฑ์หรือบริการของหน่วยงาน

 ๑7.๕ การใช้ฐานความยินยอมอาจเหมาะสมในสถานการณ์ที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เฉพาะเจาะจงมากกว่า และหน่วยงานไม่สามารถประมวลผลข้อมูลตามวัตถุประสงค์ที่เพิ่มเติมขึ้นมาใหม่เองได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หน่วยงานจะต้องขอความยินยอมใหม่หากต้องการประมวลผลข้อมูลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว เว้นแต่ หากพิจารณาแล้วว่าการประมวลผลเพื่อวัตถุประสงค์นั้นสามารถทำได้ภายใต้ฐานกฎหมายฐานอื่น

 ๑7.๖ 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 บันทึกผ่านการติดต่อ กับเจ้าของข้อมูลส่วนบุคคลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลส่วนบุคคลกดปุ่มยืนยันการให้ความยินยอม เป็นต้น ซึ่งหน่วยงานจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลส่วนบุคคลจริง นอกจากนั้นหน่วยงานควรให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคล อย่างเพียงพอต่อการตัดสินใจมีทางเลือกและเนื้อหาชัดเจนไม่ก่อให้เกิดความ เข้าใจผิด และให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมหรือไม่ให้ ความยินยอมก็ได้โดยสมัครใจไม่เป็นการบังคับ

๑7.7 การถอนความยินยอม (Withdraw of Consent)

ในกรณีที่ท่านได้ให้ความยินยอมไว้ ท่านมีสิทธิที่จะขอเพิกถอนความยินยอม ที่ให้ไว้กับหน่วยงานในการเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และหน่วยงานจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้

 หากหน่วยงานไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวมใช้หรือเปิดเผยต่อไป ให้หน่วยงานดำเนินการลบข้อมูลออก

 การใช้สิทธิถอนความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูล ส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

**ส่วนที่ ๑8. การตรวจสอบและปรับปรุงระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล**

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

**ส่วนที่ ๑9. การพัฒนาบุคคลากรผู้ที่มีส่วนเกี่ยวข้อง**

 เพื่อให้บุคลากรทุกคนของสำนักงานปลัดกระทรวงสาธารณสุขได้รับข้อมูลความรู้ และ ความเข้าใจที่เพียงพอ สำนักงานปลัดกระทรวงสาธารณสุขจะดำเนินการตามที่จำเป็นเพื่อให้บุคลากร ได้รับทราบและตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคล

 บุคลากรที่มีหน้าที่เกี่ยวข้องกับการประมวลผลข้อมูล จะต้องได้รับการอบรม เพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลส่วนบุคคลตามที่สำนักงานปลัดกระทรวงสาธารณสุขกำหนด

**ส่วนที่ 20. การควบคุมเอกสาร**

 สำนักงานปลัดกระทรวงสาธารณสุข มีการควบคุมเอกสาร แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล และคู่มือปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล เอกสารที่เกี่ยวข้อง เพื่อให้ทุกหน่วยงานในสังกัดถือปฏิบัติ ให้เป็นไปในแนวทางเดียวกันและมีประสิทธิภาพ

**ส่วนที่ ๒1. การปรับปรุงทบทวนหรือแก้ไขคู่มือปฏิบัติ**

 สำนักงานปลัดกระทรวงสาธารณสุข อาจดำเนินการปรับปรุง ทบทวน หรือ แก้ไข คู่มือปฏิบัติฉบับนี้ ไม่ว่าบางส่วนหรือทั้งหมด หรือเป็นครั้งคราว เพื่อให้สอดคล้องกับนโยบายและแนวปฏิบัติการคุ้มครองข้อมูล ส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุข กฎหมาย กฎเกณฑ์ของหน่วยงานทางราชการที่มีอำนาจ

**ส่วนที่ ๒2. กฎหมายที่ใช้บังคับและเขตอำนาจศาล**

 นโยบาย และแนวปฏิบัติตามคู่มือการคุ้มครองข้อมูลส่วนบุคคลนี้อยู่ภายใต้การบังคับและตีความตามกฎหมายไทย และให้ศาลไทยเป็นผู้มีอำนาจในการพิจารณาข้อพิพาทใดที่อาจเกิดขึ้น

**ส่วนที่ ๒3.  การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติและนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล**

๒3.๑ สำนักงานปลัดกระทรวงสาธารณสุข มีการดำเนินการตามนโยบายการคุ้มครองข้อมูล ส่วนบุคคลของ กระทรวงสาธารณสุข โดยจะเผยแพร่ผ่านทางเว็บไซต์ https://pdpa.moph.go.th รวมทั้งหากมีการปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็จะดำเนินการเผยแพร่ผ่านช่องทางดังกล่าว รวมทั้งผ่านสื่อที่ กระทรวงสาธารณสุขใช้เพื่อการประชาสัมพันธ์ตามความเหมาะสมด้วย

๒3.๒ การดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ที่สำนักงานปลัดกระทรวงสาธารณสุข ประกาศใช้นี้ จะใช้เฉพาะสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกิจการของ สำนักงานปลัดกระทรวงสาธารณสุข ซึ่งรวมตลอดถึงการบริหารงาน การให้บริการ และการเข้าถึงเว็บไซต์ของ สำนักงานปลัดกระทรวงสาธารณสุข เท่านั้น หากผู้ใช้บริการมีการเชื่อมโยง (Link) ไปยังเว็บไซต์อื่นผ่านทางเว็บไซต์ของ สำนักงานปลัดกระทรวงสาธารณสุข ผู้ใช้บริการจะต้องศึกษาและปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ปรากฏในเว็บไซต์อื่นนั้นแยกต่างหากจากสำนักงานปลัดกระทรวงสาธารณสุขด้วย

**ส่วนที่ ๒4. แนวทางการคุ้มครองข้อมูลส่วนบุคคล**

 สำนักงานปลัดกระทรวงสาธารณสุข ได้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อการประสานงานในการคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลและสิทธิประโยชน์ของสำนักงานปลัดกระทรวงสาธารณสุข ช่วยให้สามารถบริหารความเสี่ยงและจัดการข้อมูล ส่วนบุคคล 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 ๑๒13 ,0 2590 2180 ต่อ 112,316

สำนักงานปลัดกระทรวงสาธารณสุข