กฎหมายว่าด้วยการเคลื่อนย้ายและความรับผิดชอบในการประกันสุขภาพ (Health Insurance Portability and Accountability Act : HIPAA) ของประเทศสหรัฐอเมริกา*

ภรภัทร ปัญญวานิช**

บทนำ

กฎหมายว่าด้วยการเคลื่อนย้ายและความรับผิดชอบในการประกันสุขภาพ (Health Insurance Portability and Accountability Act : HIPAA) เป็นกฎหมายของรัฐบาลกลาง[๑]ที่กำหนดให้ต้องมีการสร้างมาตรฐานระดับสากลเพื่อปกป้องคุ้มครองข้อมูลด้านสุขภาพที่ละเอียดอ่อนของผู้ป่วยจากการถูกเปิดเผยโดยไม่ได้รับความยินยอมจากผู้ป่วย โดยกระทรวงสาธารณสุขและบริการประชาชนของสหรัฐอเมริกา (Health and Human Services: HHS) ได้ออกมาตรการด้านความเป็นส่วนตัว (HIPAA Privacy Rule) เพื่อดำเนินการตามข้อกำหนดและปกป้องคุ้มครองข้อมูลที่อยู่ในความคุ้มครองของมาตรการดังกล่าว

HIPAA Privacy Rule

HIPAA กล่าวถึงการใช้และการเปิดเผยข้อมูลสุขภาพที่ได้รับการคุ้มครองของแต่ละบุคคล (Protected Health Information หรือ PHI) สำหรับหน่วยงานที่อยู่ภายใต้มาตรการดังกล่าวซึ่ง HIPAA มีมาตรฐานสำหรับสิทธิส่วนบุคคลในการรับรู้และควบคุมการใช้ข้อมูลสุขภาพของพวกเขา โดยเป้าหมายหลักของ HIPAA คือการทำให้มั่นใจได้ว่าข้อมูลด้านสุขภาพของผู้ป่วยแต่ละคนจะได้รับการคุ้มครองอย่างเหมาะสม ในขณะที่อนุญาตให้มีการใช้ข้อมูลด้านสุขภาพเท่าที่จำเป็นเพื่อการส่งเสริมการดูแลสุขภาพให้มีคุณภาพที่ดีและเพื่อปกป้องสุขภาพและความเป็นอยู่ที่ดีของประชาชน

ความหมายของข้อมูลสุขภาพที่ได้รับการคุ้มครอง (Protected Health Information หรือ PHI)

HIPAA กำหนดวิธีในการควบคุมการใช้และเปิดเผยข้อมูลที่เป็นความลับของผู้ป่วย หรือที่เรียกว่าข้อมูล PHI โดยครอบคลุมทั้งการเขียนเป็นลายลักษณ์อักษร การพูด หรือการเผยแพร่ผ่านระบบอิเล็กทรอนิกส์และรวมถึงข้อมูลเกี่ยวกับสุขภาพหรือสภาวะของแต่ละบุคคล การให้บริการด้านสุขภาพ หรือการชำระ

---

* บทความนี้เผยแพร่เมื่อเดือนเมษายน ๒๕๖๖ สรุปความจากบทความ HIPAA Basics Overview โดย University of Wisconsin-Milwaukee เข้าถึงต้นฉบับได้ที่ https://uwm.edu/hipaa/overview/hipaa-basics-overview/

** บุคลากรจัดทำฐานข้อมูลกฎหมาย ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

๑ Mathias Ahlgren. “การปฏิบัติตาม HIPAA คืออะไร?” . สืบค้นเมื่อวันที่ ๒๓ เมษายน ๒๕๖๖, จาก https://www.websiterating.com/th/cloud-storage/glossary/what-is-hipaa-compliance/

ค่าบริการดังกล่าว ซึ่งการคุ้มครองข้อมูลของ HIPAA ครอบคลุมเฉพาะข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ทั้งนี้ ตัวอย่างข้อมูลที่ได้รับการกำหนดไว้โดยทั่วไปภายใต้ HIPAA เช่น ชื่อของผู้ป่วย ที่อยู่ หมายเลขประกันสังคม หมายเลขโทรสาร ที่อยู่อีเมล วันที่รับเข้าหรือออกจากโรงพยาบาล รูปถ่ายและการบันทึกเสียง นอกจากนี้ PHI ยังรวมถึงข้อมูลซึ่งอาจคาดหมายได้ว่าจะนำไปสู่การระบุตัวตนของบุคคลใดบุคคลหนึ่งอีกด้วย อย่างไรก็ตาม ข้อกำหนดของ HIPAA จะไม่ถูกนำมาบังคับใช้กับเอกสารหรือข้อมูลใด ๆ ที่ไม่ได้ระบุถึงข้อมูลส่วนบุคคลของผู้ป่วย แต่หากเอกสารหรือข้อมูลดังกล่าวเป็นที่สงสัยว่ามีการระบุถึงข้อมูลส่วนบุคคลของผู้ป่วย ให้ถือว่าเอกสารหรือข้อมูลนั้น ๆ ได้รับการคุ้มครองภายใต้ข้อกำหนดของ HIPAA ทั้งสิ้น

สาระสำคัญของ HIPAA

๑. การใช้และเปิดเผยข้อมูลเท่าที่จำเป็น

โดยทั่วไปแล้ว HIPAA กำหนดให้จำกัดการเข้าถึงข้อมูล PHI รวมถึงการใช้และการเปิดเผย ให้เป็นไปเพียงเท่าที่จำเป็นต่อการปฏิบัติงานหรือบรรลุวัตถุประสงค์ในการดำเนินงานเท่านั้น

๒. การปฏิบัติตามข้อกำหนด HIPAA เพื่อปกป้องข้อมูล PHI

HIPAA กำหนดให้บุคคลที่ทำงานให้กับหน่วยงานด้านการดูแลสุขภาพที่อยู่ภายใต้การควบคุมของ HIPAA ต้องปฏิบัติตามมาตรการในการปกป้องคุ้มครองข้อมูล PHI ตัวอย่างของแนวทางปฏิบัติทั่วไปเพื่อปกป้องข้อมูล PHI ของผู้ป่วยมีดังต่อไปนี้

- จัดเก็บบันทึกข้อมูลประวัติผู้ป่วยเมื่อไม่ใช้งาน
- จัดเก็บข้อมูล PHI ในสถานที่ปลอดภัยและมีการป้องกันการเข้าถึงที่เหมาะสม
- นำเอกสารออกจากเครื่องแฟกซ์หรือเครื่องถ่ายเอกสารทันที
- การกำจัดเอกสารที่เป็นความลับต้องใช้เครื่องทำลายเอกสารโดยเฉพาะ
- พยายามป้องกันไม่ให้ผู้อื่นได้ยินการสนทนาของเจ้าหน้าที่เมื่อกล่าวถึงผู้ป่วย

๓. การเปิดเผยข้อมูล PHI จำเป็นต้องได้รับความยินยอมจากผู้ป่วยและให้โอกาสผู้ป่วยในการคัดค้าน

ในกรณีต่อไปนี้ ผู้ป่วยต้องได้รับโอกาสในการคัดค้านการใช้หรือเปิดเผยข้อมูล PHI ของตนก่อน ได้แก่

- การเก็บรวบรวมข้อมูลผู้ป่วย เช่น ชื่อ หมายเลขห้องพิเศษ อาการ และศาสนา
- การแบ่งปันข้อมูลกับเพื่อน ครอบครัว หรือคนอื่นๆ ที่เกี่ยวข้องในการดูแลผู้ป่วยเกี่ยวกับอาการหรือสภาพทั่วไปของผู้ป่วย

๔. กรณียกเว้นที่การใช้และการเปิดเผยข้อมูล PHI ไม่จำเป็นต้องได้รับอนุญาตจากผู้ป่วย

การใช้และการเปิดเผยข้อมูล PHI ที่ไม่จำเป็นต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วย เช่น การปฏิบัติหน้าที่ประจำวันของเจ้าหน้าที่ในการรักษา การชำระเงิน และการดำเนินงานด้านการดูแลสุขภาพ ซึ่งเรียกรวมกันว่า “TPO”

- Treatment (การรักษา) ไม่จำเป็นต้องได้รับอนุญาตจากผู้ป่วยเพื่อใช้หรือเปิดเผยข้อมูลของผู้ป่วยเมื่อทำการรักษาผู้ป่วยหรือเตรียมการรักษาผู้ป่วย
- Payment (การชำระเงิน) ไม่จำเป็นต้องได้รับอนุญาตจากผู้ป่วยเพื่อใช้หรือเปิดเผยข้อมูลของผู้ป่วยเมื่อจัดทำใบเรียกเก็บเงินหรือประสานงานการเรียกเก็บเงินกับบริษัทประกันสุขภาพของผู้ป่วย
- Health Care Operations (การดำเนินงานด้านการดูแลสุขภาพ) ไม่จำเป็นต้องได้รับอนุญาตในการดำเนินงาน เช่น การให้คำแนะนำโดยแพทย์หรือผู้เชี่ยวชาญด้านสุขภาพ การปฏิบัติตามข้อกำหนดด้านใบอนุญาตและการรับรองและการตรวจสุขภาพ

เจ้าหน้าที่และผู้ให้บริการด้านสุขภาพยังสามารถเปิดเผยข้อมูล PHI ของผู้ป่วยโดยไม่ต้องได้รับอนุญาตจากผู้ป่วยสำหรับวัตถุประสงค์ด้านสาธารณสุขบางอย่างตามที่กฎหมายกำหนด หรือเพื่อวัตถุประสงค์ในการจ้างงานหรือการจ่ายค่าตอบแทนของพนักงาน

๕. การใช้งานและการเปิดเผยข้อมูล PHI ที่จำเป็นต้องได้รับอนุญาตเป็นลายลักษณ์อักษร

โดยทั่วไปการใช้และการเปิดเผยข้อมูล PHI ทั้งหมดนอกเหนือจากที่ระบุไว้ในข้อ ๓ และข้อ ๔ ข้างต้นต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วย ตัวอย่างของการใช้และการเปิดเผยดังกล่าวมีดังต่อไปนี้

- กิจกรรมการวิจัย
- กิจกรรมทางการตลาดและการระดมทุน
- การเปิดเผยบันทึกการบำบัดทางจิต
- การเปิดเผยข้อมูล PHI ต่อบุคคลที่สามหรือหน่วยงานภายนอก

๖. สิทธิความเป็นส่วนตัวของผู้ป่วย

HIPAA ให้สิทธิเกี่ยวกับข้อมูล PHI ของผู้ป่วย ดังต่อไปนี้

- สิทธิในการเลือกช่องทางการติดต่อสื่อสาร ผู้ป่วยสามารถขอให้ผู้ให้บริการด้านสุขภาพและเจ้าหน้าที่ติดต่อผู้ป่วยด้วยวิธีใดวิธีหนึ่ง เช่น ที่บ้านแทนที่ทำงาน
- สิทธิในการขอดูและรับสำเนาเวชระเบียนและการเรียกเก็บเงินของตน
- สิทธิในการขอเปลี่ยนแปลงประวัติการรักษาพยาบาลและการเรียกเก็บเงิน
- สิทธิที่จะได้รับการเปิดเผยข้อมูลที่ร้องขอ

- สิทธิในการร้องขอให้จำกัดในการใช้และเปิดเผยข้อมูลของผู้ป่วย ซึ่งผู้ให้บริการด้านสุขภาพไม่จำเป็นต้องยอมรับคำขอดังกล่าวในทุกกรณีและจะต้องไม่ยอมรับข้อจำกัดดังกล่าวที่ได้รับการร้องขอโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบที่เกี่ยวข้องก่อน
- สิทธิในการได้รับประกาศเกี่ยวกับแนวทางปฏิบัติด้านความเป็นส่วนตัว ผู้ป่วยทุกรายจะต้องได้รับสำเนาประกาศเกี่ยวกับแนวทางปฏิบัติด้านความเป็นส่วนตัวและรับทราบการแจ้งดังกล่าว

๗. ข้อกำหนดที่หน่วยงานด้านการดูแลสุขภาพต้องปฏิบัติตาม

HIPAA กำหนดให้หน่วยงานด้านการดูแลสุขภาพต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

- บุคลากรทุกคนที่เกี่ยวข้องต้องได้รับการฝึกอบรม HIPAA ขั้นพื้นฐาน
- มีการกำหนดขั้นตอนในการปฏิบัติตาม HIPAA ที่ชัดเจน
- มีขั้นตอนในการรับฟังและดำเนินการด้านข้อร้องเรียนเกี่ยวกับความเป็นส่วนตัวของผู้ป่วยโดยทั่วไปและประกาศแนวปฏิบัติด้านความเป็นส่วนตัวเพื่อให้ผู้ป่วยทราบว่าพวกเขาสามารถแจ้งข้อร้องเรียนได้อย่างไร
- กำหนดบทลงโทษสำหรับบุคลากรที่ละเมิด HIPAA
- แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสำหรับ HIPAA ตั้งแต่หนึ่งคนขึ้นไป

๘. คู่ค้าทางธุรกิจต้องปฏิบัติตาม HIPAA ด้วยเช่นกัน

ธุรกิจที่ให้บริการแก่ผู้ให้บริการด้านการดูแลสุขภาพโดยการช่วยเหลือด้านการรักษา การชำระเงินหรือหน้าที่อื่นๆ จะต้องปฏิบัติตามข้อกำหนดของ HIPAA ตัวอย่างเช่น หน่วยงานหรือแผนกหนึ่งในองค์กรอาจทำหน้าที่เป็นคู่ค้าทางธุรกิจให้กับหน่วยงานภายนอก

๙. ข้อควรปฏิบัติเมื่อมีเหตุละเมิดต่อข้อมูลส่วนบุคคลเกิดขึ้น

บุคคลใดก็ตามที่ทำงานในแผนกที่เกี่ยวข้องหรือคู่ค้าทางธุรกิจ หากมีเหตุสงสัยว่ามีการได้มา การเข้าถึง ใช้ หรือเปิดเผยข้อมูล PHI โดยไม่ได้รับอนุญาตภายใต้ HIPAA ควรรายงานสถานการณ์ของการละเมิดที่น่าสงสัยต่อหัวหน้างานของบุคคลนั้นและรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสำหรับแผนกนั้นในทันที

จากนั้นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังกล่าวจะต้องรวบรวมข้อเท็จจริงเกี่ยวกับเหตุการณ์และรายงานเหตุการณ์ดังกล่าวต่อเจ้าหน้าที่ของทางการตามที่ระบุไว้ในนโยบายและข้อกำหนดของ HIPAA เจ้าหน้าที่ดังกล่าวจะหารือเกี่ยวกับสถานการณ์ของการละเมิดที่ถูกรายงานและกำหนดขั้นตอนที่เจ้าหน้าที่ของหน่วยงานผู้แจ้งเรื่องจะต้องปฏิบัติ รวมถึงขอบเขตของในการสอบสวนข้อเท็จจริงเกี่ยวกับเหตุละเมิดที่เกิดขึ้นตามสมควรและแจ้งเตือนไปยังผู้ที่เกี่ยวข้อง

****