

ระเบียบกระทรวงสาธารณสุข

ว่าด้วยระบบคลังข้อมูลด้านสาธารณสุข

พ.ศ. ๒๕๖๖

โดยที่เป็นการสมควรให้มีระเบียบกระทรวงสาธารณสุขว่าด้วยระบบคลังข้อมูลด้านสาธารณสุข เพื่อให้กระทรวงสาธารณสุขมีระบบคลังข้อมูลด้านสาธารณสุขที่มีความถูกต้อง ครบถ้วน เป็นเอกภาพ และหน่วยงานด้านสาธารณสุขหรือหน่วยงานที่เกี่ยวข้องสามารถเชื่อมโยง และแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ในสังกัดกระทรวงสาธารณสุข เพื่อให้เกิดการใช้ประโยชน์จากระบบคลังข้อมูลด้านสาธารณสุขได้อย่างมีประสิทธิภาพ ตลอดจนใช้ในการวางแผนกำหนดยุทธศาสตร์ ทิศทาง นโยบาย ทางด้านสาธารณสุข และเพื่อให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลสอดคล้องกับบทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา ๒๐ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ รัฐมนตรีว่าการกระทรวงสาธารณสุข จึงออกระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกระทรวงสาธารณสุขว่าด้วยระบบคลังข้อมูลด้านสาธารณสุข พ.ศ. ๒๕๖๖”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในระเบียบนี้

“ด้านสาธารณสุข” หมายความว่า การดำเนินการอันเกี่ยวกับการสร้างเสริมสุขภาพ อนามัย การป้องกัน ควบคุม และรักษาโรคภัย รวมทั้งปัจจัยที่คุกคามสุขภาพ การตรวจวินิจฉัย และบำบัดสภาวะ ความเจ็บป่วย การฟื้นฟูสมรรถภาพของบุคคล ครอบครัว และชุมชน

“ข้อมูลด้านสาธารณสุข” หมายความว่า ข้อมูลส่วนบุคคลด้านสาธารณสุข และให้หมายความรวมถึง รายละเอียดหรือข้อเท็จจริงที่เกี่ยวกับสุขภาพของบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแล ของหน่วยงาน หรือรายละเอียดและข้อเท็จจริงอื่นตามที่ปลัดกระทรวงสาธารณสุขประกาศกำหนด

“ระบบคลังข้อมูลด้านสาธารณสุข” หมายความว่า ระบบการประมวลผลข้อมูลด้านสาธารณสุข เพื่อให้บรรลุวัตถุประสงค์ตามภารกิจภายใต้หน้าที่และอำนาจของส่วนราชการตามที่กฎหมายกำหนด

“การประมวลผลข้อมูลด้านสาธารณสุข” หมายความว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ด้านสาธารณสุขทางระบบอิเล็กทรอนิกส์หรือระบบดิจิทัล

“ส่วนราชการผู้ควบคุมข้อมูล” หมายความว่า ส่วนราชการในกระทรวงสาธารณสุข ตามกฎหมายว่าด้วยปรับปรุงกระทรวง ทบวง กรม และมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“หน่วยงาน” หมายความว่า หน่วยงานที่มีฐานะเป็นกองหรือเทียบเท่ากองที่อยู่ในสังกัดของส่วนราชการผู้ควบคุมข้อมูล

“เจ้าของข้อมูล” หมายความว่า บุคคลที่เป็นเจ้าของข้อมูลด้านสาธารณสุข และให้หมายความรวมถึงบุคคลอื่นที่มีสิทธิดำเนินการแทนเจ้าของข้อมูลด้านสาธารณสุขตามกฎหมายว่าด้วยสุขภาพแห่งชาติ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ

“ผู้ควบคุมข้อมูลอื่น” หมายความว่า หน่วยงานของรัฐที่มีใช้ส่วนราชการผู้ควบคุมข้อมูลหน่วยงานเอกชน หรือบุคคลที่มีใช้เจ้าของข้อมูล

“ความมั่นคงปลอดภัย” หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

“บัญชีการประมวลผลข้อมูล” หมายความว่า รายชื่อหน่วยงาน ส่วนราชการผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูลอื่น รวมถึงรายการกิจกรรมที่มีการประมวลผลข้อมูลด้านสาธารณสุข

“ศทส.สป.” หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

ข้อ ๔ ให้ปลัดกระทรวงสาธารณสุขรักษาการตามระเบียบนี้

หมวด ๑

บททั่วไป

ข้อ ๕ ขอบเขตการใช้ วัตถุประสงค์ และเป้าหมาย

ระบบคลังข้อมูลด้านสาธารณสุขเป็นการรวบรวมข้อมูลและการเชื่อมโยงข้อมูลจากหน่วยงานด้านสุขภาพและสาธารณสุข โดยมี ศทส.สป. ทำหน้าที่บริหารจัดการให้เกิดการนำไปใช้ประโยชน์เพื่อสนับสนุนการให้บริการแก่ผู้รับบริการได้อย่างมีคุณภาพ และนำไปวิเคราะห์ข้อมูลสุขภาพและสาธารณสุขในด้านต่าง ๆ ตลอดจนนำไปวางแผนและตัดสินใจในการดำเนินนโยบายด้านสาธารณสุขของประเทศ หรือช่วยเพิ่มโอกาสในการดูแลสุขภาพให้ก้าวหน้ามากยิ่งขึ้น

ข้อ ๖ ส่วนราชการผู้ควบคุมข้อมูลต้องปฏิบัติหน้าที่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และเป็นอิสระต่อกัน

ข้อ ๗ ในกรณีที่ระเบียบนี้ไม่ได้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติไว้ให้ถือปฏิบัติตามระเบียบ กฎหมายที่เกี่ยวข้องโดยอนุโลม

หมวด ๒

การประมวลผลข้อมูลด้านสาธารณสุข

ส่วนที่ ๑

มาตรฐานและคุณภาพของข้อมูลด้านสาธารณสุข

ข้อ ๘ หน่วยงานต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลด้านสาธารณสุขเกี่ยวกับการประมวลผลข้อมูลด้านสาธารณสุขกับระบบคลังข้อมูลด้านสาธารณสุขตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อน หรือในขณะที่เก็บรวบรวม ใช้ หรือเปิดเผย เว้นแต่จะมีกฎหมายกำหนดไว้เป็นอย่างอื่น

กรณีหน่วยงานไม่ได้แจ้งวัตถุประสงค์ตามวรรคหนึ่ง ให้หน่วยงานจัดทำประกาศความเป็นส่วนตัว (Privacy Notice) เพื่อแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลทราบด้วย

ข้อ ๙ ให้หน่วยงานจัดทำมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูลด้านสาธารณสุข เพื่อให้มีความถูกต้อง ครบถ้วน พร้อมใช้งาน ให้เป็นปัจจุบัน สามารถบูรณาการ เชื่อมโยง และแลกเปลี่ยนกันได้ รวมทั้งมีการวัดผลการบริหารจัดการข้อมูลด้านสาธารณสุข และต่อยอดนวัตกรรมจากการใช้ข้อมูลด้านสาธารณสุขได้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติที่ปลัดกระทรวงสาธารณสุขกำหนด

ข้อ ๑๐ ให้หน่วยงานกำหนดนโยบายหรือมาตรการเข้าถึงและใช้ประโยชน์จากข้อมูลด้านสาธารณสุขที่ชัดเจน และมีระบบบริหารจัดการในการคุ้มครองข้อมูลที่อยู่ในความครอบครอง ให้มีความมั่นคงปลอดภัย และมีให้ข้อมูลส่วนบุคคลถูกละเมิด โดยอย่างน้อยต้องจัดให้มีระบบป้องกันหรือรับมือกับภัยคุกคาม หรือความเสี่ยงทางไซเบอร์ตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑๑ ให้หน่วยงานบันทึกการกิจกรรมการประมวลผลข้อมูลด้านสาธารณสุข เพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ตามมาตรา ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๑๒ ให้ ศทส. สป. จัดทำบัญชีการประมวลผลข้อมูล เพื่อประโยชน์ในการบริหารจัดการข้อมูลด้านสาธารณสุข

ข้อ ๑๓ ให้ ศทส.สป. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ควบคุม กำกับดูแลให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานมีการพัฒนาระบบคลังข้อมูลด้านสาธารณสุขให้ได้ตามมาตรฐาน มาตรการ หรือกลไกการกำกับดูแลที่เกี่ยวข้อง รวมถึงการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) เสนอแนะออกหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติให้หน่วยงานจัดทำมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูลด้านสาธารณสุข รวมการวัดผลการบริหารจัดการข้อมูลด้านสาธารณสุข และต่อยอดนวัตกรรมตามข้อ ๙

(๓) เสนอแนะออกหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานเชื่อมโยงข้อมูลด้านสาธารณสุขที่อยู่ในความครอบครองหรือควบคุมดูแลกับระบบคลังข้อมูลด้านสาธารณสุขตามข้อ ๑๔

(๔) เสนอแนะออกหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานประมวลผลข้อมูลด้านสาธารณสุขระหว่างกันได้ตามข้อ ๑๖

(๕) เสนอแนะออกหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติให้ส่วนราชการผู้ควบคุมข้อมูลควบคุม กำกับดูแล และส่งเสริมให้หน่วยงานดำเนินการเชื่อมโยงข้อมูลด้านสาธารณสุขกับ ศทส.สป. ตามข้อ ๑๙

(๖) ให้คำแนะนำหรือเสนอความเห็นต่อปลัดกระทรวงสาธารณสุขในการพิจารณาตามข้อ ๒๐

(๗) บริหารสถานการณ์ฉุกเฉินด้านข้อมูลด้านสาธารณสุขในระบบคลังข้อมูลด้านสาธารณสุข เช่น ข้อมูลรั่วไหล ข้อมูลถูกละเมิด

ส่วนที่ ๒

การเชื่อมโยงข้อมูลด้านสาธารณสุข

ข้อ ๑๔ ให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานเชื่อมโยงข้อมูลด้านสาธารณสุขที่อยู่ในความครอบครองหรือควบคุมดูแลกับระบบคลังข้อมูลด้านสาธารณสุข ตามหลักเกณฑ์ วิธีการ และเงื่อนไข หรือแนวทางปฏิบัติที่ปลัดกระทรวงสาธารณสุขกำหนด

ข้อ ๑๕ ให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยโดยเคร่งครัดในขณะที่มีการเชื่อมโยงข้อมูลด้านสาธารณสุข เพื่อป้องกันการสูญหายเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๑๖ ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานสามารถประมวลผลข้อมูลด้านสาธารณสุขเพื่อใช้งานตามภารกิจระหว่างส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานได้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติที่ปลัดกระทรวงสาธารณสุขกำหนด

ข้อ ๑๗ ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานที่ประสงค์จะดำเนินการตามข้อ ๑๖ ให้แจ้ง ศทส.สป. เพื่อบันทึกบัญชีการประมวลผลข้อมูล

ในกรณีที่ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานประสงค์ยุติการดำเนินการตามข้อ ๑๖ ให้แจ้ง ศทส.สป. เพื่อบันทึกบัญชีการประมวลผลข้อมูลภายใน ๓๐ วันนับแต่วันที่ยุติการดำเนินการดังกล่าว

ข้อ ๑๘ ให้หน่วยงานจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลด้านสาธารณสุขที่ได้รับจากระบบคลังข้อมูลด้านสาธารณสุขตามมาตรา ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๑๙ ส่วนราชการผู้ควบคุมข้อมูล มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ควบคุม กำกับดูแล และส่งเสริมให้หน่วยงานดำเนินการเชื่อมโยงข้อมูลด้านสาธารณสุขกับระบบคลังข้อมูลด้านสาธารณสุขเพื่อให้ใช้งานอย่างมีประสิทธิภาพ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติที่ปลัดกระทรวงสาธารณสุขกำหนด

(๒) มอบหมายหน่วยงานดำเนินการกำหนดวิธีจัดการระบบข้อมูลด้านสาธารณสุขที่อยู่ในความครอบครองหรือควบคุมดูแล และจัดให้มีกระบวนการปรับปรุงข้อมูลด้านสาธารณสุขให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน เพื่อให้หน่วยงานสามารถใช้งานได้อย่างมีประสิทธิภาพ

(๓) ติดตามและประเมินผลการปฏิบัติของหน่วยงานตามระเบียบนี้

หมวด ๓

การเปิดเผยข้อมูลด้านสาธารณสุข

ส่วนที่ ๑

สำหรับส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงาน

ข้อ ๒๐ ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานสามารถขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขจากระบบคลังข้อมูลด้านสาธารณสุขได้ ภายใต้ขอบเขตที่กำหนดไว้ตามกฎหมายว่าด้วยสุขภาพแห่งชาติ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และกฎหมายอื่นที่เกี่ยวข้อง โดยยื่นคำขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขต่อปลัดกระทรวงสาธารณสุขหรือผู้ที่ปลัดกระทรวงสาธารณสุขมอบหมายพิจารณาอนุญาต ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติที่ปลัดกระทรวงสาธารณสุขกำหนด โดยอย่างน้อยต้องปฏิบัติ ดังต่อไปนี้

(๑) ให้ขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขเพียงเท่าที่จำเป็นสำหรับวัตถุประสงค์การดำเนินการตามอำนาจหน้าที่เท่านั้น

(๒) ห้ามใช้หรือเปิดเผยข้อมูลด้านสาธารณสุข เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้ หากประสงค์จะใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขที่แตกต่างไปจากวัตถุประสงค์เดิมที่ได้แจ้งไว้แก่ ศทส.สป. ให้หน่วยงานแจ้งวัตถุประสงค์ใหม่นั้นให้ปลัดกระทรวงสาธารณสุขหรือผู้ที่ปลัดกระทรวงสาธารณสุขมอบหมายพิจารณาอนุญาตก่อนใช้หรือเปิดเผยข้อมูลนั้น

(๓) ให้จัดทำรายละเอียดการขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขจากระบบคลังข้อมูลด้านสาธารณสุข ดังนี้

(ก) วัตถุประสงค์

(ข) ประเภทข้อมูลส่วนบุคคลตามมาตรา ๒๔ หรือมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พร้อมทั้งอธิบายฐานอำนาจในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis of Processing)

(ค) รายการข้อมูลด้านสาธารณสุข

(ง) มาตรการรักษาความมั่นคงปลอดภัยแก่ข้อมูลด้านสาธารณสุขที่ได้รับจากระบบคลังข้อมูลด้านสาธารณสุขเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลด้านสาธารณสุขโดยปราศจากอำนาจหรือโดยมิชอบ

หากส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานที่มีการเชื่อมโยงข้อมูลด้านสาธารณสุขไว้ที่ระบบคลังข้อมูลด้านสาธารณสุข มีความประสงค์จะขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขอื่นนอกเหนือจากวรรคหนึ่งจากระบบคลังข้อมูลด้านสาธารณสุข ให้ยื่นคำขอใช้หรือเปิดเผยข้อมูลด้านสาธารณสุขต่อปลัดกระทรวงสาธารณสุขหรือผู้ที่ปลัดกระทรวงสาธารณสุขมอบหมายพิจารณาอนุญาต ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขหรือแนวทางปฏิบัติตามวรรคหนึ่งโดยอนุโลม

ส่วนที่ ๒

สำหรับผู้ควบคุมข้อมูลอื่น

ข้อ ๒๑ การเปิดเผยข้อมูลด้านสาธารณสุขที่เป็นข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลอื่นให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานแจ้งรายละเอียดที่จำเป็นเกี่ยวกับการเปิดเผยข้อมูลและฐานทางกฎหมาย หรือหน้าที่และอำนาจโดยชอบด้วยกฎหมายที่สามารถเปิดเผยต่อผู้ควบคุมข้อมูลอื่นได้ให้แก่เจ้าของข้อมูลทราบก่อนหรือในขณะที่เปิดเผยข้อมูลดังกล่าว

กรณีการเปิดเผยข้อมูลด้านสาธารณสุขที่เป็นข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลอื่นโดยไม่มีฐานทางกฎหมายหรือไม่มีหน้าที่และอำนาจโดยชอบด้วยกฎหมาย จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนหรือในขณะนั้น

ผู้ควบคุมข้อมูลอื่นมีหน้าที่ในการประมวลผลข้อมูลด้านสาธารณสุขที่ได้รับจากระบบคลังข้อมูลด้านสาธารณสุข ดังนี้

(๑) รักษาความลับและปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลโดยเคร่งครัด

(๒) ดำเนินการประมวลผลข้อมูลด้านสาธารณสุขตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่กฎหมายที่เกี่ยวข้องจะกำหนดไว้เป็นประการอื่น

(๓) ไม่เปิดเผยข้อมูลด้านสาธารณสุขที่ได้รับแก่บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องในการประมวลผล หรือบุคคลภายนอกใด ๆ เว้นแต่ที่มีความจำเป็นต้องกระทำตามหน้าที่ หรือเพื่อปฏิบัติตามกฎหมายที่ใช้บังคับ หรือได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนเปิดเผย

ในการดำเนินการตามวรรคสามให้ถือว่าผู้ควบคุมข้อมูลอื่นได้รับทราบและตกลงว่าแต่ละฝ่ายต่างมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของข้อมูลส่วนบุคคลที่ตนประมวลผล และต่างอยู่ภายใต้บังคับในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในบทบัญญัติที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลต่างหากจากกัน

ข้อ ๒๒ ให้ผู้ควบคุมข้อมูลอื่นจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนด เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

ข้อ ๒๓ ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานอาจมอบหมายหรือจ้างผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งให้บริการในลักษณะเป็นผู้ดูแล (Hosting) รับงานบริการช่วง (Outsourcing) หรือเป็นผู้ให้บริการคลาวด์ (Cloud computing service/provider) หรือเป็นงานในลักษณะการจ้างในรูปแบบอื่นให้ทำการประมวลผลข้อมูลส่วนบุคคลแทนก็ได้

การมอบหมายหรือการจ้างตามวรรคหนึ่งให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานต้องจัดให้มีข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างกัน ซึ่งอย่างน้อยต้องมีรายละเอียดประเภทข้อมูลส่วนบุคคลที่มอบหมายให้ประมวลผล รวมถึงวัตถุประสงค์ขอบเขตในการประมวลผลข้อมูลส่วนบุคคล และข้อตกลงอื่น ๆ ที่เกี่ยวข้อง

ข้อ ๒๔ ในกรณีที่ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานเปิดเผยข้อมูลด้านสาธารณสุขไปยังต่างประเทศหรือองค์การระหว่างประเทศ โดยประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามหลักเกณฑ์ที่กำหนดในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

หมวด ๔

การแจ้งเหตุละเมิด

ข้อ ๒๕ เมื่อเกิดเหตุใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลด้านสาธารณสุขในระบบคลังข้อมูลด้านสาธารณสุข หรือในกรณีที่ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานต้องดำเนินการเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานแจ้งเหตุหรือการละเมิดกรณีดังกล่าว พร้อมทั้งแนวทางการเยียวยาความเสียหายของเจ้าของข้อมูล มาตรการที่ใช้หรือจะใช้

เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลให้แก่ ศทส.สป. ภายใน ๒๔ ชั่วโมงนับแต่ทราบเหตุ หรือการละเมิดกรณีดังกล่าว

เมื่อส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานได้ดำเนินมาตรการป้องกันเรียบร้อยแล้ว ให้รายงานการเกิดเหตุหรือการละเมิดตามวรรคหนึ่ง และมาตรการที่ใช้ในการป้องกันต่อปลัดกระทรวงสาธารณสุข เพื่อทราบต่อไป

ข้อ ๒๖ ในกรณีที่มีเหตุละเมิดเกิดขึ้นในระบบคลังข้อมูลด้านสาธารณสุขในชั้นตอนที่เกี่ยวกับ ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานให้ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานปฏิบัติตามคำสั่ง ของผู้อำนวยการ ศทส.สป. ในฐานะผู้บริหารสถานการณ์ฉุกเฉินด้านข้อมูลด้านสาธารณสุข เพื่อตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดโดยไม่ชักช้า

ในกรณีที่ส่วนราชการผู้ควบคุมข้อมูลหรือหน่วยงานไม่ปฏิบัติตามคำสั่งของผู้อำนวยการ ศทส.สป. ตามวรรคหนึ่ง ให้ผู้อำนวยการ ศทส.สป. รายงานการไม่ปฏิบัติตามคำสั่ง พร้อมทั้งความเห็นเกี่ยวกับ ความเสียหายหรือผลกระทบที่อาจเกิดจากการไม่ปฏิบัติตามคำสั่งต่อปลัดกระทรวงสาธารณสุข เพื่อพิจารณาสั่งการต่อไป

หมวด ๕

สิทธิของเจ้าของข้อมูล

ข้อ ๒๗ เจ้าของข้อมูลมีสิทธิดำเนินการเกี่ยวกับข้อมูลด้านสาธารณสุขของตนที่อยู่ในระบบ คลังข้อมูลด้านสาธารณสุขได้ ตามสิทธิที่กำหนดไว้ในกฎหมายว่าด้วยสุขภาพแห่งชาติ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ โดยหน่วยงาน ที่ควบคุมดูแลข้อมูลด้านสาธารณสุขของเจ้าของข้อมูลดังกล่าว มีหน้าที่พิจารณาดำเนินการตามคำขอ

ประกาศ ณ วันที่ ๒๖ ธันวาคม พ.ศ. ๒๕๖๖

ชลน่าน ศรีแก้ว

รัฐมนตรีว่าการกระทรวงสาธารณสุข