



ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๔

โดยที่เป็นการสมควรปรับปรุงแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานหลักประกันสุขภาพแห่งชาติ ให้เป็นไปพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดหลักเกณฑ์ กลไก และมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปไว้

อาศัยอำนาจตามความในมาตรา ๓๖ วรรคหนึ่ง (๒) แห่งพระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. ๒๕๔๕ ประกอบมาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานหลักประกันสุขภาพแห่งชาติ และให้หมายความรวมถึงสำนักงานสาขาด้วย

“เลขาธิการ” หมายความว่า เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ

“ผู้ปฏิบัติงาน” หมายความว่า ผู้ปฏิบัติงานตามข้อบังคับคณะกรรมการหลักประกันสุขภาพแห่งชาติ ว่าด้วยการบริหารงานบุคคล

“แนวนโยบาย” หมายความว่า หลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานกำหนดขึ้นและประกาศใช้งาน

“แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานกำหนดขึ้นและประกาศใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

“บุคคล” หมายความว่า บุคคลธรรมดา

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“เจ้าของข้อมูล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลหรือผู้มีสิทธิโดยชอบตามกฎหมาย “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า สำนักงานซึ่งเป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลซึ่งมีหน้าที่ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งการเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล ให้เป็นไปตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด ทั้งนี้ บุคคลดังกล่าวไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า ผู้ปฏิบัติงานหรือบุคคลภายนอก ซึ่งเป็นผู้มีความรู้ด้านกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

“ข้อมูลนิรนาม” หมายความว่า ข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

“การประมวลผลข้อมูลส่วนบุคคล” หมายความว่า การดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยระบบอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดเก็บ การใช้ เปลี่ยนแปลงเปิดเผย ส่งต่อ ทำลาย ทำให้เป็นข้อมูลนิรนาม หรือดำเนินการอื่นใดต่อข้อมูลดังกล่าว

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า เหตุการณ์ใด ๆ ที่ทำให้เกิดการสูญหาย การเข้าถึง การใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิได้รับอนุญาตตามกฎหมาย

ข้อ ๔ แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ประกอบด้วย

- (๑) การกำหนด และแยกแยะข้อมูลส่วนบุคคล
- (๒) การนำข้อมูลส่วนบุคคลไปใช้ หรือการประมวลผลข้อมูลส่วนบุคคล
- (๓) แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- (๔) แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- (๕) แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์กรระหว่างประเทศ

(๖) แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม

ข้อ ๕ ในกรณีที่กฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยการดำเนินงานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นอย่างอื่น ให้ถือปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการนั้น

ข้อ ๖ การกำหนด และแยกแยะข้อมูลส่วนบุคคล ประกอบด้วย

- (๑) การกำหนดความหมาย และขอบเขตของข้อมูลส่วนบุคคล
- (๒) การตรวจสอบข้อมูลส่วนบุคคล
- (๓) แหล่งที่มาความเชื่อมโยง และเส้นทางของข้อมูลส่วนบุคคลในสำนักงาน
- (๔) การกำหนดความเสี่ยงของข้อมูลส่วนบุคคล
- (๕) การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล
- (๖) ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ

ข้อ ๗ การนำข้อมูลส่วนบุคคลไปใช้ หรือการประมวลผลข้อมูลส่วนบุคคล ต้องดำเนินการภายใต้
ฐานทางกฎหมาย ดังต่อไปนี้

- (๑) ฐานความยินยอม
- (๒) ฐานสัญญา
- (๓) ฐานประโยชน์สำคัญต่อชีวิต
- (๔) ฐานภารกิจของรัฐ
- (๕) ฐานประโยชน์อันชอบธรรม
- (๖) ฐานการปฏิบัติตามกฎหมาย
- (๗) ฐานเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยหรือสถิติ

ข้อ ๘ ให้มีแนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผล
ข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนี้

- (๑) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมข้อมูลส่วนบุคคล
- (๒) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ประมวลผลข้อมูลส่วนบุคคล
- (๓) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้เป็นเจ้าหน้าที่คุ้มครองข้อมูล

ส่วนบุคคล

(๔) แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล
และผู้ประมวลผลข้อมูลส่วนบุคคล

(๕) แนวปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคลในการรับคำร้องขอตามสิทธิของเจ้าของ
ข้อมูลส่วนบุคคล

- (๖) แนวปฏิบัติตามคำร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- (๗) แนวปฏิบัติของผู้ประมวลผลข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ
- (๘) แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ
- (๙) แนวปฏิบัติเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล
- (๑๐) ความรับผิดชอบทางแพ่ง ความรับผิดชอบทางอาญา และโทษทางปกครอง

ข้อ ๙ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล มีขั้นตอนที่จะต้องพิจารณา ดังนี้

- (๑) ขอบเขตการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- (๒) ขั้นตอนของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๑๐ การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องเป็นไป
ตามหลักเกณฑ์และเงื่อนไขว่าประเทศปลายทางหรือองค์การระหว่างประเทศนั้น มีมาตรฐานการคุ้มครอง
ข้อมูลส่วนบุคคลที่เพียงพอ หรือไม่

ข้อ ๑๑ เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูล
ส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ให้กำหนดมาตรการหรือกระบวนการป้องกันการละเมิด
ข้อมูลส่วนบุคคล ให้จัดทำเป็นข้อมูลนิรนาม

ข้อ ๑๒ เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน เป็นไปอย่าง
มีประสิทธิภาพ และสามารถปฏิบัติได้อย่างเป็นรูปธรรม ให้แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
ของสำนักงาน เป็นไปตามรายละเอียดที่กำหนดไว้แนบท้ายประกาศนี้

ข้อ ๑๓ ในกรณีที่เจ้าของข้อมูล มีข้อสงสัย ข้อเสนอแนะ หรือข้อติชมใด ๆ เกี่ยวกับ
นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลตามประกาศนี้ สามารถติดต่อได้ที่
ผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สำนักงานหลักประกันสุขภาพแห่งชาติ
เลขที่ ๑๒๐ ชั้น ๒-๔ หมู่ ๓ อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม
๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ โทรศัพท์ ๐๒ ๑๔๑ ๔๐๐๐
โทรสาร ๐๒ ๑๔๑ ๙๗๓๐ - ๑ เว็บไซต์ : www.nhso.go.th

ข้อ ๑๔ ให้ส่วนงานภายในสำนักงานที่เกี่ยวข้อง ในการรวบรวม การจัดเก็บ การใช้ เผย และดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคล เป็นผู้รับผิดชอบในการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคลที่ตนจัดเก็บตามประกาศนี้โดยเคร่งครัด

ข้อ ๑๕ ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานให้ความเห็นและข้อเสนอแนะเกี่ยวกับการทบทวนแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๖ กรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการเป็นผู้มีอำนาจวินิจฉัยชี้ขาด โดยอาจมอบหมายให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเสนอความเห็นประกอบการพิจารณาก่อนก็ได้

ประกาศ ณ วันที่ ๑ เมษายน พ.ศ. ๒๕๖๙

เวลาดำเนินการ: 2026-04-01 12:57
ลงนามโดย: จเด็จ ธรรมธัชอารี
หมายเลขเอกสาร: 9e8d-29e4-08a0

8/10/20

(นายจเด็จ ธรรมรัชอารี)

เลขานุการสำนักงานหลักประกันสุขภาพแห่งชาติ