คำสั่งสถาบันการแพทย์แผนไทย
ที่ ๒ /๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานควบคุมข้อมูลส่วนบุคคล สถาบันการแพทย์แผนไทย

---

ตามคำสั่งกรมการแพทย์แผนไทยและการแพทย์ทางเลือก ที่ ๗๖๔/๒๕๖๗ ลงวันที่ ๒๔ เมษายน พ.ศ. ๒๕๖๗ ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนของตนในกรณี (๑) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (๒) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด และ (๓) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖ ซึ่งสถาบันการแพทย์แผนไทย มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้การดำเนินงานคุ้มครองข้อมูลส่วนบุคคลของสถาบันการแพทย์แผนไทย เป็นไปด้วยความเรียบร้อย นั้น

อาศัยอำนาจตามความในมาตรา ๓๓ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ผู้อำนวยการสถาบันการแพทย์แผนไทย จึงได้ออกคำสั่งแต่งตั้งคณะทำงานควบคุมข้อมูลส่วนบุคคลคลสถาบันการแพทย์แผนไทย โดยมีองค์ประกอบ หน้าที่ และอำนาจ ดังต่อไปนี้

ข้อ ๑ องค์ประกอบ

| | | |
|---|---|---|
| ๑.๑ | ผู้อำนวยการสถาบันการแพทย์แผนไทย | ที่ปรึกษา |
| ๑.๒ | นางนันท์นภัส ต้อยติ่ง<br>นักวิชาการสาธารณสุขชำนาญการพิเศษ | ประธาน |
| ๑.๓ | นางอัจฉรา เชียงทอง<br>นักวิชาการสาธารณสุขชำนาญการพิเศษ | รองประธาน |
| ๑.๔ | นางมาลา สร้อยสำโรง<br>แพทย์แผนไทยชำนาญการพิเศษ | รองประธาน |
| ๑.๕ | นายศุภจิต แพจุ้ย<br>นักวิชาการสาธารณสุขชำนาญการ<br>กลุ่มงานวิชาการเภสัชกรรมไทย | คณะทำงาน |
| ๑.๖ | นายนิเวศน์ บวรกุลวัฒน์<br>แพทย์แผนไทยชำนาญการ<br>กลุ่มงานวิชาการการนวดไทย | คณะทำงาน |

๑.๗ นางสาวกัลยาณี...

๑.๗ นางสาวกัลยาณี กฤษณกาศ คณะทำงาน
แพทย์แผนไทยชำนาญการ
กลุ่มงานวิชาการสมุนไพรไทย

๑.๘ นางสาววไลรัตน์ ศิริวงศ์ คณะทำงาน
แพทย์แผนไทยปฏิบัติการ
กลุ่มงานวิชาการเวชกรรมไทย

๑.๙ นายเธียรธรรม อภิจรรยาธรรม คณะทำงาน
แพทย์แผนไทยปฏิบัติการ
กลุ่มงานวิชาการการผดุงครรภ์ไทย

๑.๑๐ นายจตุพร สุกิตติวงศ์ คณะทำงาน
แพทย์แผนไทยปฏิบัติการ
กลุ่มงานพัฒนามาตรฐานบริการการแพทย์แผนไทย

๑.๑๑ นายตรีภพ เฉลิมพร คณะทำงาน
แพทย์แผนไทยปฏิบัติการ
กลุ่มงานส่งเสริมบริการการแพทย์แผนไทย

๑.๑๒ นายธนดล มางาม คณะทำงาน
นักวิชาการสาธารณสุขปฏิบัติการ
กลุ่มงานพัฒนามาตรฐานกำลังคนด้านการแพทย์แผนไทย

๑.๑๓ นางสาวรุ่งทิพย์ เลาะวิถี คณะทำงาน
นักวิชาการสาธารณสุขปฏิบัติการ
กลุ่มงานส่งเสริมการใช้ผลิตภัณฑ์สมุนไพร

๑.๑๔ นางสาวเพ็ญผกา จันทร์กล้า คณะทำงาน
แพทย์แผนไทย
กลุ่มงานพัฒนามาตรฐานยาแผนไทย

๑.๑๕ นางปภาภัทร พุกะนัดด์ คณะทำงาน
หัวหน้ากลุ่มงานอำนวยการ และเลขานุการ

๑.๑๖ นางสาวประกายพร วงศ์มอก คณะทำงาน
เจ้าพนักงานธุรการ และผู้ช่วยเลขานุการ
กลุ่มงานอำนวยการ

ข้อ ๒ หน้าที่และอำนาจ

๒.๑ ศึกษาและทำความเข้าใจกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๒.๒ กำหนดกรอบแนวทาง และรูปแบบในการจัดทำแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

๒.๓ สำรวจ...

๒.๓ สำรวจ วิเคราะห์ และตรวจสอบการบันทึกรายการของกิจกรรมข้อมูลส่วนบุคคล (Records of Processing Activity : ROPA) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานให้ถูกต้องและเป็นปัจจุบัน

๒.๔ ติดต่อประสานงานภายในหน่วยงาน ให้มีการดำเนินงานที่ถูกต้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งให้คำแนะนำแก่หน่วยงานที่เกี่ยวข้อง

๒.๕ สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

๒.๖ ปฏิบัติงานอื่น ๆ ตามที่อธิบดีกรมการแพทย์แผนไทยและการแพทย์ทางเลือกมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๗

(นายสมศักดิ์ กรีชัย)
ผู้อำนวยการสถาบันการแพทย์แผนไทย

# มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของสถาบันการแพทย์แผนไทย พ.ศ. ๒๕๖๗

ตามมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้มีประกาศ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ทั้งนี้กระทรวงสาธารณสุขได้ประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕ เมื่อวันที่ ๒๓ มีนาคม ๒๕๖๕ เพื่อการดำเนินงานเป็นไปตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สถาบันการแพทย์แผนไทย จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสถาบันการแพทย์แผนไทย เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสถาบันการแพทย์แผนไทย พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

“บุคลากรของสถาบันการแพทย์แผนไทย” หมายความว่า บุคลากรทั้งปวงในสถาบันการแพทย์แผนไทย และให้หมายความถึงที่ปรึกษาและคณะกรรมการต่างๆ ของสถาบันการแพทย์แผนไทย ด้วย
“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๓ บุคลากรของสถาบันการแพทย์แผนไทย ต้องตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมการแพทย์แผนไทยและการแพทย์ทางเลือก พ.ศ. ๒๕๖๗ และประกาศนี้อย่างเคร่งครัด

ข้อ ๔ สถาบันการแพทย์แผนไทย ได้จัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งแบ่งออกเป็นมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) ทั้งนี้ มาตรการรักษาความมั่นคงปลอดภัย คลอบคลุมการดำเนินการ ดังต่อไปนี้

การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

การบริหารจัดการในการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล (audit trails) ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๕ สถาบันการแพทย์แผนไทย ได้จัดทำมาตรการรักษาความมั่นคงปลอดภัย ซึ่งแบ่งออกเป็น มาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม และมาตรการทางกายภาพ (physical measures) ที่จำเป็น โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ ๖ สถาบันการแพทย์แผนไทย ได้จัดทำรายละเอียดของมาตรการรักษาความมั่นคงปลอดภัย โดยได้กำหนดการดำเนินการตามมาตรการดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุ เมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

ข้อ ๗ สถาบันการแพทย์แผนไทย ได้กำหนดให้การดำเนินการใด ๆ ภายใต้มาตรการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ในประกาศนี้ จะต้องคำนึงถึงความสามารถในการธำรงไว้ ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๘ สถาบันการแพทย์แผนไทย ได้กำหนดให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ในประกาศนี้ ทั้งนี้ รูปแบบอิเล็กทรอนิกส์ดังกล่าวจะครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์

และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยง ในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัย ในบางสถานการณ์

ข้อ ๙ สถาบันการแพทย์แผนไทย ได้กำหนดให้การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ประกอบกัน

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need -to -know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de -registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๑๐ สถาบันการแพทย์แผนไทย ได้กำหนดให้มีการสร้างเสริมความตระหนักรู้ ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากรของกรมการแพทย์แผนไทยและการแพทย์ทางเลือกหรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวมใช้ เปลี่ยนแปลง แก้ไข ลบ

หรือเปิดเผยข้อมูลส่วนบุคคลทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการที่กำหนดไว้ในประกาศนี้ด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๑๑ สถาบันการแพทย์แผนไทย ได้กำหนดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลมมีการดำเนินการ ดังต่อไปนี้

มีการติดตามเป็นระยะว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

กรณีที่เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ต่อผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ

การศึกษาวิจัยหรือสถิติ

เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและ การให้บริการด้านสังคมสงเคราะห์

การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ข้อ ๑๒ สถาบันการแพทย์แผนไทย จะพิจารณาทบทวนมาตรการรักษาความมั่นคงปลอดภัย ที่กำหนดไว้ในประกาศนี้ในกรณีมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคง ปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน

ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็น ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยง ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๑๓ สถาบันการแพทย์แผนไทย จะจัดให้มีข้อตกลงระหว่างสถาบันการแพทย์แผนไทยในฐานะผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล ให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง ให้ผู้ประมวลผลข้อมูลส่วนบุคคล แจ้งให้สถาบันการแพทย์แผนไทย ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อ ๑๔ สถาบันการแพทย์แผนไทย ประกาศแนวปฏิบัติเพื่อกำหนดรายละเอียดการปฏิบัติตามมาตรการรักษาความมั่งคงปลอดภัยที่กำหนดไว้ในประกาศนี้

(นายสมศักดิ์ กรีชัย)
ผู้อำนวยการสถาบันการแพทย์แผนไทย
ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๗