



ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน
พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานหลักประกันสุขภาพแห่งชาติ ให้เป็นไปพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดหลักเกณฑ์ กலை และมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปไว้

อาศัยอำนาจตามความในมาตรา ๓๑ วรรคหนึ่ง และมาตรา ๓๖ (๒) แห่งพระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. ๒๕๔๕ ประกอบมาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ เมษายน พ.ศ. ๒๕๖๕ เป็นต้นไป

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 ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

/“เจ้าของข้อมูล” ...

“เจ้าของข้อมูล” หมายความว่า บุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลหรือผู้มีสิทธิโดยชอบตามกฎหมาย

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า สำนักงานซึ่งเป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลซึ่งมีหน้าที่ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลตามรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” การเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลกำหนด ทั้งนี้ บุคคลดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า ผู้ปฏิบัติงานหรือบุคคลภายนอกซึ่งเป็นผู้มีความรู้ด้านกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

“ข้อมูลนิรนาม” หมายความว่า ข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

ข้อ ๔ แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานประกอบด้วย

- (๑) การกำหนดและแยกแยะข้อมูลส่วนบุคคล
- (๒) การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล
- (๓) แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- (๔) แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- (๕) แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ

(๖) แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม

ข้อ ๕ ในกรณีที่กฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล การดำเนินงานธุรกรรมทางอิเล็กทรอนิกส์ กำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นอย่างอื่น ให้ถือปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการนั้น

ข้อ ๖ การกำหนดและแยกแยะข้อมูลส่วนบุคคล ประกอบด้วย

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

ข้อ ๗ การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล จะต้องขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล ภายใต้หลักการดังต่อไปนี้

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

ข้อ ๘ ให้มีแนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนี้

- (๑) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมข้อมูลส่วนบุคคล
- (๒) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ประมวลผลข้อมูลส่วนบุคคล
- (๓) แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- (๔) แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผล

ข้อมูลส่วนบุคคล

- (๕) แนวปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคลในการรับคำร้องขอตามสิทธิของเจ้าของข้อมูล

ส่วนบุคคล

- (๖) แนวปฏิบัติตามคำร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- (๗) แนวปฏิบัติของผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ
- (๘) แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ
- (๙) ความรับผิดชอบทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

ข้อ ๙ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล มีขั้นตอนที่จะต้องพิจารณาดังนี้

- (๑) ขอบเขตการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- (๒) ขั้นตอนของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๑๐ การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ จะต้องเป็นไปตามหลักเกณฑ์ และเงื่อนไขว่าประเทศปลายทางหรือองค์การระหว่างประเทศนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หรือไม่

ข้อ ๑๑ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้กำหนดมาตรการหรือกระบวนการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยจัดทำเป็นข้อมูลนิรนาม

ข้อ ๑๒ เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน เป็นไปอย่างมีประสิทธิภาพและสามารถปฏิบัติได้อย่างเป็นรูปธรรม ให้แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน เป็นไปตามรายละเอียดที่กำหนดไว้แนบท้ายประกาศนี้

ข้อ ๑๓ ในกรณีที่เจ้าของข้อมูล มีข้อสงสัย ข้อเสนอแนะ หรือข้อติชมใด ๆ เกี่ยวกับแนวนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน สามารถติดต่อได้ที่ ผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 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 ๘๗๓๐-๑ เว็บไซต์ : www.nhso.go.th

ข้อ ๑๔ ให้ส่วนงานภายในสำนักงานที่เกี่ยวข้องในการรวบรวม จัดเก็บ ใช้ เปิดเผย และดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคล เป็นผู้รับผิดชอบในการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคลที่ตนจัดเก็บตามประกาศนี้โดยเคร่งครัด

ข้อ ๑๕ ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ทบทวนแนวนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ให้เป็นปัจจุบันอย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๑๖ กรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการเป็นผู้มีอำนาจ วินิจฉัยชี้ขาดโดยอาจมอบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานพิจารณาเสนอความเห็น ก่อนก็ได้

ประกาศ ณ วันที่ ๑๓ เมษายน พ.ศ. ๒๕๖๕

www.nhso.go.th
โทรสาร ๐๒ ๑๔๑ ๘๗๓๐-๑
โทรเลข ๐๒ ๑๔๑ ๘๗๓๐-๑
www.nhso.go.th



(นายจเด็จ ธรรมธัชอารี)

เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ