พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๔๙ และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙"

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

(๑) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(๒) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้ เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๓) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(๔) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใดเพื่อเป็นหลักฐานว่าได้มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

มาตรา ๔ นอกจากที่บัญญัติไว้ในมาตรา ๓ ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๑) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดหลงอันเห็นได้ชัดว่าเกิดจากความไม่รู้หรือความเลินเล่อของผู้ยื่นคำขอ หรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณี ในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(๒) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่าคู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

มาตรา ๑๐ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

(สำเนาคู่ฉบับ)

คำสั่ง โรงพยาบาลพระนารายณ์มหาราช
ที่ ๒๗๖ / ๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลพระนารายณ์มหาราช มีประสิทธิภาพ มีมาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันจะส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศของโรงพยาบาล จึงขอแต่งตั้งคณะกรรมการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โรงพยาบาลพระนารายณ์มหาราชขึ้น เพื่อบริหารจัดการระบบงานต่างๆ ที่เกี่ยวข้องในระบบสารสนเทศโรงพยาบาลพระนารายณ์มหาราชมีความมั่นคงปลอดภัย ดังรายชื่อต่อไปนี้

๑. นางนุชรินทร์	อักษรดี	ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช	ประธานกรรมการ
๒. นางสาวปาริชาติ	ติระวัฒน์	รองผู้อำนวยการฝ่ายการแพทย์	รองประธาน
๓. นางสาววิภา	โพธิโต	รองผู้อำนวยการด้านภารกิจสุขภาพดิจิทัล	รองประธาน
๔. นายธภัทร	ติระวัฒน์	รองผู้อำนวยการฝ่ายบริหาร	กรรมการ
๕. นางมารยาท	รัตนประทีป	รองผู้อำนวยการฝ่ายการพยาบาล	กรรมการ
๖. นายกัมพล	วิบูลย์ศักดิ์สกุล	เภสัชกรเชี่ยวชาญ	กรรมการ
๗. นายณัฐพงศ์	สุวรรณศิริโชค	นายแพทย์ชำนาญการ	กรรมการ
๘. นายอธิพงศ์	วงษ์อยู่น้อย	ทันตแพทย์ชำนาญการพิเศษ	กรรมการ
๙. นายพีรวัฒน์	ตระกูลทวีสุข	นายแพทย์ชำนาญการพิเศษ	กรรมการ
๑๐. นางสาวอนัญญา	มานิตย์	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๑. นางบุญสม	พวงนาค	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๒. นางสาวพิศวรรณ	พูลสุข	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๓. นางนิตยา	กุลกุศล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๔. นางสาววรัญญา	เกษไชย	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๑๕. นางฐิตาภา	เชื้ออินท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
๑๖ นายวรพงศ์	พ่วงพลับ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและเลขานุการ
๑๗. นางสาวญาธิกานต์	มากสินธ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและผู้ช่วยเลขานุการ
๑๘. นายภาคภูมิ	เภาพาน	นักวิชาการคอมพิวเตอร์	กรรมการ
๑๙. นายธาราภูมิ	บุตรศรี	นักวิชาการคอมพิวเตอร์	กรรมการ

ให้คณะกรรมการ ..

คำสั่ง โรงพยาบาลพระนารายณ์มหาราช

ที่ / ๒๕๖๗

เรื่อง แต่งตั้งคณะกรรมการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลพระนารายณ์มหาราช มีประสิทธิภาพ มีมาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันจะส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศของโรงพยาบาล จึงขอแต่งตั้งคณะกรรมการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โรงพยาบาลพระนารายณ์มหาราชขึ้น เพื่อบริหารจัดการระบบงานต่างๆ ที่เกี่ยวข้องในระบบสารสนเทศโรงพยาบาลพระนารายณ์มหาราชมีความมั่นคงปลอดภัย ดังรายชื่อต่อไปนี้

๑. นางนุชรินทร์	อักษรดี	ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช	ประธานกรรมการ
๒. นางสาวปาริชาติ	ติระวัฒน์	รองผู้อำนวยการฝ่ายการแพทย์	รองประธาน
๓. นางสาววิภา	โพธิโต	รองผู้อำนวยการด้านภารกิจสุขภาพดิจิทัล	รองประธาน
๔. นายธภัทร	ติระวัฒน์	รองผู้อำนวยการฝ่ายบริหาร	กรรมการ
๕. นางมารยาท	รัตนประทีป	รองผู้อำนวยการฝ่ายการพยาบาล	กรรมการ
๖. นายกัมพล	วิบูลย์ศักดิ์สกุล	เภสัชกรเชี่ยวชาญ	กรรมการ
๗. นายณัฐพงศ์	สุวรรณศิริโชค	นายแพทย์ชำนาญการ	กรรมการ
๘. นายอธิพงศ์	วงษ์อยู่น้อย	ทันตแพทย์ชำนาญการพิเศษ	กรรมการ
๙. นายพีรวัฒน์	ตระกูลทวีสุข	นายแพทย์ชำนาญการพิเศษ	กรรมการ
๑๐. นางสาวอนัญญา	มานิตย์	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๑. นางบุญสม	พวงนาค	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๒. นางสาวพิศวรรณ	พูลสุข	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๓. นางนิตยา	กุลกุศล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
๑๔. นางสาววรัญญา	เกษไชย	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๑๕. นางฐิตาภา	เชื้ออินท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
๑๖ นายวรพงศ์	พ่วงพลับ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและเลขานุการ
๑๗. นางสาวญาธิกานต์	มากสินธ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและผู้ช่วยเลขานุการ
๑๘. นายภาคภูมิ	เภาพาน	นักวิชาการคอมพิวเตอร์	กรรมการ
๑๙. นายธาราภูมิ	บุตรศรี	นักวิชาการคอมพิวเตอร์	กรรมการ

ให้คณะกรรมการ...

ให้คณะกรรมการที่ได้รับการแต่งตั้ง ดังนี้

๑. เสนอแนะ และสนับสนุนการจัดทำนโยบาย และแผนแม่บท แผนปฏิบัติการว่าด้วยการรักษาความปลอดภัยภัย ไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลพระนารายณ์มหาราช

๑. ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์และประกาศใช้ในโรงพยาบาล

๒. ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. ดำเนินการ และประสานงานกับหน่วยงานของรัฐ และเอกชน เพื่อรับมือกับภัยคุกคามทางไซเบอร์

๔. เฝ้าระวังความเสี่ยง ติดตาม วิเคราะห์ ประมวลผล ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ในองค์กรทราบ

๕. สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๖. ให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแกโครงสร้างพื้นฐานสำคัญทางสารสนเทศของโรงพยาบาลพระนารายณ์มหาราช

๗. เผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ รวมถึงดำเนินการฝึกอบรมเพื่อยกระดับทักษะความชำนาญในการปฏิบัติหน้าที่ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทุกระดับ ในโรงพยาบาล

๘. มอบหมายให้เลขานุการ รายงานความคืบหน้า และสถานการณ์ที่เกี่ยวกับปัญหา และอุปสรรค เพื่อเสนอต่อคณะทำงานเพื่อพิจารณาดำเนินการ ตามระยะเวลาที่คณะกรรมการกำหนด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๑ เดือน สิงหาคม พ.ศ. ๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

(นางสาวปาริชาติ ดิระวัฒน์)
รองผู้อำนวยการฝ่ายการแพทย์

ให้คณะกรรมการที่ได้รับการแต่งตั้ง ดังนี้

๑. เสนอแนะ และสนับสนุนการจัดทำนโยบาย และแผนแม่บท แผนปฏิบัติการว่าด้วยการรักษาความปลอดภัยภัย ไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลพระนารายณ์มหาราช

๑. ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์และประกาศใช้ในโรงพยาบาล

๒. ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. ดำเนินการ และประสานงานกับหน่วยงานของรัฐ และเอกชน เพื่อรับมือกับภัยคุกคามทางไซเบอร์

๔. เฝ้าระวังความเสี่ยง ติดตาม วิเคราะห์ ประมวลผล ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ในองค์กรทราบ

๕. สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๖. ให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแกโครงสร้างพื้นฐานสำคัญทางสารสนเทศของโรงพยาบาลพระนารายณ์มหาราช

๗. เผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ รวมถึงดำเนินการฝึกอบรมเพื่อยกระดับทักษะความชำนาญในการปฏิบัติหน้าที่ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทุกระดับ ในโรงพยาบาล

๘. มอบหมายให้เลขานุการ รายงานความคืบหน้า และสถานการณ์ที่เกี่ยวกับปัญหา และอุปสรรคเพื่อเสนอต่อคณะทำงานเพื่อพิจารณาดำเนินการ ตามระยะเวลาที่คณะกรรมการกำหนด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๐ เดือน สิงหาคม พ.ศ. ๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

ประกาศ โรงพยาบาลพระนารายณ์มหาราช
เรื่อง ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๗

ตามพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศนั้น ตามที่กลุ่มงานเทคโนโลยีสารสนเทศได้ประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๑๕ มกราคม พ.ศ. ๒๕๖๖ ปัจจุบันคณะกรรมการพัฒนาระบบสุขภาพดิจิทัล รพ.พระนารายณ์มหาราช ได้มีการปรับปรุงเนื้อหาให้สอดคล้องกับระบบดิจิทัล เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระนารายณ์มหาราชเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากเครือข่ายภายนอกต่าง ๆ ดังนั้น โรงพยาบาลพระนารายณ์มหาราช จึงเห็นสมควรยกเลิกประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๑๕ มกราคม พ.ศ. ๒๕๖๖ กำหนดระเบียบปฏิบัติ ใหม่ดังนี้

๑. ด้านการรักษาความปลอดภัยของระบบสารสนเทศโรงพยาบาล (HOSxP)

๑.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเข้าใช้งาน (Password) ทุก ๙๐ วัน

๑.๒ รหัสผ่านจะต้องประกอบด้วย ตัวอักษรผสมตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก (a-z, A-Z) ตัวอักขระพิเศษ และตัวเลข โดยมีความยาวของตัวอักษรอย่างน้อย ๘ ตัวอักษร ตัวอย่าง เช่น Irobot๒๐๑๙

๑.๓ ห้ามเขียนรหัสผ่านไว้บริเวณจุดทำงาน หรือเปิดเผยในที่สาธารณะ เช่น หน้าจอ คีย์บอร์ด โดยต้องเก็บไว้เป็นความลับส่วนบุคคล

๑.๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำต่างๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

๑.๕ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ จะต้องทำการ log out ออกจากระบบทุกครั้ง

๒. ด้านการควบคุมเข้าถึงระบบเครือข่าย

๒.๑ สำหรับผู้ใช้งานใหม่ให้ทำการลงทะเบียนการขอใช้งานระบบอินเตอร์เน็ต (Internet) และระบบ HOSxP และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์ม

๒.๒ กรณีบุคคลภายนอกที่ต้องการเข้าสู่ระบบเครือข่ายและระบบ HOSxP ต้องทำหนังสือขออนุญาตก่อนเข้าใช้งาน และแจ้งผู้ดูแลระบบทุกครั้งก่อนเข้าใช้งาน

๓. ด้านการจัดการความมั่นคงของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑ ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาเชื่อมต่อกับระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เช่น CD-ROM, USB Drive, External Hard Disk Hub, Switch, Wi-Fi Router

๓.๒ ห้ามใช้งานอินเตอร์เน็ตเพื่อประโยชน์ส่วนบุคคล ยกเว้นระบบเว็บไซต์ของโรงพยาบาล หรือหน่วยงานราชการที่เกี่ยวข้อง

๓.๓ ห้ามติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ด้วยตนเอง กรณีจำเป็นต้องติดตั้งโปรแกรมให้ประสานศูนย์คอมพิวเตอร์

๓.๔ หากพบว่าคอมพิวเตอร์ หรืออุปกรณ์ที่เกี่ยวข้องทำงานผิดปกติ ให้ประสานผู้รับผิดชอบเทคโนโลยีสารสนเทศประจำหน่วยงาน (admin หน่วยงาน) หรือศูนย์คอมพิวเตอร์

๓.๕ ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ รวมถึงอุปกรณ์คอมพิวเตอร์ ก่อนได้รับอนุญาตจากศูนย์คอมพิวเตอร์

๔. ด้านการใช้สังคมออนไลน์ ที่เกี่ยวกับโรงพยาบาล

๔.๑ ผู้ใช้งานห้ามเผยแพร่ภาพ ข้อความ หรือข้อมูล เช่น ภาพผู้ป่วยที่เห็นใบหน้า ชื่อ-สกุล รหัสบัตรประชาชน รหัสผู้ป่วย รหัสเอกซเรย์ ที่สามารถระบุตัวตนผู้ป่วยได้

๔.๒ ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟซบุ๊ค (Facebook), ไลน์ (Line), เว็บไซต์ (Website) หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต

๔.๓ มีการจัดทำทะเบียนบัญชีผู้ใช้งานทุกคน และใช้ Username และ Password ก่อนเข้าใช้งาน Internet ของทุกคนในโรงพยาบาล

๔.๔ หลังจากใช้งานระบบอินเตอร์เน็ตเรียบร้อยแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์ที่ใช้งานและออกจากเครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการระบบเพื่อป้องกันการเข้าถึงการใช้งานโดยบุคคลอื่นๆ ที่ไม่เกี่ยวข้องกับโรงพยาบาล

ประกาศ ณ วันที่ ๔ มิถุนายน พ.ศ.๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

(สำเนาคู่ฉบับ)

ประกาศโรงพยาบาลพระนารายณ์มหาราช
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลพระนารายณ์มหาราช

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระนารายณ์มหาราชเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลพระนารายณ์มหาราช จึงเห็นสมควรกำหนดนโยบาย ดังนี้

๑. โรงพยาบาลพระนารายณ์มหาราชส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๒. โรงพยาบาลพระนารายณ์มหาราช กำหนดให้มีการควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศเพื่อให้ข้อมูลผู้ใช้งานและข้อมูลความลับของผู้ป่วยมีความปลอดภัย

๓. โรงพยาบาลพระนารายณ์มหาราช กำหนดให้มีการจัดทำระบบสำรองข้อมูลเพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ

๔. โรงพยาบาลพระนารายณ์มหาราช กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเพื่อให้หน่วยงานทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และเพื่อป้องกันไม่ให้เกิดความเสี่ยงกับระบบสารสนเทศ

๕. โรงพยาบาลพระนารายณ์มหาราชกำหนดให้บุคลากรทุกระดับ ปฏิบัติตามแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาลพระนารายณ์มหาราช พ.ศ.๒๕๖๗ เพื่อให้ปฏิบัติงานอย่างมีประสิทธิภาพ และมีความมั่นคงปลอดภัยระบบสารสนเทศ

ประกาศ ณ วันที่ ๒๑ สิงหาคม พ.ศ.๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

(สำเนาคู่ฉบับ)

ประกาศโรงพยาบาลพระนารายณ์มหาราช
เรื่อง ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๗

ตามพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศนั้น ตามที่กลุ่มภารกิจสุขภาพดิจิทัลได้ประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๗ ปัจจุบันคณะกรรมการพัฒนาระบบสุขภาพดิจิทัล โรงพยาบาล-พระนารายณ์มหาราช ได้มีการปรับปรุงเนื้อหาให้สอดคล้องกับสถานการณ์ปัจจุบัน เพื่อให้ระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากเครือข่ายภายนอกต่าง ๆ ดังนั้น โรงพยาบาลพระนารายณ์มหาราช จึงเห็นสมควรยกเลิกประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๗ และกำหนดระเบียบปฏิบัติใหม่ดังนี้

๑. ห้ามเขียนรหัสผ่านไว้บริเวณจุดทำงานหรือเปิดเผยในที่สาธารณะ เช่น หน้าจอ คีย์บอร์ด โต๊ะทำงาน โดยต้องเก็บไว้เป็นความลับส่วนบุคคล

๒. ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบ ต่อการกระทำต่าง ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

๓. กรณีบุคคลภายนอกที่ต้องการเข้าสู่ระบบเครือข่ายและระบบ HOSxP ต้องทำหนังสือขออนุญาตก่อนเข้าใช้งานและแจ้งผู้ดูแลระบบทุกครั้งก่อนเข้าใช้งานเก็บบันทึกการเข้าใช้งาน

๔. ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาเชื่อมต่อกับระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เช่น CD-ROM, USB Drive External, Hard Disk, Hub Switch, Wi-Fi Router

๕. ห้ามใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ ในระหว่างเวลาปฏิบัติราชการ

๖. ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้ง ก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๗. ผู้ใช้งานห้ามเผยแพร่ภาพ ข้อความ หรือข้อมูลใด ๆ เช่น ชื่อ-สกุล เลขบัตรประจำตัวประชาชน ที่สามารถระบุตัวตนผู้ป่วยได้ ผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook) ไลน์ (Line) เว็บไซต์ (Website) หรือโปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต

๘. ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้รับอนุญาตจากแพทย์เจ้าของไข้ หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ ๒๐ สิงหาคม พ.ศ.๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

ประกาศโรงพยาบาลพระนารายณ์มหาราช
เรื่อง ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๗

ตามพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศนั้น ตามที่กลุ่มภารกิจสุขภาพดิจิทัลได้ประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๗ ปัจจุบันคณะกรรมการพัฒนาระบบสุขภาพดิจิทัล โรงพยาบาล-พระนารายณ์มหาราช ได้มีการปรับปรุงเนื้อหาให้สอดคล้องกับสถานการณ์ปัจจุบัน เพื่อให้ระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากเครือข่ายภายนอกต่าง ๆ ดังนั้น โรงพยาบาลพระนารายณ์มหาราช จึงเห็นสมควรยกเลิกประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๗ และกำหนดระเบียบปฏิบัติใหม่ดังนี้

๑. ห้ามเขียนรหัสผ่านไว้บริเวณจุดทำงานหรือเปิดเผยในที่สาธารณะ เช่น หน้าจอ คีย์บอร์ด โต๊ะทำงาน โดยต้องเก็บไว้เป็นความลับส่วนบุคคล

๒. ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบ ต่อการกระทำต่าง ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

๓. กรณีบุคคลภายนอกที่ต้องการเข้าสู่ระบบเครือข่ายและระบบ HOSxP ต้องทำหนังสือขออนุญาตก่อนเข้าใช้งานและแจ้งผู้ดูแลระบบทุกครั้งก่อนเข้าใช้งานเก็บบันทึกการเข้าใช้งาน

๔. ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาเชื่อมต่อกับระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เช่น CD-ROM, USB Drive External, Hard Disk, Hub Switch, Wi-Fi Router

๕. ห้ามใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ ในระหว่างเวลาปฏิบัติราชการ

๖. ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้ง ก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๗. ผู้ใช้งานห้ามเผยแพร่ภาพ ข้อความ หรือข้อมูลใด ๆ เช่น ชื่อ-สกุล เลขบัตรประจำตัวประชาชน ที่สามารถระบุตัวตนผู้ป่วยได้ ผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook) ไลน์ (Line) เว็บไซต์ (Website) หรือโปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต

๘. ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้รับอนุญาตจากแพทย์เจ้าของไข้ หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ ๒๐ สิงหาคม พ.ศ.๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

โรงพยาบาลพระนารายณ์มหาราช

โรงพยาบาลพระนารายณ์มหาราช ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่นเกี่ยวกับท่าน (รวมเรียกว่า "ข้อมูล") เพื่อให้ท่านสามารถเชื่อมั่นได้ว่า โรงพยาบาลพระนารายณ์มหาราช มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ("กฎหมายคุ้มครองข้อมูลส่วนบุคคล") รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ("นโยบาย") นี้จึงได้ถูกจัดทำขึ้นเพื่อชี้แจงแก่ท่านถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า "ประมวลผล") ข้อมูลส่วนบุคคลซึ่งดำเนินการโดย โรงพยาบาลพระนารายณ์มหาราช รวมถึงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องผู้ดำเนินการแทนหรือในนามของโรงพยาบาล โดยมีเนื้อหาสาระดังต่อไปนี้

1. คำนิยาม

"โรงพยาบาลฯ" หมายถึง โรงพยาบาลพระนารายณ์มหาราช

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ข้อมูลส่วนบุคคลอ่อนไหว" หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้แก่ ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (เช่น ข้อมูลลายนิ้วมือ ข้อมูลภาพจำลองใบหน้า ข้อมูลภาพจำลองม่านตา) หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

"การประมวลผลข้อมูลส่วนบุคคล" หมายถึง การดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น เก็บรวบรวม บันทึกสำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้กู้คืน เปิดเผย ส่งต่อ เผยแพร่โอน รวม ลบ ทำลาย เป็นต้น

"เจ้าของข้อมูลส่วนบุคคล" หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่โรงพยาบาลเก็บรวบรวม ใช้ หรือเปิดเผย

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

2. แหล่งที่มาของข้อมูลส่วนบุคคล

โรงพยาบาลฯ เก็บรวมหรือได้มาซึ่งข้อมูลส่วนบุคคลประเภทต่างๆ จากแหล่งข้อมูลดังต่อไปนี้

1) ข้อมูลส่วนบุคคลที่โรงพยาบาลฯ เก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรงในช่องทางให้บริการต่างๆ เช่น ขั้นตอนการสมัคร ลงทะเบียน การลงทะเบียนเข้ารับบริการตรวจและรักษาโรคไม่ว่าจะด้วยตนเอง หรือผ่านช่องทางออนไลน์ สมัครงาน ลงนามในสัญญา เอกสาร ทำแบบสำรวจ หรือช่องทางให้บริการอื่นที่ควบคุมดูแลโดยโรงพยาบาลฯ หรือเมื่อเจ้าของข้อมูลส่วน บุคคลติดต่อสื่อสารกับโรงพยาบาลฯ ณ ที่ทำการหรือผ่านช่องทางติดต่ออื่นที่ควบคุมดูแลโดยโรงพยาบาลฯ เป็นต้น

2) ข้อมูลส่วนบุคคลที่โรงพยาบาลฯ เก็บรวมโดยทางอ้อม ได้แก่ บุคคลที่มีความใกล้ชิดกับท่าน เช่น ญาติ คู่สมรส บุคคลที่ท่านมอบอำนาจให้ดำเนินการแทนตัวท่านในการติดต่อกับโรงพยาบาลฯสถานพยาบาลอื่นๆ ในกรณีที่ท่านได้ให้ความยินยอมกับสถานพยาบาลนั้นๆว่าให้เปิดเผยข้อมูล ส่วนบุคคลของท่านได้ บุคคล นิติบุคคล หรือหน่วยงานไม่ว่าภาครัฐ เอกชน หรือรัฐวิสาหกิจ ที่เป็นผู้ส่งท่านมาตรวจรักษากับโรงพยาบาลฯ หรือเป็นผู้ชำระค่าบริการตรวจรักษาให้กับท่าน

3) ข้อมูลที่โรงพยาบาลฯ เก็บรวบรวมจากการที่เจ้าของข้อมูลส่วนบุคคลเข้าใช้งานเว็บไซต์ หรือบริการอื่นๆ ตามสัญญาหรือตามพันธกิจ เช่น การติดตามพฤติกรรมการใช้งานเว็บไซต์ หรือบริการของโรงพยาบาลฯ ด้วยการใช้คุกกี้ (Cookies) หรือจากซอฟต์แวร์บนอุปกรณ์ของเจ้าของ ข้อมูลส่วนบุคคล เป็นต้น

4) ข้อมูลส่วนบุคคลที่โรงพยาบาลฯ เก็บรวบรวมจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล โดยที่แหล่งข้อมูลดังกล่าวมีอำนาจหน้าที่ มีเหตุผลที่ชอบด้วยกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในการเปิดเผยข้อมูลแก่ โรงพยาบาลฯ เช่น การเชื่อมโยงบริการ ดิจิทัลของหน่วยงานของรัฐในการให้บริการเพื่อประโยชน์สาธารณะแบบเบ็ดเสร็จแก่เจ้าของ ข้อมูลส่วนบุคคลเอง การรับข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นในฐานะที่ โรงพยาบาลฯ มีหน้าที่ตามพันธกิจในการดำเนินการจัดให้มีศูนย์แลกเปลี่ยนข้อมูลกลาง เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล รวมถึงจากความจำเป็นเพื่อให้บริการตามสัญญาที่อาจมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานคู่สัญญาได้

นอกจากนี้ ยังหมายความรวมถึงกรณีที่ท่านเป็นผู้ให้ข้อมูลส่วนบุคคลของบุคคลภายนอกแก่ โรงพยาบาลฯ ดังนี้ ท่านมีหน้าที่รับผิดชอบในการแจ้งรายละเอียดตามนโยบายนี้หรือประกาศของบริการ ตามแต่กรณี ให้บุคคลดังกล่าวทราบ ตลอดจนขอความยินยอมจากบุคคลนั้นหากเป็นกรณีที่ต้องได้รับความยินยอมในการเปิดเผยข้อมูลแก่ โรงพยาบาลฯ

ทั้งนี้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ให้ข้อมูลที่มีความจำเป็นในการให้บริการของโรงพยาบาลฯ อาจเป็นผลให้โรงพยาบาลฯ ไม่สามารถให้บริการได้อย่างถูกต้องแก่เจ้าของข้อมูลส่วนบุคคลดังกล่าวได้ทั้งหมดหรือบางส่วน

3. ข้อมูลส่วนบุคคลที่โรงพยาบาลฯ เก็บรวบรวม

ข้อมูลที่โรงพยาบาลฯ เก็บรวบรวม สามารถจำแนกออกเป็นประเภทดังต่อไปนี้

ประเภทข้อมูลส่วนบุคคล	รายละเอียด
1. ข้อมูลระบุตัวตน	เช่น ชื่อ นามสกุล เพศ วันเดือนปีเกิด รูปถ่ายใบหน้า เลขที่บัตรประจำตัวประชาชน หนังสือเดินทาง หรือหมายเลขที่ระบุตัวตนอื่นๆ
2. ข้อมูลสำหรับการติดต่อ	เช่น ที่อยู่ หมายเลขโทรศัพท์ หมายเลขโทรศัพท์มือถือ อีเมล์
3. ข้อมูลเพื่อประกอบการวินิจฉัยโรค/ เพื่อติดตามการรักษา	เช่น ข้อมูลการรักษาพยาบาล รายงานที่เกี่ยวกับสุขภาพกายและสุขภาพจิต การดูแลสุขภาพของผู้รับบริการ การวินิจฉัยชื่อโรคที่ได้รับการวินิจฉัย ข้อมูลที่เกี่ยวข้องกับการใช้ยา รายการยาที่แพทย์ได้สั่ง ผลการทดสอบจากห้องทดลอง ผลการทดสอบจากห้องปฏิบัติการ ผลเลือด ผลตรวจชิ้นเนื้อทางพยาธิวิทยา ภาพถ่ายทางรังสีวิทยาและรายงานผลการตรวจทางรังสีวิทยา ข้อมูลที่จำเป็นต่อการให้บริการทางการแพทย์และการรักษา ข้อมูลผลการรักษา ข้อมูลคำแนะนำในการรักษาและปฏิบัติตัวระหว่างการรักษาข้อมูลปัจจัยเสี่ยง ข้อมูลการประสบอุบัติเหตุ พฤติกรรมการใช้ชีวิต การบริโภค หรือพฤติกรรมการนอน รวมไปถึงการถ่ายภาพนิ่งภาพเคลื่อนไหว หรือการกระทำใดๆ ตามหลักวิชาชีพที่เกี่ยวข้อง เป็นต้น
4. ข้อมูลอ่อนไหว	เช่น ศาสนา ข้อมูลสุขภาพ รวมถึง หมู่โลหิต ประวัติการเจ็บป่วย ประวัติการรักษาพยาบาล ประวัติการแพ้ยาหรือแพ้อาหาร ประวัติการพบแพทย์เวชกรรม แพทย์แผนไทย ผู้ประกอบวิชาชีพด้านสุขภาพ ประวัติทันตกรรม ประวัติกายภาพบำบัด ความต้องการพิเศษในการรักษาพยาบาล ข้อมูลชีวภาพ เช่น ข้อมูลพันธุกรรม พฤติกรรมทางเพศ เป็นต้น
5. ข้อมูลการเงิน	เช่น สิทธิ์การรักษา ข้อมูลการเรียกเก็บเงิน ข้อมูลบัตรเครดิตหรือเดบิต รายละเอียดบัญชีธนาคาร ข้อมูลเงินเดือน ข้อมูลใบเสร็จ ข้อมูลใบราคา ข้อมูลสังคมสงเคราะห์

ประเภทข้อมูลส่วนบุคคล	รายละเอียด
6. ข้อมูลสิทธิประโยชน์การรักษาพยาบาล	เช่น สิทธิประกันสุขภาพถ้วนหน้า ประกันสังคม สวัสดิการราชการ หรือ สวัสดิการอื่นๆ การประกันสุขภาพ และประกันภัย
7. ข้อมูลสถิติ (Statistical data)	เช่น ข้อมูลที่ไม่ระบุตัวตน จำนวนผู้ป่วย และจำนวนการเข้าชมเว็บไซต์
8. ข้อมูลการสมัครข่าวสารและกิจกรรมทางการตลาด (Marketing data)	เช่น ข้อมูลการลงทะเบียนเพื่อรับข่าวสารและเข้าร่วมการเข้าร่วมกิจกรรมทางการตลาด
9. ข้อมูลจากการเข้าใช้เว็บไซต์ (Technical data)	เช่น หมายเลข IP Address ของคอมพิวเตอร์ ชนิดของบราวเซอร์ข้อมูล Cookies การตั้งค่าเรื่องเขตเวลา (timezone) ระบบปฏิบัติการ แพลตฟอร์มและเทคโนโลยีของอุปกรณ์ที่ใช้เข้าเว็บไซต์ และระบบการนัดหมายผู้ป่วย
10. ข้อมูลบัญชีผู้ใช้	เช่น ชื่อผู้ใช้ รหัสผ่าน ที่ใช้เพื่อการเข้าถึงเว็บไซต์ หรือแอปพลิเคชั่น
11. ข้อมูลอื่นๆ	เพื่อประโยชน์ในการให้บริการสุขภาพและเพื่อการดูแลสุขภาพของเจ้าของข้อมูล

4. วัตถุประสงค์ของการประมวลผลข้อมูล (การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล) ส่วนบุคคล

โรงพยาบาลฯ มีวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ดังนี้

1) เพื่อการให้บริการทางการแพทย์แก่ท่านในทุกช่องทาง ซึ่งรวมถึง การระบุตัวตนของคนไข้การจัดตาราง และแจ้งเตือนการนัดพบแพทย์หรือตารางการรักษาพยาบาล การวิเคราะห์วินิจฉัยและให้คำปรึกษาเกี่ยวกับการรักษาพยาบาลแก่ท่าน การดูแลให้ความปลอดภัยแก่ท่านขณะรักษาพยาบาลหรือเข้าพักในสถานที่ของโรงพยาบาลฯ การให้บริการที่เกี่ยวข้องกับการรักษาพยาบาลแก่ท่าน ประสานงานกับหน่วยงานภายในหรือหน่วยงานภายนอก เกี่ยวกับการรักษาพยาบาลของท่าน เป็นต้น

2) เพื่อการค้นคว้า วิจัย ทดลอง และพัฒนาผลิตภัณฑ์ทางการแพทย์ การรักษาพยาบาล หรือการให้บริการ ของโรงพยาบาลฯ เช่น การวิจัยวัคซีนชนิดต่าง ๆ หรือ การวิเคราะห์ และทดลองการตอบสนองต่อการ รักษาด้วยวิธีการต่าง ๆ เป็นต้น

3) เพื่อการศึกษาวิจัยหรือการจัดทำสถิติ รายงานที่เป็นไปตามวัตถุประสงค์การดำเนินโรงพยาบาลฯ ตามที่กฎหมายกำหนด

4) เพื่อให้โรงพยาบาลฯ สามารถให้ความช่วยเหลือตอบข้อซักถามและข้อร้องเรียนของท่าน

5) เพื่อเชิญท่านเข้าร่วมกิจกรรมโครงการต่าง ๆ ของโรงพยาบาลฯ เพื่อช่วยโรงพยาบาลฯ พัฒนาปรับปรุงบริการ และการดำเนินกิจกรรมต่าง ๆ บริการ หรือร่วมกิจกรรมต่าง ๆ ของโรงพยาบาลฯ โดยการเข้าร่วมดังกล่าขึ้นอยู่กับความสมัครใจและจะไม่กระทบต่อการเข้าถึงบริการของโรงพยาบาลฯ

6) เพื่อสนับสนุนกิจกรรมด้านการศึกษา เช่น เพื่อให้การศึกษาต่อนักศึกษาแพทย์ และนักศึกษาพยาบาล ซึ่งปฏิบัติงาน ภายในโรงพยาบาลของโรงพยาบาลฯ เป็นต้น

7) เพื่อเป็นการป้องกันการกระทำที่ไม่เหมาะสมหรือผิดกฎหมาย โรงพยาบาลฯอาจมีการตรวจสอบข้อมูลที่เก็บ รวบรวม รวมถึงข้อมูลในกล้อง CCTV เพื่อสอดส่องดูแล ตรวจจับ และ ป้องกันไม่ให้มีการกระทำที่ไม่เหมาะสมหรือผิดกฎหมาย

8) เพื่อปกป้องและระงับอันตรายที่อาจเกิดกับท่าน อาจมีการใช้ข้อมูลของท่านในกรณีที่โรงพยาบาลฯ เห็นว่าอาจมีความเสี่ยงหรืออันตรายอย่างร้ายแรงหรือมีการละเมิดต่อท่านหรือ ผู้ใดก็ตาม

9) เพื่อปฏิบัติตามกฎหมายที่ใช้บังคับหรือปฏิบัติหน้าที่ตามกฎหมายของโรงพยาบาลฯ

5. ระยะเวลาในการจัดเก็บข้อมูล

โรงพยาบาลฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้เป็นระยะเวลา ตราบเท่าที่วัตถุประสงค์ของการนำข้อมูลดังกล่าวไปใช้ยังคงมีอยู่ หลังจากนั้นโรงพยาบาลฯ จะลบ ทำลายข้อมูล หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ เว้นแต่กรณีจำเป็นต้องเก็บ รักษาข้อมูลต่อไปตามที่กฎหมายที่เกี่ยวข้องกำหนด หรือเพื่อเป็นการคุ้มครองสิทธิประโยชน์ของโรงพยาบาลฯ

โดยปกติในกรณีทั่วโประยะเวลาการเก็บข้อมูลจะไม่เกินกำหนดระยะเวลา 10 (สิบ) ปี เว้นแต่จะมีกฎหมายกำหนดให้เก็บรักษา ข้อมูลไว้เป็นระยะเวลานานกว่าที่กำหนดไว้ดังกล่าวข้างต้น หรือหากมีความจำเป็นเพื่อวัตถุประสงค์อื่น ๆ เช่น เพื่อความปลอดภัย เพื่อการป้องกันการละเมิดหรือการประพฤติมิชอบ หรือเพื่อการเก็บบันทึกทางการเงิน

6. การเปิดเผยหรือแบ่งปันข้อมูลส่วนบุคคล

โรงพยาบาลฯ จะไม่เปิดเผยข้อมูลส่วนบุคคลของเข้าของข้อมูลโดยไม่มีฐานการประมวลผลข้อมูลโดยชอบด้วย กฎหมาย โดยข้อมูลของท่านอาจถูกเปิดเผย หรือโอนไปยังองค์กร หน่วยงานของรัฐ หรือบุคคลภายนอก รวมถึงโรงพยาบาลหรือหน่วยงานภายในอื่น ๆ ของโรงพยาบาลฯ เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินการดังนี้

1) **เพื่อวัตถุประสงค์ในการตรวจรักษาโรคและให้บริการทางการแพทย์**

โรงพยาบาลฯ อาจทำการเปิดเผยข้อมูลส่วนบุคคลของ ท่านไปให้หน่วยงานภายนอก เช่น การประสานงานกับโรงพยาบาลอื่น นอกเหนือจากโรเพยาบาลในสังกัดของโรงพยาบาลฯ เพื่อ ติดต่อปรึกษาแพทย์หรือบุคลากรหรือระบบอื่น ที่มีความเชี่ยวชาญในด้านที่จำเป็นแก่การบำบัดรักษาท่าน ซึ่งจะทำให้ท่านให้รับบริการทางการแพทย์ที่เหมาะสมหรือมีประสิทธิภาพมากขึ้น

2) **เพื่อการให้บริการทางการแพทย์ในกรณีจำเป็นต้องเชื่อมโยงข้อมูลระหว่างสถานพยาบาล**

การส่ง "สิ่งส่งตรวจ" ของท่านไปยังหน่วยงานเฉพาะทาง การร้องขอสิ่งสนับสนุนที่จำเป็น เช่น การขอโลหิตหรือการขอรับบริจาคอวัยวะ เพื่อการรับ-ส่งห่อผู้ป่วยระหว่างโรงพยาบาล (Refer)

การเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่โรงพยาบาล หรือสถาบันการศึกษาอื่น ๆ เพื่อประโยชน์ด้านการศึกษาและการพัฒนาบุคลากรทางการแพทย์และพยาบาล

3) เพื่อวัตถุประสงค์ในการเชื่อมโยงฐานข้อมูลสุขภาพรายบุคคล

โรงพยาบาลฯ จะนำข้อมูลส่วนบุคคลของท่านเข้าสู่ระบบคอมพิวเตอร์ เพื่อเชื่อมโยงฐานข้อมูลสุขภาพระหว่างสถานพยาบาลในเครือข่าย ให้สามารถเรียกดูข้อมูลสุขภาพส่วน บุคคลของท่านผ่านอุปกรณ์ต่าง ๆ เพื่อประโยชน์ในการให้บริการสุขภาพและเพื่อการดูแล สุขภาพของเจ้าของข้อมูล

4) เพื่อใช้สิทธิประโยชน์ในการรักษาพยาบาล

โรงพยาบาลฯ จะเปิดเผยข้อมูลส่วนบุคคลของท่านเพื่อใช้สิทธิประโยชน์ในการรักษาพยาบาลจากกองทุนประกันสุขภาพถ้วนหน้า ประกันสังคม สวัสดิการราชการ หรือ สวัสดิการอื่นๆตามที่ท่านได้ขึ้นทะเบียนไว้ หรือตามที่กฎหมายกำหนด

5) สถาบันการเงิน

โรงพยาบาลฯ อาจทำการเปิดเผยข้อมูลส่วนบุคคลของท่านไปให้สถาบันการเงินธนาคาร บริษัท บัตรเครดิต บริษัทประกันภัยที่เป็นคู่สัญญาของท่าน หรือหน่วยงานทวงถามหนี้ ตามที่จำเป็นในการทำการจ่ายและรับชำระเงินตามที่มีการร้องขอ โดยโรงพยาบาลฯจะเปิดเผยข้อมูลส่วน บุคคลต่อบุคคลที่มีอำนาจในการเข้าถึง ข้อมูลดังกล่าวตามที่กฎหมายกำหนด และสามารถ พิสูจน์ได้ว่าตนมีอำนาจในการเข้าถึงดังกล่าวเท่านั้น

6) หน่วยงานราชการที่เกี่ยวข้อง

โรงพยาบาลฯอาจทำการเปิดเผยข้อมูลส่วนบุคคลของท่านไปยังหน่วยงาน ราชการที่เกี่ยวข้องเพื่อการปฏิบัติตามกฎหมาย เช่น การรายงานกับหน่วยงานกำกับดูแลต่าง ๆ ที่เกี่ยวข้อง หรือการปฏิบัติตามข้อกำหนดทางกฎหมายอื่นใดที่โรงพยาบาลฯต้องปฏิบัติตาม

7) ผู้ให้บริการภายนอก

โรงพยาบาลฯ อาจทำเก็บข้อมูลส่วนบุคคลไว้ในระบบประมวลผลแบบคลาวด์ (Cloud Computing) โดยใช้บริการจากบุคคลที่สามไม่ว่าตั้งอยู่ในประเทศไทยหรือต่างประเทศ หรือ ผู้ให้บริการเซิร์ฟเวอร์สำหรับเว็บไซต์ การวิเคราะห์ข้อมูล การประมวลผลการจ่ายและรับชำระเงิน การทำคำสั่งซื้อ การให้บริการโครงสร้างพื้นฐานเกี่ยวกับเทคโนโลยีสารสนเทศ เป็นต้น

ในกรณีที่โรงพยาบาลฯ จำเป็นต้องส่งข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้แก่บุคคลภายนอกโรงพยาบาลฯ จะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อให้มั่นใจว่า บุคคลภายนอกจะดูแลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ไม่ให้เกิดการสูญหาย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้ การดัดแปลง หรือการเปิดเผยและการใช้งานที่ไม่ถูกต้อง

7. การโอนข้อมูลไปต่างประเทศ

โรงพยาบาลฯ จะทำการเปิดเผยข้อมูลส่วนบุคคลต่อผู้รับข้อมูลในต่างประเทศ เฉพาะกรณีที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ทำได้เท่านั้น ทั้งนี้ โรงพยาบาลฯอาจปฏิบัติตามหลักเกณฑ์การโอนข้อมูลระหว่างประเทศโดยเข้าทำข้อสัญญามาตรฐานหรือใช้กลไกอื่นที่พึงมีตามกฎหมายว่าด้วยการคุ้มครองข้อมูลที่ใช้บังคับ และโรงพยาบาลฯอาจอาศัยสัญญาการโอนข้อมูล หรือกลไกอื่นที่ได้รับการอนุมัติ เพื่อการโอนข้อมูล ส่วนบุคคลไปยังต่างประเทศ

8. มาตรการรักษาความปลอดภัยของข้อมูล

โรงพยาบาลฯ จะใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึง มาตรการป้องกัน ด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และ มาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) เพื่อป้องกันการเข้าถึงและเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และสอดคล้องกับการดำเนินงานของโรงพยาบาลฯและมาตรฐานที่รับรองโดยทั่วไป

โรงพยาบาลฯ กำหนดให้เจ้าหน้าที่ของโรงพยาบาลฯเข้ารับการฝึกอบรมเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของข้อมูล

การจัดจ้างผู้ให้บริการภายนอก โรงพยาบาลฯจะมีการสอบทานและปรับปรุงมาตรการต่างๆ เพื่อให้แน่ใจว่าผู้ให้บริการภายนอกที่โรงพยาบาลฯทำการว่าจ้างจะมีการใช้มาตรการในการ เก็บรวบรวม ประมวลผล โอนย้าย จัดการ และรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเพียงพอในการให้บริการภายใต้วัตถุประสงค์ของโรงพยาบาลฯ เป็นไปตามมาตรฐานต่าง ๆ ของประเทศ และกฎระเบียบที่เกี่ยวข้อง

โรงพยาบาลฯ จัดทำนโยบายและขั้นตอนวิธีการต่าง ๆ เพื่อการจัดการข้อมูลอย่างปลอดภัย และป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาตโดยมีรายละเอียดดังต่อไปนี้

- กำหนดนโยบายและขั้นตอนวิธีการต่าง ๆ เพื่อจัดการข้อมูลอย่างปลอดภัย และอาจกำหนดเพิ่มเติมในสัญญาระหว่างโรงพยาบาลฯกับคู่สัญญาแต่ละราย
- มีการบริหารจัดการสิทธิของพนักงานและลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคล อย่างเหมาะสม
- ป้องกันการเข้าถึงข้อมูลของท่านโดยไม่ได้รับอนุญาต โดยใช้การเข้ารหัสข้อมูล การตรวจสอบตัวตนและเทคโนโลยีการตรวจจับไวรัส ตามความจำเป็น รวมถึงจัดให้มีช่องทางการสื่อสารแบบปลอดภัยสำหรับ ข้อมูลดังกล่าวด้วยการเข้ารหัสลับข้อมูลดังกล่าว เช่น จัดให้มีการใช้ Secure - Socket Layer (SSL) protocol เป็นต้น
- บริหารจัดการให้ ผู้ให้บริการภายนอกที่โรงพยาบาลฯทำการว่าจ้าง ต้องปฏิบัติตามหลักเกณฑ์ตามกฎหมาย และระเบียบต่าง ๆ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- มีติดตามตรวจสอบเว็บไซต์และระบบออนไลน์ของโรงพยาบาลฯ ผ่านหน่วยงานที่มีความเชี่ยวชาญ ด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย
- จัดให้มีการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรของโรงพยาบาลฯ
- ประเมินผลแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การจัดการข้อมูล และการรักษาความมั่นคงปลอดภัยของข้อมูลของโรงพยาบาลฯ เป็นประจำ

อย่างไรก็ดีแม้ว่าโรงพยาบาลฯ จะทุ่มเทและใช้ความพยายามในการดูแลข้อมูลให้มีความปลอดภัยด้วยการใช้เครื่องมือ ทางเทคนิคร่วมกับการบริหารจัดการโดยบุคคล เพื่อควบคุมและรักษาความปลอดภัยของข้อมูล มิให้มีการเข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของเจ้าของข้อมูลโดยไม่ได้รับอนุญาต แต่ไม่อาจ รับประกันได้ว่าจะสามารถป้องกันความผิดพลาดได้ทุกประการ

9. สิทธิของเจ้าของข้อมูล

ในฐานะเจ้าของข้อมูลส่วนบุคคลท่านมีสิทธิร้องขอให้โรงพยาบาลฯ ดำเนินการเกี่ยวกับข้อมูลส่วน บุคคลของท่านตามขอบเขตที่กฎหมายอนุญาตให้กระทำได้ ดังนี้

9.1 สิทธิในการขอรับข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิที่จะขอรับสำเนาข้อมูลส่วนบุคคลของตน และมีสิทธิที่จะร้องขอให้ เปิดเผยถึงการได้มาซึ่งข้อมูลของเจ้าของข้อมูล

9.2 สิทธิ์ในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิที่จะคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนได้ ด้วยเหตุบางประการตามที่กฎหมายกำหนด

9.3 สิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ด้วยเหตุบางประการได้ตามที่กฎหมายกำหนด

9.4 สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิขอให้โรงพยาบาลฯ ระงับการใช้ข้อมูลส่วนบุคคลของตนเองด้วยเหตุบางประการตามที่กฎหมายกำหนด

9.5 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง: ในกรณีที่ข้อมูลส่วนบุคคลมีการเปลี่ยนแปลงเจ้าของข้อมูลสามารถดำเนินการยื่นคำขอแก้ไขข้อมูลดังกล่าวได้ เพื่อทำให้ข้อมูลส่วนบุคคลของ เจ้าของข้อมูลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

9.6 สิทธิในการเพิกถอนความยินยอม: เจ้าของข้อมูลมีสิทธิที่จะเพิกถอนความยินยอมเมื่อใดก็ได้ โดย การถอนความยินยอมดังกล่าวจะไม่กระทบต่อการประมวลผลข้อมูลส่วนบุคคลใด ๆ ที่เจ้าของข้อมูลได้ให้ความยินยอมไปแล้วก่อนหน้านี้ ทั้งนี้หากการถอนความยินยอมจะส่งผลกระทบต่อข้อมูลส่วนบุคคลในเรื่องใด สป.สธ. จะแจ้งให้เจ้าของข้อมูล ทราบถึงผลกระทบจากการถอนความยินยอม

อนึ่ง โรงพยาบาลฯอาจปฏิเสธคำขอใช้สิทธิข้างต้น หากการดำเนินการใด ๆ เป็นไปเพื่อวัตถุประสงค์หรือเป็นกรณีที่ ต้องปฏิบัติตามกฎหมายหรือคำสั่งศาล หรือเป็นกรณีที่อาจส่งผลกระทบและก่อให้เกิดความเสียหายต่อสิทธิหรือเสรีภาพของเจ้าของข้อมูลหรือบุคคลอื่น หรือเป็นการดำเนินการเพื่อการศึกษาวิจัยทางสถิติที่มีมาตรการปกป้องข้อมูลที่เหมาะสม หรือเพื่อการก่อตั้งสิทธิเรียกร้อง การปฏิบัติตามหรือการใช้สิทธิเรียกร้องหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

หากท่านต้องการใช้สิทธิ สามารถติดต่อมายังเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล ประจำหน่วยงานเพื่อดำเนินการยื่นคำร้องขอดำเนินการตามสิทธิข้างต้น ได้ตามช่องทางใน ข้อ 11

10. การปรับปรุงนโยบายการประมวลผลข้อมูลส่วนบุคคล

โรงพยาบาลฯ อาจมีปรับปรุงเนื้อหาของหนังสือแจ้งการประมวลผลนี้เป็นครั้งคราว เพื่อให้แน่ใจว่าเนื้อหาจะมีความเหมาะสมและเป็นปัจจุบัน หาก โรงพยาบาลฯ มีการปรับปรุงและแก้ไขหนังสือแจ้งฉบับนี้ จะแสดงบนทางเว็บไซต์ http://www.kingnaraihospital.go.th/ ของโรงพยาบาลฯ

11. ช่องทางการติดต่อ

ในกรณีที่เจ้าของข้อมูลต้องการใช้สิทธิ หรือมีคำถามเกี่ยวกับการใช้สิทธิของตน หรือความยินยอมที่เจ้าของข้อมูลได้ให้ไว้ ท่านสามารถติดต่อได้ที่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

สถานที่ติดต่อ งานเทคโนโลยีสารสนเทศ กลุ่มงานสุขภาพดิจิทัล โรงพยาบาลพระนารายณ์มหาราช

เลขที่ 260 ม.1 ตำบลเขาสามยอด อำเภอเมืองลพบุรี จังหวัดลพบุรี 15000

โทรศัพท์ 036-785-440-5 ต่อ 4530,4528

หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลนี้ มีผลบังคับใช้ตั้งแต่วันที่ สิงหาคม พ.ศ. 2567

(นางนุชรินทร์ อักษรดี)

ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช

ทำที่ โรงพยาบาลพระนารายณ์มหาราช

เลขที่ 260 หมู่ 1 ต. เขาสามยอด อ.เมือง จ.ลพบุรี 15000

วันที่.....เดือน.....พ.ศ.....

โดยหนังสือฉบับนี้ ข้าพเจ้า บริษัท.....โดย.....

ตำแหน่ง.....ผู้รับมอบอำนาจตามหนังสือมอมอบอำนาจฉบับลวันที่.....

สำนักงานเลขที่.....อาคาร.....ซอย.....ถนน.....

ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด..... (ซึ่งต่อไปในหนังสือฉบับนี้จะเรียกว่า "**ผู้รับข้อมูล**") ซึ่งเป็นผู้รับจ้างภายใต้สัญญาในโครงการ.....

ฉบับลงวันที่.....สัญญาเลขที่.....

ขอให้คำมั่นเพื่อผูกพันต่อ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล (ซึ่งต่อไปในหนังสือฉบับนี้จะเรียกว่า"**ผู้ให้ข้อมูล**") โดยมีรายละเอียดและเงื่อนไข ดังนี้

ข้อ 1. คำนิยาม

"สัญญา" หมายถึง สัญญาในโครงการ.....

ฉบับลงวันที่.....สัญญาเลขที่.....

"วัตถุประสงค์" หมายถึง วัตถุประสงค์ตามสัญญา

"ผู้มีอำนาจ" หมายถึง บุคคลที่เกี่ยวข้องโดยตรงกับการปฏิบัติงานตามสัญญา และมีความจำเป็นอย่างยิ่งที่จะต้องได้รับการเปิดเผยซึ่งข้อมูลอันเป็นความลับเพื่อดำเนินการให้สำเร็จตามวัตถุประสงค์

" ข้อมูลอันเป็นความลับ " หมายถึง ข้อมูลใดๆ ไม่ว่าอยู่ในลักษณะและรูปแบบใด ที่ผู้ให้ข้อมูลได้เปิดเผยต่อผู้รับข้อมูล ทั้งที่ได้เปิดเอมาก่อนหรือหลังจากวันที่ลงนามในหนังสือแสดนาฉบับนี้

ทั้งนี้ ข้อมูลอันเป็นความลับ ให้หมายความรวมถึงข้อมูลดังต่อไปนี้ด้วย

(1) ข้อมูลของระบบ ข้อมูลลูกค้า ตลอดจนข้อมูลอื่นใดที่อาจก่อให้เกิดความเสียหายกับผู้ให้ข้อมูล

(2) ข้อมูลเกี่ยวกับระบบทั้งหมดที่ผู้ให้ข้อมูลพัฒนาขึ้น ไม่ว่าจะพัฒนาขึ้นเองหรือจ้างบุคคลภายนอกพัฒนาขึ้น ตัวอย่างเช่น รูปแบบการนำส่งข้อมูล, ข้อกำหนดของระบบ, คุณสมบัติของระบบบ, ความรู้ทางด้านเทคนิค ความชำนาญ, วิธีการจัดการ, ชื่อบัญชีผู้ใช้งาน (User Name/User ID) และรหัสผ่าน (Password) เป็นต้น

(3) ข้อมูลไม่ว่าอยู่ในลักษณะและรูปแบบใดที่มีเนื้อหาที่ไม่พึงเปิดเผยแก่บุคคลทั่วไป หรือเป็นความลับทางการค้า หรือผลการวิจัย การวิเคราะห์ ศึกษา รายงาน บันทึก

(4) ภาพถ่าย หรือสำเนา ของข้อมูลอันเป็นความลับ

ข้อ 2. การรักษาความลับและข้อกำหนดในการเข้าติดต่อประสานงาน

2.1 ผู้รับข้อมูลตกลงที่จะปฏิบัติตนตาม กฎ ระเบียบ แนวปฏิบัติ นโยบาย ข้อบังคับ รวมถึงข้อตกลงต่างๆ และกฎหมายใดๆ ที่เกี่ยวข้องกับการดำเนินงานของผู้ให้ข้อมูล

2.2 ผู้รับข้อมูลจะไม่ใช้ข้อมูลอันเป็นความลับ ไม่ว่าทั้งหมดหรือเพียงบางส่วน เพื่อวัตถุประสงค์อื่นใดนอกจากวัตถุประสงค์ของสัญญา

2.3 รับข้อมูลจะไม่เปิดเผยข้อมูลอันเป็นความลับให้แก่บุคคลใดๆ (รวมทั้ง กรรมการ เจ้าหน้าที่ ตัวแทน ผู้แทน ตลอดจนที่ปรึกษา ของผู้ให้ข้อมูลและผู้รับข้อมูล) โดยปราศจากความยินยอมเป็นอักษรจากผู้ให้ข้อมูลก่อน เว้นแต่บุคคลดังกล่าวจะเป็นผู้มีอำนาจ ทั้งนี้ ผู้รับข้อมูลมีหน้าที่ต้องดำเนินการให้ผู้มีอำนาจบุคคลที่เกี่ยวข้อโดยตรงกับการปฏิบัติงานตามสัญญา ปฏิบัติตามข้อกำหนดและเงื่อนไขการรักษาความลับซึ่งเป็นข้อกำหนดและเงื่อนไขที่ไม่น้อยกว่าข้อกำหนดและเงื่อนไขของหนังสือฉบับนี้ และหากผู้ให้บข้อมูลต้องดำเนินการให้ผู้มีอำนาจและบุคคลที่เกี่ยวข้องโดยตรงกับการปฏิบัติงานตามสัญญา ลงนางมในหนังสือแสดงเจตนาไม่เปิดเผยข้อมูล หรือในสัญญารักษาความลับตามที่ผู้ให้ข้อมูลกำหนดด้วย ในการนี้ หากผู้มีอำนาจและบุคคลที่เกี่ยวข้องโดยตรงกับการปฏิบัติงานตามสัญญา ไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขการรักษาเจตนาไม่เปิดเผยข้อมูล หรือสัญญารักษาความลับดังกล่าว ผู้รับข้อมูลต้องชำระค่าชดเชยควเกิดขึ้นแก่ผู้ให้ข้อมูลทั้งนี้ ผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบทันทีที่ล่วงรู้ว่าได้มีการนำข้อมูลอันเป็นความลับไปเปิดเผยต่อบุคคลโด หรือตกอยู่ในครอบครองของบุคคลใดซึ่งไม่ใช่ผู้มีอำนาจ

2.4 ผู้รับข้อมูลจะไม่ทำซ้ำ สำเนา หรือทำสรุปย่อ หรือทำหรือทำบันทึกรายการ เกี่ยวกับรายละเอียดข้อมูลอันเป็นความลับไม่ว่าทั้งหมดหรือในส่วนใดส่วนหนึ่ง เว้นแต่เป็นเรื่องที่จำเป็นอย่างยิ่งเพื่อดำเนินการตามวัตถุประสงค์ รวมทั้งได้แจ้งให้ผู้ให้ข้อมูลได้รับทราบเป็นลายลักษณ์อักษรก่อนดำเนินการแล้ว และให้ถือว่าสำเนา สรุปย่อ และบันทึกรายการดังกล่าว เป็นข้อมูลอันเป็นความลับ ซึ่งผู้รับข้อมูลจะต้องแสดงให้เห็นอย่างชัดแจ้งว่าสำเนา สรุปย่อ และบันทึกรายการดังกล่าวเป็นข้อมูลอันเป็นความลับด้วย

2.5 ผู้รับข้อมูลจะไม่ใช้ข้อมูลอันเป็นความลับ ไปในทางที่ทำให้หรืออาจทำให้เกิดความเสียหายหายต่อผู้ให้ข้อมูล ไม่ว่าโดยทางตรงหรือทางอ้อม

2.6 ผู้รับข้อมูลจะเก็บรักษาข้อมูลอันเป็นความลับไว้ในสถานที่ปลอดภัย และจะปฏิบัติต่อข้อมูลอันเป็นความลับด้วยวิธีการที่เหมาะสมและมีมาตรฐานเพียงพอ ที่จะป้องกันไม่ให้มีการเข้าถึงข้อมูลอันเป็นความลับ หรือมีการนำข้อมูลอันเป็นความลับนั้นไปเปิดเผย หรือนำไปทำสำทำสำสำเนา หรือนำไปใช้ โดยมิได้รับอนุญาตจาตจากผู้ให้ข้อมูล

2.7 ผู้รับข้อมูลต้องแจ้งรายชื่อของบุคคลที่จะเข้าปฏิบัติงานตามสัญญาต่อผู้ให้ข้อมูลก่อนเริ่มปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน ผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบเพื่อให้ผู้ให้ข้อมูลให้ความเห็นชอบล่วงหน้าทุกครั้ง

2.8 ผู้รับข้อมูลต้องได้รับข้อมูลอันเป็นความลับโดยวิธีการตามที่ผู้ให้ข้อมูลกำหนด (เช่น กำหนดตัวบุคคลผู้มีสิทธิเปิดเผยข้อมูลต่อผู้รับข้อมูล กำหนดวิธีการส่งมอบข้อมูลให้แก่ผู้รับข้อมูล เป็นต้น) และในกรณีที่ผู้รับข้อมูลได้รับข้อมูลอันเป็นความลับโดยวิธีการที่แตกต่างจากวิธีการตามที่ผู้ให้ข้อมูลกำหนด ผู้รับข้อมูลลต้องแจ้งให้ผู้ให้ข้อมูลทราบ โดยทันที

ข้อ 3. ระยะเวลาในการรักษาความลับ

ผู้รับข้อมูลจะเก็บรักษาข้อมูลอันเป็นความลับที่ได้รับมา ไว้เป็นความลับตลอดไป แม้ว่าสัญญาหรือหนังสือแสดงเจตนาฉบับนี้จะสิ้นสุดลงแล้ว ไม่ว่าด้วยเหตุใดๆ ก็ตาม

ข้อ 4. การรับรองให้เป็นทรัพย์สินของผู้ให้ข้อมูล

ข้อมูลอันเป็นความลับ และข้อมูลใดๆ ที่ได้มาจากหรือเกิดขึ้นมาจากการปฏิบัติงานตามสัญญา (รวมถึงสำเนาของข้อมูลดังกล่าว ไม่ว่าอยู่ในลักษณะและรูปแบบใด) ถือเป็นทรัพย์สินของผู้ให้ข้อมูลแต่เพียงผู้เดียว

ข้อ 5. การส่งคืนหรือทำลายข้อมูลอันเป็นความลับ

เมื่อสัญญาสิ้นสุดลง หรือเมื่อได้รับการร้องขอจากผู้ให้ข้อมูล ผู้รับข้อมูลต้องส่งคืนซึ่งข้อมูลอันเป็นความลับและข้อมูลใดๆ ที่ได้มาจากหรือเกิดขึ้นมาจากการปฏิบัติงานตามสัญญา (รวมถึงสำเนาของข้อมูลดังกล่าว ไม่ว่าอยู่ในลักษณะและรูปแบบใด) ให้แก่ผู้ให้ข้อมูลทันที หรือทำลายทิ้งทันทีในกรณีที่ผู้ให้ข้อมูลมีความประสงค์ให้ทำลาย โดยผู้รับข้อมูลต้องแจ้งต่อผู้ให้ข้อมูลเป็นลายลักษณ์อักษรว่า ได้ทำลายข้อมูลอันเป็นความลับและสำเนาทั้งหมดของข้อมูลอันเป็นความลับนั้นแล้ว และหากผู้ให้ข้อมูลร้องขอ ผู้รับข้อมูลต้องจัดการอำนวยความสะดวกให้แก่ผู้ให้ข้อมูลเข้าตรวจสอบทุกขั้นตอนในการส่งคืนหรือทำลายข้อมูลอันเป็นความลับทั้งหมด ทั้งนี้ กระบวนการดังกล่าวถือเป็นกระบวนการที่ผู้รับข้อมูลต้องเก็บเป็นความลับด้วยเช่นกัน

ข้อ 6. ทรัพย์สินทางปัญญา

ผู้รับข้อมูลตกลงว่า ทรัพย์สินทางปัญญาใดๆ ซึ่งรวมถึง ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า และสิทธิอื่นใดที่เกี่ยวข้องกับทรัพย์สินทางปัญญา ซึ่งเกี่ยวกับ หรือเป็นผลมาจาก หรือเกิดขึ้นเนื่องมาจาก การปฏิบัติงานตามสัญญา หรือการได้รู้หรือได้ใช้ข้อมูลอันเป็นความลับ ให้ทรัพย์สินทางปัญญาดังกล่าวตกเป็นของผู้ให้ข้อมูลแต่เพียงผู้เดียว

ข้อ 7. การไม่ประกอบธุรกิจแข่งขันกับการดำเนินงานของผู้ให้ข้อมูล

ผู้รับข้อมูลจะไม่ประกอบกิจการใดหรือกระทำการใดอันเป็นการแข่งขันหรืออาจเป็นการแข่งขันกับการดำเนินงานของผู้ให้ข้อมูล และจะไม่ให้ความช่วยเหลือ หรือให้คำปรึกษาแก่บุคคลภายนอก หรือบุคคลอื่น อันอาจเป็นทางเสียหายหรือเป็นการแข่งขันกับการดำเนินงานของผู้ให้ข้อมูล ไม่ว่าจะโดยทางตรงหรือทางอ้อม ไม่ว่าข้อมูลหรือคำปรึกษานั้นจะถูกนำไปใช้ประโยชน์ในด้านใดก็ตาม

ข้อ 8. การแยกส่วนที่เป็นโมฆะออกจากส่วนที่สมบูรณ์

ในหนังสือฉบับนี้ หากมีข้อความหรือข้อกำหนดใดที่ตกเป็นโมฆะหรือไม่สมบูรณ์ไม่ว่าด้วยเหตุใดๆ ก็ตาม ผู้รับข้อมูลตกลงให้แยกส่วนที่เป็นโมฆะหรือที่ไม่สมบูรณ์นั้น ออกจากข้อความหรือข้อกำหนดอื่นๆ ที่สมบูรณ์ โดยให้ถือว่าข้อความหรือข้อกำหนดอื่นๆ ที่สมบูรณ์มีผลผูกพันและใช้บังคับได้ตามกฎหมาย

ข้อ 9. การแก้ไขเยียวยา

ผู้ให้ข้อมูลมีสิทธิเรียกร้องให้ผู้รับข้อมูลชดใช้ค่าเสียหาย และ/หรือ ค่าใช้จ่ายอื่นใดที่เกิดขึ้น หรืออาจเกิดขึ้นอันเนื่องมาจากการที่ผู้รับข้อมูลปฏิบัติผิดข้อกำหนดข้อหนึ่งข้อใดในหนังสือฉบับนี้ รวมถึงที่เกิดจากการเรียกร้อง ฟ้องร้องดำเนินคดี และการบังคับตามกฎหมายทุกประการ

ข้อ 10. การเปลี่ยนแปลงแก้ไข

การเปลี่ยนแปลงแก้ไขข้อความหรือข้อกำหนดโดยๆ ในหนังสือฉบับนี้ จะกระทำไม่ได้ เว้นแต่ผู้ให้ข้อมูลจะได้ให้ความยินยอมเป็นลายลักษณ์อักษรก่อน

ผู้รับข้อมูลได้อ่านและเข้าใจข้อความในหนังสือแสดงเจตนาไม่เปิดเผยข้อมูลฉบับนี้โดยตลอดและยินยอมตามนั้น จึงได้ลงลายมือชื่อและประทับตรา (ถ้ามี) ไว้เป็นสำคัญ

ลงชื่อ.....ผู้รับข้อมูล

(.....)

ตำแหน่ง.....

บริษัท.....

วันที่.....

โรงพยาบาลพระนารายณ์มหาราช

บันทึกรายการประมวลผลข้อมูลส่วนบุคคลของ โรงพยาบาลพระนารายณ์มหาราช
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

โรงพยาบาลพระนารายณ์มหาราช กำหนดกรอบการทำงานของผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจากมาตรา ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่องการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้

โดยในทุกกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการจัดทำตารางบันทึกการประมวลผลในรูปแบบอิเล็กทรอนิกส์ ประกอบด้วยหัวข้อต่าง ๆ ดังนี้

๑. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

ชื่อผู้ควบคุมข้อมูล	กลุ่มภารกิจสุขภาพดิจิทัล โรงพยาบาลพระนารายณ์มหาราช
ที่อยู่	ที่อยู่ เลขที่ ๒๕๐ หมู่ ๑ ตำบลเขาสามยอด อำเภอเมือง จังหวัด ลพบุรี ๑๕๐๐๐
ข้อมูลการติดต่อ	
เจ้าหน้าที่คุ้มครองข้อมูล ส่วน บุคคล (ถ้ามี)	ชื่อ พญ.ชลมาศ ตริตรอง ที่อยู่ โรงพยาบาลพระนารายณ์มหาราช
ผู้ประสานงาน/ผู้แทน	

๒. บันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) แยกออกเป็น ๒ ตาราง ย่อย ๒.๑ และ ๒.๒ คือ จัดเก็บข้อมูลหลัก (ไม่ค่อยเปลี่ยนแปลง) และกิจกรรมของข้อมูล (แยกตามรายการเปลี่ยนแปลง)

ตารางที่ ๒.๑

ลำดับ	ชื่อรายการ	ตัวอย่างการบันทึก
๑	ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	๑. ข้อมูลส่วนบุคคลทั่วไป ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้ตัวอย่างการบันทึกสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม (ตาม ม.๖๔ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒) เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน พาสปอร์ต วันเกิด หมายเลขประจำตัวผู้ป่วย เบอร์โทรศัพท์ ๒. ข้อมูลส่วนบุคคลอ่อนไหว (ตาม ม.๒๖ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒) เช่น ข้อมูลสุขภาพ ข้อมูลความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ(Biometric)
๒	วัตถุประสงค์ของการเก็บรวบรวม	๑. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูล ส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม (อุบัติเหตุ ฉุกเฉิน) ๒. เป็นการปฏิบัติตามกฎหมาย หน้าที่และอำนาจตามพระราชบัญญัติ ปรับปรุงกระทรวง ทบวง กรม พ.ศ.ศ. ๒๕๔๕และกฎหมายลำดับรอง กฎกระทรวงแบ่งส่วนราชการ เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ ๓. จำเป็นในการดำเนินภารกิจเพื่อประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพ ของยาเวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

๓	ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล	กลุ่มงานเทคโนโลยีสารสนเทศและดิจิทัลโรงพยาบาลพระนารายณ์มหาราช
๔	ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	ระยะเวลาในการจัดเก็บเวชระเบียนผู้ป่วย พิจารณาระยะเวลาในการจัดเก็บรักษาที่จำเป็นและเหมาะสมภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย หมวดที่ ๓ ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ.๒๕๒๖ ดังนี้ เรื่องการเก็บรักษาและทำลายหนังสือ ข้อ ๕๗ - ผู้ป่วยนอก กำหนดระยะเวลา ๑๐ ปี (อายุการเก็บ ปกติเก็บไว้ไม่น้อยกว่า ๑๐ ปี หากแต่ขาดการติดต่อเกิน ๑๐ ปี จึงทำลาย) ข้อ ๕๗.๔ - ผู้ป่วยใน กำหนดระยะเวลา ๕ ปี (ถึงกำหนดเวลา ทำลายตามระเบียบ)
๕	สิทธิและวิธีการถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลบุคคลนั้น	๑. เฉพาะเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศและดิจิทัลโรงพยาบาลพระนารายณ์มหาราช ที่ได้รับมอบหมายหน้าที่ให้เป็นผู้ดูแลระบบฐานข้อมูลซึ่งสามารถเข้าถึงได้ผ่าน Software ที่ได้รับอนุญาตเท่านั้น ๒. บุคลากรกลุ่มงานทรัพยากรบุคคลและบุคลากรทางการแพทย์ที่มีการจำกัดสิทธิ์ในการเข้าถึงข้อมูลและสามารถเข้าถึงข้อมูลในส่วนที่เกี่ยวข้องกับบุคลากรในส่วนที่กำหนดเท่านั้น
๖	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม	๑. โรงพยาบาลพระนารายณ์มหาราชได้นำข้อมูลไปทำสถิติและหาที่ได้รับการยกเว้นไม่ต้องขอความยินยอมหลักสูตรของผู้เข้าร่วมการอบรมโดยไม่ระบุชื่อความสัมพันธ์ระหว่างวิทยากรกับความพึงพอใจที่มีต่อจำเพาะตัวบุคคล ๒. กลุ่มงานเทคโนโลยีสารสนเทศและดิจิทัล ได้นำข้อมูล ๕๓ แฟ้มไปยัง HDC กระทรวงสาธารณสุข ๓. กลุ่มงานเทคโนโลยีสารสนเทศและดิจิทัล ได้นำข้อมูล ๕๓ แฟ้มไปยัง Data Center ของกรสุขภาพจิต ๔.กลุ่มงานเทคโนโลยีสารสนเทศและดิจิทัล นำส่งข้อมูลบุคลากรในกลุ่มงานต่างๆของ โรงพยาบาลเพื่อหัวหน้างานหรือกรรมการด้านต่างๆที่ได้ทำการกรอกแบบฟอร์มขอข้อมูลในระบบเพื่อทำเป็นข้อมูลประกอบการพิจารณาด้านต่างๆ

๗	มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรา ๓๗ (๑)	๑) การธำรงไว้ซึ่งความลับ (confidentiality) ● มีการกำหนดและจำกัดสิทธิ์ในการเข้าถึงข้อมูลในการใช้ระHIS ของรพ.เพื่อการรักษาความลับของข้อมูลผู้ป่วย มีการยืนยันตัวตน กำหนดชั้นความลับในการเข้าถึงของข้อมูลส่วนบุคคล และมีการกำหนดรหัสบุคคลในการเข้าระบบอินเทอร์เน็ตและระบบอินทราเน็ตของโรงพยาบาล มีระบบ Wi-Fi ที่แยกการใช้งานของบุคคลภายนอกกับระบบรพ. มีแนวปฏิบัติด้านสารสนเทศ มีการประกาศนโยบายที่เกี่ยวข้องให้บุคลากรและบุคคลภายนอกได้รับทราบผ่านทางเว็บไซต์และการแจ้งเวียนหนังสือภายใน ● มีห้องปฏิบัติการควบคุมระบบคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บเครื่องแม่ข่ายและอุปกรณ์ระบบ network โดยมีการติดตั้งระบบสแกนลายนิ้วมือเพื่อพิสูจน์ตัวตนก่อนเข้าห้องปฏิบัติการและมีการบันทึกผลการปฏิบัติงานทุกครั้งที่มีการเปลี่ยนแปลงหรือตรวจสอบเครื่องแม่ข่ายหรืออุปกรณ์ ● มีแนวทางการรักษาความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ มีการประกาศแนวทางการรักษาความมั่นคงปลอดภัย จากการประเมินพบว่า ผู้ใช้งานรับทราบนโยบายและเริ่มตระหนักถึงความสำคัญของความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ และจากการตรวจสอบรายงานความเสี่ยงในปี ๒๕๖๕ ยังไม่พบการรายงานความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล ● มีการบริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล เช่น การขยายผล Consent Form, การคุ้มครองข้อมูลส่วนบุคคล เป็นต้น ผลลัพธ์ที่ได้ คือ ผู้บัวยสามารถร้องขอประวัติการรักษาผ่านApplication ผ่านอุปกรณ์อิเล็กทรอนิกส์ของผู้ป่วยได้ โดยมีระบบ

		Consent form เพื่อแสดงการยืนยอมการเปิดเผยข้อมูล และแพทย์ผู้รักษาสามารถดูประวัติการรักษาได้ในทันทีผ่านระบบ โดยไม่ต้องรอเอกสารการรักษาจากโรงพยาบาลต้นสังกัดและมีความสะดวกรวดเร็วต่อการรักษาในกรณีที่มีการเดินทางข้ามจังหวัด ซึ่งข้อมูลที่ส่งเข้าระบบจากโรงพยาบาลสวนปรุงมีการเข้ารหัสมาตรฐาน Fast Healthcare Interoperability Resources (FHIR) จากองค์กร Health Level Seven (HL๗) International ซึ่งเป็นมาตรฐานการแลกเปลี่ยนข้อมูลสุขภาพซึ่งมีความน่าเชื่อถือด้านความปลอดภัยของข้อมูล ● มีการกำหนดผู้ดูแลบริหารจัดการระบบฐานข้อมูลและระบบเครือข่าย คณะกรรมการธรรมาภิบาลข้อมูล เพื่อดูแล ตรวจสอบรักษาความปลอดภัยของข้อมูล ดูแลป้องกันการบุกรุกของระบบเครือข่าย (Firewall) หรือระบบตรวจสอบการเชื่อมต่อที่ไม่พึงประสงค์ของเครือข่าย (Instruction Detection System : IDS) จากเครือข่ายภายนอก โดยผู้ดูแลระบบจะทำการตรวจสอบระบบทุกเช้าเวลา ๐๘.๐๐ - ๖๙.๐๐ น.ในวันทำการและปฏิบัติตามระเบียบปฏิบัติแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan) กรณีเกิดเหตุการณ์ไม่พึงประสงค์ (เช่น เครื่องคอมพิวเตอร์ภายในโรงพยาบาลพระนารายณ์มหาราช หรือตรวจพบว่าถูกโจมตีจากครือข่ายภายนอกดังที่เกิดขึ้นในปี ๒๕๖๖ sever ของโรงพยาบาลติดไวรัสเรียกค่าไถ่ทำให้ข้อมูลถูกเข้ารหัสหรือล็อกไฟล์ ไม่สามารถเข้าถึงเรียกใช้ข้อมูล/กู้คืนข้อมูลได้ เกิดความเสียหายกับข้อมูลของโรงพยาบาล) จากการประเมินและความคุมความเสียงที่สำคัญในปี ๒๕๖๓-๒๕๖๕ และได้ทำการเฝ้าระวังอย่างต่อเนื่องยังไม่พบรายงานอุบัติการณ์ของหน่วยงาน

หมายเหตุ

๑. ข้อมูลต่าง ๆ ที่บันทึกในตารางช้างต้นเป็นขั้นต่ำตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนด ผู้ใช้งานสามารถปรับเพิ่มเติมได้ตามความเหมาะสม

๒. เมื่อนำไปใช้งานจริง ตารางต่าง ๆ สามารถนำไปพัฒนาลงในฐานข้อมูล หรือ จัดเก็บด้วยซอฟต์แวร์ประเภทสเปรดชีต ตามที่ผู้ใช้เห็นสมควร หรืออาจจะพัฒนาโปรแกรมเพื่อสร้างส่วนติดต่อผู้ใช้สำหรับบันทึกข้อมูลผ่านระบบออไลน์/ออไฟไลน์ ได้

๓.การพัฒนากระดานรายงานข้อมูล (dashboard) สามารถพัฒนาเพิ่มเติมได้เองตามที่ต้องการ

ประกาศ ณ วันที่ สิงหาคม ๒๕๖๗

(นางนุชรินทร์ อักษรดี)
ผู้อำนวยการโรงพยาบาลพระนารายณ์มหาราช