



ระเบียบกระทรวงสาธารณสุข

เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑

โดยที่กระทรวงสาธารณสุขมีนโยบายที่จะให้ประชาชนทุกคนสามารถเข้าถึงบริการด้านการให้คำแนะนำด้านสุขภาพและวินิจฉัยโรคเบื้องต้น โดยบูรณาการระบบประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์ เชื่อมต่อกันทั้งประเทศที่ประชาชนสามารถเข้าถึงและบริหารจัดการข้อมูลสุขภาพของตนเองได้ เพื่ออำนวยความสะดวกในการเข้ารับการรักษาและเป็นข้อมูลสำคัญประกอบการรักษากรณีฉุกเฉิน นอกจากนี้ข้อมูลสุขภาพด้านบุคคลยังสามารถนำไปใช้ประโยชน์ในการพัฒนาระบบสุขภาพของประเทศต่อไป ดังนั้นจึงมีความจำเป็นที่จะต้องมีการควบคุม กำกับเพื่อให้การได้มา การบริหารจัดการ การใช้และการคุ้มครองข้อมูลด้านสุขภาพของบุคคลมีความสะดวก ปลอดภัย เกิดประโยชน์สูงสุดแก่ประชาชนเจ้าของข้อมูล หน่วยบริการและระบบสุขภาพของประเทศไทย จึงเป็นการสมควรมีระเบียบ เรื่องการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล เพื่อกำหนดหลักเกณฑ์ วิธีการ และแนวทางปฏิบัติให้เหมาะสม สอดคล้องกับ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายอื่นที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๐ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม รัฐมนตรีว่าการกระทรวงสาธารณสุขจึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกระทรวงสาธารณสุขเรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวัน (๑๒๐ วัน) นับจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในกรณีที่มีการดำเนินการใดๆ เกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ระเบียบนี้ไม่ได้กำหนดไว้ให้ปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศหรือคำสั่งที่ออกตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายอื่นที่เกี่ยวข้อง

ข้อ ๔ ในระเบียบนี้

“ข้อมูลด้านสุขภาพของบุคคล” หมายความว่า ข้อมูลหรือสิ่งใด ๆ ที่แสดงออกมาในรูปเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องมือทางอิเล็กทรอนิกส์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏขึ้นในเรื่องที่เกี่ยวกับสุขภาพของบุคคลที่สามารถระบุตัวบุคคลได้และให้รวมถึงข้อมูลอื่น ๆ ตามที่คณะกรรมการเปิดเผยข้อมูลอิเล็กทรอนิกส์ประกาศกำหนด

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อมูลด้านสุขภาพของบุคคลที่เป็นเอกสารหรือข้อความในรูปแบบอิเล็กทรอนิกส์

“ระเบียบน...

“ระเบียบสุขภาพ” หมายความว่า ทะเบียนหรือรายการ ข้อมูลด้านสุขภาพของบุคคล ที่กระทรวงสาธารณสุข หน่วยงานทั้งภาครัฐและเอกชน นำมาเก็บ จัดการ ใช้และเปิดเผยเพื่อประโยชน์ ของเจ้าของข้อมูลตามระเบียบนี้

“เจ้าของข้อมูล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลด้านสุขภาพ

“ผู้ควบคุมข้อมูล” หมายความว่า ส่วนราชการ หน่วยงาน โรงพยาบาล โรงเรียน สถานส่งเสริมสุขภาพตำบล สถานีอนามัยในสังกัดกระทรวงสาธารณสุขและหมายรวมถึงสถานพยาบาล ตามพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ และหน่วยงานของรัฐอื่นที่ประสงค์เข้าร่วมใช้ข้อมูล ด้านสุขภาพร่วมกับกระทรวงสาธารณสุขซึ่งเป็นผู้จัดทำ เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลด้านสุขภาพ ของบุคคล

“ผู้บริหารจัดการข้อมูล” หมายความว่า กระทรวงสาธารณสุขรวมถึงบุคคลหรือหน่วยงาน ที่ได้รับมอบหมายจากกระทรวงสาธารณสุข

“ผู้รับข้อมูล” หมายความว่า บุคคลหรือนิติบุคคลที่ได้รับข้อมูลด้านสุขภาพของ บุคคลจากผู้ควบคุมข้อมูลและนำข้อมูลนั้นไปใช้เพื่อประโยชน์ของเจ้าของข้อมูล

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองและจัดการข้อมูลด้านสุขภาพ ของบุคคล

“เจ้าหน้าที่” หมายความว่า ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้าง ของกระทรวงสาธารณสุขที่ปฏิบัติงานเกี่ยวกับข้อมูลด้านสุขภาพของกระทรวงสาธารณสุข

ข้อ ๕ การจัดทำระเบียบสุขภาพ การจัดการ เก็บรวบรวม ใช้หรือเปิดเผยข้อมูล ด้านสุขภาพของบุคคลต้องเป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลหรือเพื่อดำเนินงานตามหน้าที่และ อำนาจของผู้ควบคุมข้อมูล หรือหน้าที่และอำนาจของกระทรวงสาธารณสุขตามที่ได้รับมอบหมาย

หมวด ๑

คณะกรรมการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล

ข้อ ๖ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการคุ้มครองและจัดการข้อมูล ด้านสุขภาพของบุคคล” ประกอบด้วย

(๑) ปลัดกระทรวงสาธารณสุขเป็นประธานกรรมการ

(๒) รองปลัดกระทรวงสาธารณสุขผู้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงประจำกระทรวงสาธารณสุขเป็นรองประธานกรรมการ

(๓) ผู้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำสำนักงาน ปลัดกระทรวงสาธารณสุข ผู้แทนกรมควบคุมโรค ผู้แทนกรมสุขภาพจิต ผู้แทนกรมการแพทย์ ผู้แทนกรม สนับสนุนบริการสุขภาพ ผู้แทนนายแพทย์สาธารณสุขจังหวัด ผู้แทนโรงพยาบาลในสังกัดสำนักงาน ปลัดกระทรวงสาธารณสุขและผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่ปลัดกระทรวงสาธารณสุขแต่งตั้งจาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ สำนักงาน คณะกรรมการคุ้มครองผู้บริโภค สำนักงานคณะกรรมการกฤษฎีกา และสำนักงานคณะกรรมการสุขภาพ แห่งชาติหน่วยงานละ ๑ คน เป็นกรรมการ

(๔) นักวิชาการที่ปลัดกระทรวงสาธารณสุขแต่งตั้งจำนวน ๒ คนเป็นกรรมการ

(๕) ผู้อำนวยการ...

(๕) ผู้อำนวยการกองบริหารการสาธารณสุข สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๖) ผู้อำนวยการกองกฎหมาย สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๗) ผู้อำนวยการกองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการ

(๘) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขเป็นกรรมการและเลขานุการ

ให้เลขานุการแต่งตั้งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวนไม่เกิน ๒ คนเป็นผู้ช่วยเลขานุการ

ข้อ ๗ ให้คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) กำหนดข้อมูลที่จะต้องนำไปไว้ในระเบียบสุขภาพ

(๒) กำหนดนโยบายการดำเนินการและการพัฒนาข้อมูลด้านสุขภาพของบุคคลและระเบียบสุขภาพ

(๓) กำหนดข้อมูลด้านสุขภาพของบุคคลตามข้อ ๑๑ (๕)

(๔) ออกประกาศ ข้อกำหนด หลักเกณฑ์หรือแนวทางการปฏิบัติในการจัดการข้อมูลด้านสุขภาพของบุคคลให้เกิดประโยชน์สูงสุดกับเจ้าของข้อมูลตามข้อ ๒๙

(๕) ออกประกาศ ข้อกำหนด หลักเกณฑ์หรือแนวทางการปฏิบัติตามข้อ ๓๐ และข้อ ๓๑

(๖) ออกประกาศ ข้อกำหนด หลักเกณฑ์เกี่ยวกับทะเบียนผู้ควบคุมข้อมูลและผู้รับข้อมูลตามข้อ ๓๓

(๗) ดำเนินการต่าง ๆ เพื่อให้เป็นไปตามวัตถุประสงค์ของระเบียบสุขภาพตามข้อ ๒๗

(๘) ติดตาม กำกับการดำเนินการจัดการข้อมูลด้านสุขภาพของบุคคล

(๙) เสนอแนะหรือให้คำปรึกษาแก่รัฐมนตรีว่าการกระทรวงสาธารณสุขหรือปลัดกระทรวงสาธารณสุขในการดำเนินการเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลของกระทรวงสาธารณสุข

(๑๐) แต่งตั้งคณะกรรมการหรือที่ปรึกษาเพื่อดำเนินการตามระเบียบนี้หรือตามที่คณะกรรมการมอบหมาย

(๑๑) พิจารณาทบทวนระเบียบนี้ให้มีความเหมาะสมกับสถานการณ์ และเสนอแก้ไขระเบียบต่อรัฐมนตรีว่าการกระทรวงสาธารณสุข

(๑๒) ปฏิบัติการอื่นใดเพื่อให้บรรลุวัตถุประสงค์ของระเบียบนี้

ข้อ ๘ การประชุมคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงจะเป็นองค์ประชุม

ในการประชุมคณะกรรมการถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ให้รองประธานกรรมการเป็นประธานในที่ประชุม ถ้ารองประธานกรรมการไม่มาหรือไม่อาจปฏิบัติหน้าที่ได้ให้ที่ประชุมเลือกกรรมการคนหนึ่งทำหน้าที่ประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงในการลงคะแนนเท่ากันให้ประธานกรรมการออกเสียงเพิ่มอีกหนึ่งเสียงเป็นเสียงชี้ขาด

ข้อ ๙ การประชุมคณะกรรมการให้นำข้อ ๘ มาบังคับใช้โดยอนุโลม

ข้อ ๑๐ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขทำหน้าที่สำนักงานเลขานุการคณะกรรมการ เพื่อดำเนินการตามที่คณะกรรมการมอบหมายและตามที่กำหนดไว้ในระเบียบนี้

หมวด ๒

การคุ้มครองข้อมูลด้านสุขภาพของบุคคล

ข้อ ๑๑ ข้อมูลดังต่อไปนี้ถือเป็นข้อมูลด้านสุขภาพของบุคคล

(๑) ประวัติสุขภาพเฉพาะของบุคคล เช่น ส่วนสูง น้ำหนัก หมู่เลือด รูปร่าง ลักษณะทั่วไปของร่างกาย เป็นต้น

(๒) ประวัติการรักษาพยาบาล เช่น เวชระเบียน บันทึกการพยาบาล การตรวจทางห้องปฏิบัติการ พิล์มเอ็กซเรย์ เป็นต้น

(๓) เอกสารและวัตถุต่างๆ ที่เกี่ยวกับ (๑) และ (๒)

(๔) ภาพถ่ายการปฏิบัติงานรักษาพยาบาลผู้ป่วยของบุคลากรทางการแพทย์หรือเจ้าหน้าที่อื่นในการรักษาพยาบาล รวมถึงการกระทำด้วยประการใดๆ ให้ปรากฏภาพ เสียงของบุคคลดังกล่าว

(๕) ข้อมูลที่คณะกรรมการกำหนด

ข้อ ๑๒ ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดให้มีสถานที่เก็บรวบรวมข้อมูลด้านสุขภาพของบุคคลให้อยู่ในสภาพที่เหมาะสม มีมาตรการด้านความปลอดภัยที่รัดกุม

เจ้าหน้าที่ต้องเป็นผู้ที่มีความรู้ด้านการจัดการข้อมูลและด้านกฎหมายที่เกี่ยวข้อง

ข้อ ๑๓ ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล จะเปิดเผยได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลหรือผู้มีอำนาจกระทำการแทนตามข้อ ๑๔ (๒) - (๕) และตามที่กฎหมายบัญญัติไว้เท่านั้น และการเปิดเผยจะทำให้เกิดความเสียหายแก่เจ้าของข้อมูลและผู้ครอบครองข้อมูลไม่ได้

ข้อ ๑๔ บุคคลดังต่อไปนี้ มีสิทธิขอให้เปิดเผยข้อมูลด้านสุขภาพของบุคคล

(๑) ผู้เป็นเจ้าของข้อมูล

(๒) ผู้ที่ได้รับมอบอำนาจจากผู้เป็นเจ้าของข้อมูล

(๓) ผู้ที่ได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล

(๔) ผู้มีอำนาจกระทำการแทนเจ้าของข้อมูล คือ ผู้แทนโดยชอบธรรม กรณีเจ้าของข้อมูลเป็นเด็กหรือผู้เยาว์ ผู้อนุบาล กรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถหรือผู้พิทักษ์ กรณีเจ้าของข้อมูลเป็นคนเสมือนไร้ความสามารถ ทั้งนี้ถ้าผู้เยาว์อายุ ๑๕ ปีบริบูรณ์แล้วต้องได้รับความยินยอมจากผู้เยาว์นั้นก่อน

(๕) ทายาท ในกรณีผู้เป็นเจ้าของข้อมูลเสียชีวิต

ทายาทตาม (๕) หมายถึง สามีหรือภรรยาโดยชอบด้วยกฎหมาย บุตรหรือผู้สืบสันดานตามความเป็นจริง บุตรบุญธรรมตามกฎหมาย บิดาหรือมารดาตามความเป็นจริง

ข้อ ๑๕...

ข้อ ๑๕ บุคคลดังต่อไปนี้มีอำนาจขอให้ผู้ควบคุมข้อมูลเปิดเผยข้อมูลด้านสุขภาพของบุคคลโดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลหรือผู้มีอำนาจกระทำการคือ ศาล พนักงานสอบสวนเจ้าหน้าที่ตำรวจ คณะกรรมการสิทธิมนุษยชน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าหน้าที่ที่มีกฎหมายให้อำนาจในการเรียกเอกสารข้อมูลด้านสุขภาพของบุคคลได้ ทั้งนี้ ต้องอยู่ภายใต้หลักการไม่เป็นการนำข้อมูลไปใช้ในทางให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือทายาท

ข้อ ๑๖ ผู้ขอข้อมูลจะต้องดำเนินการดังต่อไปนี้

- (๑) ยื่นคำขอเป็นหนังสือและลงลายมือชื่อผู้ขอ
- (๒) ระบุวัตถุประสงค์ของการขอข้อมูลว่าจะนำไปใช้ประโยชน์อย่างไร
- (๓) แนบเอกสารประกอบการขอข้อมูลตามที่กำหนดไว้
- (๔) รับทราบเงื่อนไขที่ผู้ควบคุมข้อมูลกำหนด

ข้อ ๑๗ เอกสารประกอบคำขอตามข้อ ๑๖ (๓) มีดังนี้

- (๑) สำเนาบัตรประจำตัวผู้ขอ
- (๒) กรณีเป็นผู้รับมอบอำนาจ ต้องมีสำเนาบัตรประจำตัวผู้มอบอำนาจ ผู้รับมอบอำนาจและหนังสือมอบอำนาจ (ติดอากรแสตมป์) ด้วย
- (๓) กรณีเจ้าของข้อมูลให้ความยินยอม ต้องมีหนังสือแสดงความยินยอมที่ลงลายมือชื่อเจ้าของข้อมูลมาแสดงด้วย (ถ้าเป็นสำเนาควรขอตัวจริง)
- (๔) กรณีทายาท ต้องมีใบมรณะบัตรและเอกสารแสดงการเป็นทายาท เช่น ใบทะเบียนสมรส สำเนาทะเบียนบ้าน สูติบัตร คำสั่งศาล เป็นต้น
- (๕) กรณีเป็นทารก เด็ก ผู้เยาว์ หรือผู้ที่ไม่สามารถช่วยเหลือตนเองได้หรือเป็นผู้พิการไม่สามารถรับรู้การกระทำหรือเป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ ผู้แทนโดยชอบธรรมคือบิดาหรือมารดาตามความเป็นจริง ผู้ปกครองที่ศาลตั้ง ผู้อนุบาลหรือผู้พิทักษ์ต้องแสดงคำสั่งศาลหรือหลักฐานที่แสดงการเป็นผู้ปกครอง ผู้อนุบาล ผู้พิทักษ์ หรือผู้แทนโดยชอบธรรม
- (๖) เอกสารอื่นๆตามที่ผู้ควบคุมข้อมูลกำหนด

ข้อ ๑๘ เมื่อเจ้าหน้าที่ได้รับคำขอให้ตรวจสอบคำขอและเอกสารที่เกี่ยวข้องให้ถูกต้องครบถ้วนแล้วจึงเสนอคำขอพร้อมความเห็นไปให้ผู้มีอำนาจพิจารณาอนุมัติให้เปิดเผยข้อมูลดังกล่าวหรืออาจนำเสนอคณะกรรมการข้อมูลข่าวสารของผู้ควบคุมข้อมูลก่อนก็ได้

ผู้มีอำนาจกระทำการแทนผู้ควบคุมข้อมูลหรือผู้ที่ได้รับมอบหมายเป็นผู้มีอำนาจอนุมัติการเปิดเผยข้อมูลด้านสุขภาพของบุคคล

ข้อ ๑๙ ในกรณีผู้ขอให้เปิดเผยข้อมูล ขอสำเนาข้อมูลด้านสุขภาพของบุคคลให้กำหนดเงื่อนไข ดังนี้

- (๑) ผู้ขอต้องใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น
- (๒) ผู้ขอต้องไม่นำข้อมูลไปเผยแพร่ จำหน่าย จ่าย แจก หรือกระทำโดยประการใดๆ ในลักษณะเช่นว่านั้น
- (๓) ผู้ขอต้องไม่นำข้อมูลไปใช้ในทางที่อาจจะก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือผู้ควบคุมข้อมูล หากมีความเสียหายเกิดขึ้น ผู้ขอต้องรับผิดชอบทั้งสิ้น

เมื่อผู้ขอข้อมูลลงนามรับทราบเงื่อนไขดังกล่าวแล้วจึงมอบสำเนาข้อมูลดังกล่าวแก่ผู้ขอต่อไป ในกรณีผู้ขอรับทราบเงื่อนไขแล้วไม่ยอมลงนามให้บันทึกไว้และเจ้าหน้าที่ลงนามกำกับพร้อมพยานและมอบสำเนาข้อมูลให้ผู้ขอ

ข้อ ๒๐...

ข้อ ๒๐ ในกรณีผู้ขอข้อมูลไม่ใช่เจ้าของข้อมูล และเจ้าหน้าที่เห็นว่า ควรมีการขอความยินยอมจากเจ้าของข้อมูลก่อน ให้ผู้ขอดำเนินการขอความยินยอมจากเจ้าของข้อมูลก่อน

ข้อ ๒๑ ผู้ควบคุมข้อมูล อาจขอให้เจ้าของข้อมูลให้ความยินยอมล่วงหน้าในการเปิดเผยข้อมูลด้านสุขภาพของบุคคล ในกรณีดังต่อไปนี้

(๑) ต่อบุคลากรทางการแพทย์ของผู้ควบคุมข้อมูล ในการปฏิบัติงานในหน้าที่ หรือเพื่อประโยชน์ของเจ้าของข้อมูล

(๒) เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อ หรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลด้านสุขภาพของบุคคลใด

(๓) เป็นการจำเป็นเพื่อการป้องกัน หรือระงับอันตรายต่อชีวิต หรือสุขภาพของบุคคล

(๔) มีเหตุจำเป็นอื่น ๆ เพื่อประโยชน์ของเจ้าของข้อมูล (ถ้ามี)

ในการดำเนินการตามวรรคหนึ่ง ต้องอธิบายให้เจ้าของข้อมูลทราบและเข้าใจด้วย ในกรณีเป็นการศึกษา วิเคราะห์ วิจัยเพื่อการพัฒนาทางด้านสุขภาพของผู้ควบคุมข้อมูลถือเป็นการปฏิบัติงานในหน้าที่และอำนาจของผู้ควบคุมข้อมูลให้สามารถดำเนินการได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล

ข้อ ๒๒ เมื่อได้ดำเนินการจนเสร็จสิ้นแล้ว ให้เก็บเอกสารต่าง ๆ ไว้เป็นหลักฐานด้วย

หมวด ๓

การแก้ไขข้อมูลด้านสุขภาพของบุคคล

ข้อ ๒๓ เจ้าของข้อมูลมีสิทธิที่จะขอให้แก้ไขข้อมูลด้านสุขภาพของตนเอง โดยยื่นคำขอต่อผู้ควบคุมข้อมูลพร้อมพยานหลักฐานแสดงข้อมูลที่ถูกต้องตามความเป็นจริงเมื่อเจ้าหน้าที่ได้ตรวจสอบแล้วเห็นว่าถูกต้องให้เสนอผู้มีอำนาจอนุมัติและทำการแก้ไขข้อมูลดังกล่าวแล้วแจ้งเจ้าของข้อมูลทราบต่อไป

ข้อ ๒๔ เจ้าหน้าที่ผู้เขียนข้อมูลด้านสุขภาพของบุคคลอาจแก้ไขข้อมูลได้ โดยอยู่ในเงื่อนไขดังนี้

(๑) ต้องแก้ไขตามความเป็นจริง

(๒) ไม่ควรแก้ไข โดยลบหรือขีดฆ่าโดยไม่จำเป็น ถ้าต้องการแก้ไขโดยขีดฆ่าต้องเซ็นชื่อกำกับทุกครั้ง

(๓) การเพิ่มเติมแก้ไขทุกครั้งให้เขียนเหตุผลไว้ด้วย โดยอาจมีบันทึกติดไว้กับเวชระเบียน หรือทำรายการไว้ท้ายเวชระเบียนหน้านั้น ๆ

(๔) เมื่อมีการแก้ไขให้มีหัวหน้าหน่วยและผู้ที่อยู่ในเหตุการณ์ลงชื่อเป็นพยานด้วย

(๕) ไม่ควรแก้ไขเมื่อมีการร้องเรียนหรือฟ้องร้องคดีแล้ว

หมวด ๔ ข้อมูลทางอิเล็กทรอนิกส์

ข้อ ๒๕ ผู้ควบคุมข้อมูลและผู้บริหารจัดการข้อมูลที่ดำเนินการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลด้านสุขภาพส่วนบุคคลโดยวิธีการทางอิเล็กทรอนิกส์ต้องมีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ซึ่งเป็นวิธีการที่เชื่อถือได้อย่างน้อยต้องครอบคลุมหัวข้อดังต่อไปนี้

- (๑) การเข้าถึงและควบคุมการใช้งาน โดยต้องมีองค์ประกอบดังนี้
 - (ก) การระบุตัวตน (Identification)
 - (ข) การยืนยันตัวตน (Authentication)
 - (ค) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)
 - (ง) ความรับผิดชอบต่อผลการกระทำ (Accountability)

ทั้งนี้เพื่อให้สามารถยืนยันได้ว่าข้อมูลอิเล็กทรอนิกส์ที่มีการจัดทำหรือแปลงได้ดำเนินการโดยผู้มีสิทธิเข้าถึงเท่านั้น ผู้มีสิทธิในการเข้าถึงดังกล่าวให้หมายความรวมถึงผู้รับผิดชอบดำเนินงานจัดทำหรือแปลงเอกสารหรือข้อความและมีสิทธิตรวจสอบซึ่งจะเป็นคนเดียวกันหรือไม่ก็ได้

(๒) จัดให้มีระบบการใช้งานและระบบสำรองซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติอย่างต่อเนื่อง

- (๓) การตรวจสอบและประเมินความเสี่ยงของระบบที่ใช้อย่างสม่ำเสมอ

ข้อ ๒๖ ในการส่งต่อข้อมูลทางอิเล็กทรอนิกส์ ผู้ควบคุมข้อมูล และผู้บริหารข้อมูลต้องจัดให้มีการบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบการจัดการข้อมูลด้านสุขภาพของบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้วและต้องมีการดำเนินการดังนี้

(๑) ฝึกอบรมสร้างความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักในผลกระทบที่อาจเกิดจากการใช้งานระบบการจัดการข้อมูลด้านสุขภาพของบุคคล รวมถึงการกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) โดยต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบแล้วและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access right) โดยต้องจัดให้มีกระบวนการทบทวนการเข้าถึงสิทธิของผู้ใช้งานระบบการจัดการข้อมูลด้านสุขภาพของบุคคลตามระยะเวลาที่กำหนดไว้

(๖) การป้องกัน...

(๖) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์โดยต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๗) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์โดยต้องควบคุมไม่ให้สินทรัพย์ เช่น เอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

(๘) การควบคุมเครือข่าย (network access control)

(๙) การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

ทั้งนี้ให้เป็นไปตามประกาศนโยบายการรักษาความมั่นคงปลอดภัยของกระทรวงสาธารณสุข ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งมาตรการตามเอกสารหมายเลข ๑ แนบท้ายระเบียบนี้

หมวด ๕

ระเบียบสุขภาพ

ข้อ ๒๗ ระเบียบสุขภาพจัดทำขึ้นเพื่อ

(๑) รวบรวมข้อมูลด้านสุขภาพของบุคคลของประชาชน

(๒) คຸ້มครองข้อมูลด้านสุขภาพของบุคคล

(๓) นำข้อมูลด้านสุขภาพของบุคคลไปใช้ประโยชน์ในการดูแลสุขภาพของ

เจ้าของข้อมูลนั้น

(๔) นำไปศึกษา วิเคราะห์ วิจัย เพื่อพัฒนาระบบสุขภาพของประเทศ

(๕) ให้หน่วยงานที่เกี่ยวข้องสามารถนำข้อมูลด้านสุขภาพของบุคคลไปใช้เพื่อประโยชน์ของเจ้าของข้อมูล และหน่วยงานนั้น

(๖) การอื่นที่คณะกรรมการกำหนด

ข้อ ๒๘ ระเบียบสุขภาพ ประกอบด้วยข้อมูลด้านสุขภาพของบุคคล ทั้งนี้ให้เป็นไปตามเอกสารหมายเลข ๒ แนบท้ายของระเบียบนี้

ข้อ ๒๙ ผู้บริหารจัดการข้อมูลเป็นผู้ดำเนินการบริหารจัดการข้อมูลเพื่อประโยชน์ของเจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องตามหลักเกณฑ์ เงื่อนไข และวิธีการที่คณะกรรมการกำหนด

ข้อ ๓๐ ผู้บริหารจัดการข้อมูลต้องจัดให้มีสถานที่จัดเก็บข้อมูลด้านสุขภาพของบุคคลที่เหมาะสม มีระบบการรักษาความปลอดภัยของการเก็บ การรวบรวม การใช้และการเปิดเผยข้อมูลตามที่คณะกรรมการกำหนด

ข้อ ๓๑ ผู้ควบคุมข้อมูลต้องเป็นผู้ดำเนินการส่งมอบข้อมูลด้านสุขภาพของบุคคลให้ผู้บริหารจัดการข้อมูลเพื่อจัดทำระเบียบสุขภาพรวมทั้งขอความยินยอมจากเจ้าของข้อมูลตามแบบที่กำหนดท้ายระเบียบนี้หรือตามที่คณะกรรมการกำหนด

ในกรณีเจ้าของข้อมูลไม่ยินยอมให้บันทึกไว้เป็นหลักฐานด้วย

ข้อ ๓๒ ผู้ควบคุมข้อมูลมีหน้าที่ต้องตรวจสอบและบันทึกข้อมูลให้เป็นปัจจุบันเสมอและ
ส่งมอบให้ผู้บริหารจัดการข้อมูลภายในเวลาที่กำหนด

ข้อ ๓๓ ผู้บริหารจัดการข้อมูลต้องจัดให้มีทะเบียนผู้ควบคุมข้อมูลและผู้รับข้อมูลการ
จัดการข้อมูลตามหลักเกณฑ์ วิธีการ และเงื่อนไขการใช้งานข้อมูลด้านสุขภาพของบุคคลที่คณะกรรมการกำหนด

ข้อ ๓๔ เมื่อผู้รับข้อมูลได้รับข้อมูลและใช้ประโยชน์แล้ว ต้องส่งข้อมูลด้านสุขภาพของ
บุคคลที่เป็นปัจจุบันของเจ้าของข้อมูลไปให้ผู้บริหารจัดการข้อมูลเพื่อเก็บรวบรวม และใช้ประโยชน์ตามที่
ระเบียบนี้กำหนดไว้ต่อไป

ข้อ ๓๕ ให้ปลัดกระทรวงสาธารณสุขเป็นผู้รักษาการตามระเบียบนี้

ประกาศ ณ วันที่ ๒๘ เดือน มีนาคม พ.ศ. ๒๕๖๑



(นายปิยะสกล สกลสัตยาทร)

รัฐมนตรีว่าการกระทรวงสาธารณสุข