



คลินิกทันตกรรมกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: หน้าที่ทางกฎหมาย ความเสี่ยง และโอกาสในการสร้างความเชื่อถือจากผู้รับบริการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA เป็นกฎหมายกลางที่กำหนดหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและกำหนดความรับผิดชอบขององค์กรที่ประมวลผลข้อมูลเหล่านั้น สำหรับคลินิกทันตกรรม กฎหมายฉบับนี้มีความสำคัญเป็นพิเศษ เนื่องจากการให้บริการทางทันตกรรมย่อมเกี่ยวข้องกับข้อมูลส่วนบุคคลหลายประเภท ทั้งข้อมูลระบุตัวบุคคล ข้อมูลการติดต่อ ข้อมูลการชำระเงิน และโดยเฉพาะข้อมูลสุขภาพซึ่งเป็นข้อมูลส่วนบุคคลลักษณะพิเศษที่กฎหมายคุ้มครองอย่างเข้มงวด

ในอดีต คลินิกทันตกรรมอาจมองการจัดการข้อมูลผู้ป่วยเป็นเรื่องของความลับทางวิชาชีพและการเก็บเวชระเบียนตามมาตรฐานวิชาชีพเป็นหลัก แต่เมื่อ PDPA มีผลใช้บังคับอย่างเต็มรูปแบบ การจัดการข้อมูลไม่ใช่เพียงเรื่องจริยธรรมหรือการบริหารงานภายในอีกต่อไป หากแต่เป็นหน้าที่ตามกฎหมายที่ต้องสามารถอธิบาย ตรวจสอบ และพิสูจน์ความชอบด้วยกฎหมายได้ คลินิกจึงต้องขยับจากการ “เก็บข้อมูลเพื่อการรักษา” ไปสู่การ “กำกับดูแลวงจรข้อมูลทั้งหมด” ตั้งแต่การรับข้อมูล การใช้ การเปิดเผย การเก็บรักษา การทำลาย ไปจนถึงการรองรับสิทธิของเจ้าของข้อมูล

สถานะของคลินิกทันตกรรมและการแต่งตั้ง DPO ภายใต้กฎหมาย

แนวทางจาก PDPATHailand ระบุว่า คลินิกในฐานะสถานให้บริการสุขภาพไม่ว่าจะดำเนินการโดยนิติบุคคลหรือแม้กระทั่งบุคคลธรรมดา จัดว่ามีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” เนื่องจากเป็นผู้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลของผู้ป่วย ลูกค้า และบุคลากร สถานะดังกล่าวทำให้คลินิกมีหน้าที่โดยตรงในการกำหนดฐานกฎหมาย จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย แจ้งรายละเอียดการใช้ข้อมูล และรับผิดชอบต่อความเสียหายหากเกิดการละเมิดข้อมูลส่วนบุคคล

อีกประเด็นสำคัญคือเรื่องการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO (Data Protection Officer) เนื่องจากกิจการคลินิกทันตกรรมมีการประมวลผลข้อมูลส่วนบุคคลลักษณะพิเศษ โดยเฉพาะข้อมูลสุขภาพและเวชระเบียน อันเป็นสาระสำคัญของการให้บริการ หากการประมวลผลข้อมูลส่วนบุคคลลักษณะพิเศษเป็นกิจกรรมหลักขององค์กร ย่อมต้องพิจารณาบทบัญญัติเรื่อง DPO อย่างจริงจังตามมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยเหตุนี้ คลินิกทันตกรรมจึงไม่ควรมองเรื่อง DPO เป็นเพียงภาระเชิงเอกสาร แต่ควรเข้าใจว่าเป็นกลไกกำกับดูแลภายในที่ช่วยให้การปฏิบัติตามกฎหมายมีความต่อเนื่องและตรวจสอบได้

บุคคลภายนอกบางรายอาจมีสถานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” เช่น ผู้ให้บริการซอฟต์แวร์ ผู้ให้บริการคลาวด์ ผู้รับจ้างทำลายเอกสาร หรือผู้ดูแลระบบนัดหมายออนไลน์ ส่วนแล็บทันตกรรมควรพิจารณาสถานะตามบทบาทจริงในแต่ละกรณี ดังนั้น การปฏิบัติตาม PDPA ของคลินิกจึงไม่อาจจำกัดอยู่เพียงกระบวนการภายใน แต่ต้องครอบคลุมการกำกับดูแลคู่สัญญา การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) และการตรวจสอบมาตรการป้องกันข้อมูลของผู้รับจ้างภายนอกด้วย



ลักษณะข้อมูลที่คลินิกทันตกรรมต้องดูแล

กิจการทันตกรรมเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งแบบทั่วไปและแบบอ่อนไหวอย่างหลีกเลี่ยงไม่ได้ ข้อมูลส่วนบุคคลทั่วไปที่คลินิกมักเก็บ ได้แก่ ชื่อ-นามสกุล เลขประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล ที่อยู่ ข้อมูลการนัดหมาย และข้อมูลการชำระเงิน ส่วนข้อมูลส่วนบุคคลลักษณะพิเศษ ได้แก่ ประวัติสุขภาพ เวชระเบียน ข้อมูลการแพ้ยา ภาพเอกซเรย์ หรือภาพถ่ายทาง การแพทย์ที่เปิดเผยข้อมูลสุขภาพ ส่วนภาพใบหน้า ภาพก่อน-หลัง การรักษา หรือข้อมูลเกี่ยวกับโครงสร้างช่องปาก อาจเป็นข้อมูลสุขภาพหรือข้อมูลชีวภาพได้ ขึ้นอยู่กับลักษณะข้อมูล วัตถุประสงค์ และเทคโนโลยีที่ใช้ประมวลผล

ความละเอียดอ่อนของข้อมูลเหล่านี้ทำให้การประมวลผล ในคลินิกทันตกรรมมีความเสี่ยงสูงกว่าธุรกิจทั่วไป เพราะข้อมูลสุขภาพเกี่ยวข้องกับศักดิ์ศรี ความเป็นส่วนตัว และความเชื่อมั่น ระหว่างผู้ป่วยกับผู้ประกอบวิชาชีพ แนวทางของทันตแพทยสภา จึงให้ความสำคัญกับการจัดทำเอกสารแจ้งการประมวลผลข้อมูล แบบฟอร์มความยินยอม บันทึกกิจกรรมการประมวลผลข้อมูล (ROPA) และเอกสารกำกับ การเข้าถึงหรือการเปิดเผยข้อมูลของ ทั้งผู้ป่วยและบุคลากร

ฐานกฎหมายและการขอความยินยอม

การปฏิบัติตาม PDPA ไม่ได้หมายความว่าต้องขอความยินยอมทุกครั้งที่มีการเก็บข้อมูล แต่หมายถึงการต้องมี “ฐานกฎหมาย” ที่เหมาะสมรองรับการประมวลผลในแต่ละวัตถุประสงค์ ในกิจการทันตกรรม ฐานกฎหมายที่ใช้บ่อย ได้แก่ ความจำเป็นเพื่อให้บริการทางการแพทย์ การปฏิบัติตามสัญญา การปฏิบัติตามกฎหมาย การป้องกันอันตรายต่อชีวิตหรือสุขภาพ และในบางกรณีคือความยินยอมโดยชัดแจ้ง โดยความยินยอมโดยชัดแจ้งควรใช้ในกรณีที่ ไม่สามารถอาศัยข้อยกเว้นตามมาตรา 26 หรือเป็นการใช้ข้อมูล นอกเหนือจากการรักษา เช่น การนำภาพผู้ป่วยไปใช้เพื่อการตลาด การประชาสัมพันธ์ หรือการเผยแพร่กรณีศึกษาในลักษณะที่ระบุตัวบุคคลได้

ประเด็นสำคัญคือ คลินิกต้องแยกวัตถุประสงค์การใช้ข้อมูลให้ชัดเจน และหลีกเลี่ยงการใช้ “แบบฟอร์มยินยอมแบบครอบจักรวาล” คลินิกควรระบุให้ชัดว่าแต่ละกิจกรรมใช้ฐานกฎหมายใด ใครเป็นผู้เข้าถึงข้อมูล และจะเก็บรักษาข้อมูลไว้นานเพียงใด ไม่ว่าจะเป็นการรักษา การติดตามผล การส่งต่อให้แล็บทันตกรรม การออกใบเสร็จ การติดต่อกลับ หรือการประชาสัมพันธ์ ทั้งนี้ก็เพื่อให้เกิดความโปร่งใสและทำให้เจ้าของข้อมูลเข้าใจอย่างแท้จริงว่า ข้อมูลของตนถูกนำไปใช้อย่างไร

เอกสารและระบบกำกับดูแลสิทธิของเจ้าของข้อมูล

แนวทางของทันตแพทยสภาได้จัดเตรียมแม่แบบเอกสารสำคัญสำหรับคลินิกทุกขนาด เช่น หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) แบบฟอร์มขอความยินยอม คำประกาศการใช้กล้องวงจรปิด (CCTV Notice) บันทึกการรายการกิจกรรมการประมวลผลข้อมูล (ROPA) ข้อตกลงการประมวลผลข้อมูล (DPA) และแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) เอกสารเหล่านี้ช่วยให้คลินิกมีระบบหลักฐานที่พร้อมตรวจสอบ และช่วยลดความคลุมเครือในการปฏิบัติงาน

อย่างไรก็ตาม สิ่งที่คลินิกจะละเลยไม่ได้คือการจัดให้มีช่องทางและมาตรการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูล ในทางปฏิบัติ เจ้าของข้อมูลมีสิทธิต่าง ๆ เช่น สิทธิขอเข้าถึงและรับสำเนาข้อมูลสุขภาพ ทั้งนี้ ภายใต้ข้อจำกัดตามกฎหมาย และต้องไม่กระทบสิทธิ เสรีภาพ หรือข้อมูลส่วนบุคคลของบุคคลอื่น สิทธิขอให้ลบหรือทำลายข้อมูลสามารถใช้ได้ภายใต้เงื่อนไขและข้อยกเว้นตามกฎหมาย โดยคลินิกอาจปฏิเสธได้หากยังจำเป็นต้องเก็บรักษาเวชระเบียนตามกฎหมาย มาตรฐานวิชาชีพ หรือเพื่อการก่อตั้ง ใช้ หรือยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือสิทธิขอถอนความยินยอมในการนำรูปภาพไปใช้เพื่อการโฆษณา ดังนั้น คลินิกจึงต้องมีขั้นตอนการยืนยันตัวตน มีแบบฟอร์มคำร้อง และมีระบบติดตามผลที่สามารถดำเนินการได้ภายในระยะเวลาที่กฎหมายกำหนด





ความเชื่อถือจากลูกค้า ในฐานะผลลัพธ์ของการปฏิบัติตาม PDPA

การปฏิบัติตาม PDPA ไม่ควรถูกมองเพียงในมิติของการหลีกเลี่ยงโทษ แต่ควรถูกมองว่าเป็นโอกาสเชิงกลยุทธ์ในการสร้างความเชื่อถือจากผู้รับบริการด้วย ผลวิเคราะห์ด้านธุรกิจชี้ให้เห็นว่าเมื่อลูกค้ารับรู้ว่าการให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลก็ย่อมเกิดความไว้วางใจต่อองค์กร ซึ่งส่งผลดีต่อชื่อเสียง ภาพลักษณ์และความสัมพันธ์ในระยะยาว

ในบริบทของคลินิกทันตกรรม ประเด็นนี้ยิ่งมีความสำคัญมากกว่าธุรกิจทั่วไป เพราะผู้ป่วยต้องเปิดเผยข้อมูลที่มีความเป็นส่วนตัวสูงและอาจกระทบต่อภาพลักษณ์ของตนโดยตรง เช่น ภาพใบหน้า ภาพฟัน ภาพก่อน-หลังการรักษา และประวัติสุขภาพ หากคลินิกสื่อสารอย่างชัดเจนว่าข้อมูลจะถูกใช้เพื่ออะไร ไม่ใช่เก็บไว้เฉยๆ และเปิดโอกาสให้ผู้ป่วยเลือก ใช้สิทธิ หรือถอนความยินยอมในเรื่องที่ไม่จำเป็น ผู้ป่วยย่อมรู้สึกว่าได้ได้รับความเคารพในฐานะเจ้าของข้อมูล ไม่ใช่เป็นเพียงแหล่งข้อมูลของธุรกิจ

ความเชื่อถือดังกล่าวสามารถแปลงเป็นผลเชิงพฤติกรรมได้อย่างเป็นรูปธรรม เช่น ผู้ป่วยยินดีให้ข้อมูลที่ครบถ้วนมากขึ้นเพื่อประโยชน์ต่อการรักษา กลับมาใช้บริการซ้ำ บอกต่อแก่บุคคลใกล้ชิด และลดความกังวลต่อการใช้เทคโนโลยีดิจิทัลของคลินิก เช่น ระบบนัดหมายออนไลน์หรือเวชระเบียนอิเล็กทรอนิกส์ ดังนั้นการคุ้มครองข้อมูลที่ดียิ่งขึ้นทั้งเครื่องมือสร้างความมั่นใจและองค์ประกอบของความได้เปรียบทางการแข่งขันในเวลาเดียวกัน



บทลงโทษตามกฎหมาย และความเสี่ยงที่ต้องตระหนัก

แม้การปฏิบัติตาม PDPA จะช่วยสร้างความเชื่อถือได้ แต่การละเลยก็อาจนำไปสู่ความเสี่ยงทางกฎหมาย 3 ประเภท ได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง สำหรับคลินิกทันตกรรม ความเสี่ยงเหล่านี้มักมีได้เกิดจากเจตนาร้ายเพียงอย่างเดียว หากยังเกิดจากความบกพร่องพื้นฐาน เช่น การไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสม การไม่แจ้งเหตุข้อมูลรั่วไหล การไม่กำกับดูแลผู้รับจ้างภายนอก หรือการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลอย่างไม่ถูกต้อง

ในทางปฏิบัติ คลินิกอาจเผชิญโทษทางปกครองได้ หากไม่มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม ไม่จัดให้มีช่องทางหรือกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูลโดยไม่มีความเหมาะสม หรือเพิกเฉยต่อหน้าที่ตามกฎหมายในประเด็นสำคัญ เช่น การกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลลักษณะพิเศษ ยิ่งเมื่อกิจการเกี่ยวข้องกับข้อมูลสุขภาพและข้อมูลชีวภาพ ความบกพร่องเพียงเล็กน้อย เช่น การทำลายเอกสารไม่ถูกต้อง การตั้งค่าระบบไม่เหมาะสม หรือการละเลยคำขอของผู้ป่วย ก็อาจส่งผลกระทบต่อทั้งทางกฎหมายและทางชื่อเสียงได้พร้อมกัน



การบังคับใช้จริงในประเทศไทย และบทเรียนสำหรับคลินิกทันตกรรม

การบังคับใช้ PDPA ในประเทศไทยพัฒนาย่างมีนัยสำคัญภายหลังการมีผลบังคับใช้เต็มรูปแบบ โดยคณะกรรมการผู้เชี่ยวชาญได้มีคำสั่งลงโทษปรับทางปกครองแล้วหลายกรณี รวมมูลค่ากว่า 20 ล้านบาท สะท้อนว่าการกำกับดูแลได้ก้าวเข้าสู่ระยะของ “การลงโทษจริง” แนวทางการบังคับใช้ในระยะหลังมุ่งเน้นไปที่การไม่มีมาตรการความปลอดภัยที่เพียงพอ การไม่แจ้งเหตุละเมิดข้อมูล การไม่กำกับผู้ประมวลผลข้อมูลอย่างเหมาะสม และการขาดระบบกำกับดูแลภายในที่เพียงพอ

กรณีศึกษาที่เกี่ยวข้องโดยตรงกับภาคสุขภาพ คือกรณีโรงพยาบาลเอกชนแห่งหนึ่งซึ่งถูกปรับจากการจัดการทำลายเวชระเบียนที่เป็นกระดาษอย่างไม่เหมาะสม ขณะที่ผู้รับจ้างทำลายเอกสารก็ถูกลงโทษเช่นกัน เนื่องจากเอกสารผู้ป่วยถูกจัดการโดยไม่รัดกุมจนข้อมูลรั่วไหลออกไป กรณีดังกล่าวชี้ให้เห็นว่า ความรับผิดชอบ PDPA อาจเกิดขึ้นได้จากการบริหารผู้รับจ้างภายนอก การทำลายเอกสาร และการกำกับวงจรข้อมูลในทางกายภาพ ไม่ใช่เฉพาะจากการโจมตีทางไซเบอร์หรือการใช้ระบบออนไลน์เท่านั้น

ดังนั้น คลินิกทันตกรรมจึงควรตระหนักว่า การทำ PDPA ไม่ใช่เรื่องของการเตรียมเอกสารไว้เผื่อมีการตรวจเท่านั้น หากแต่เป็นการวางระบบเพื่อรักษาความเชื่อมั่นของผู้ป่วยและลดความเสี่ยงขององค์กรในระยะยาว องค์กรที่ดำเนินการได้ดีจะได้รับประโยชน์สองด้านพร้อมกัน คือ ลดโอกาสถูกลงโทษ และเพิ่มความไว้วางใจจากผู้รับบริการในฐานะผู้ให้บริการที่มีมาตรฐาน

ข้อเสนอเชิงปฏิบัติ

แนวทางที่เหมาะสมสำหรับคลินิกทันตกรรม คือการเริ่มจากการทำ Data Mapping เพื่อให้เห็นเส้นทางข้อมูลทั้งหมดในองค์กร จากนั้นจึงทบทวนฐานกฎหมาย จัดทำเอกสารที่จำเป็น ปรับแบบฟอร์มความยินยอมให้แยกวัตถุประสงค์อย่างชัดเจน กำหนดผู้รับผิดชอบด้านการคุ้มครองข้อมูล วางกระบวนการรองรับคำขอใช้สิทธิของผู้ป่วยให้ชัดเจน ทำสัญญากับผู้ประมวลผลข้อมูล และกำหนดมาตรการตอบสนองเหตุละเมิดข้อมูลให้เป็นรูปธรรม

หากคลินิกดำเนินการอย่างเป็นระบบ PDPA จะไม่ใช่ข้อบังคับที่ต้องทำเพราะเกรงกลัวบทลงโทษเท่านั้น แต่จะกลายเป็นรากฐานของความน่าเชื่อถือในระยะยาว สำหรับธุรกิจบริการสุขภาพที่ความไว้วางใจของผู้ป่วยเป็นหัวใจสำคัญ การคุ้มครองข้อมูลส่วนบุคคลอย่างถูกต้อง โปร่งใส และตรวจสอบได้ จึงเป็นทั้งหน้าที่ทางกฎหมายและโอกาสเชิงกลยุทธ์ที่มีมูลค่าสูงต่ออนาคตของคลินิกทันตกรรม



บทความโดย

ดร.อุดมธิปไตย ไพรเกษตร

นายกสมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย

คุณสุกฤษฎี โภยอักษรเดช

เลขาธิการสมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย