คู่มือการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

บันทึกประวัติการแก้ไขเอกสาร (Revision History)

แก้ไขครั้งที่ (No.)	วันที่จัดทำ (Date)	รายละเอียดการแก้ไขเอกสาร (Description of revision)	วันที่บังคับใช้ (Effective date)
00	2 พ.ค. 2565	จัดทำเอกสารและขออนุมัติประกาศใช้	1 มิ.ย. 2565

สารบัญ

คู่มือระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

ปัจจุบันมีการเปลี่ยนแปลง พัฒนาเรื่องเทคโนโลยีให้ก้าวหน้ามากขึ้นเป็นอย่างมาก ทำให้การเก็บรวบรวมให้เปิดเผยข้อมูลส่วนบุคคลทำได้ง่ายสะดวกและรวดเร็วจึงอาจก่อให้เกิดการละเมิดสิทธิส่วนบุคคล ของเจ้าของข้อมูล อันเป็นเหตุให้เกิดความเสียหายเป็นอย่างมาก นอกจากนี้ยังก่อให้เกิดความเสียหายแก่ บริษัท ผู้ประกอบการและกระทบต่อความน่าเชื่อถือและภาพลักษณ์อันดีงามขององค์กร บริษัท โรงพยาบาลศุภมิตร จำกัด (มหาชน) ผู้ประกอบกิจการ โรงพยาบาล ได้ให้ความสำคัญในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้าธุรกิจ และ พันธมิตรทางธุรกิจ โดยโรงพยาบาลจะปกป้องข้อมูลส่วนบุคคลจากการถูกนำไปใช้ในนอกเหนือวัตถุประสงค์ และรักษาข้อมูลดังกล่าวให้ปลอดภัยตามกฎหมายและตามหลักมาตรฐานสากล เพื่อให้สอดคล้องกับการ ดำเนินธุรกิจในปัจจุบัน โรงพยาบาลจึงจัดให้มีระบบการเก็บรวบรวมไม่เปิดเผย และโอนข้อมูลส่วนบุคคลไป ยังบุคคลที่สาม ซึ่งข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลที่เป็นเจ้าของข้อมูล อาจส่งผลให้เป็นยืนยันถึงตัวตน ของเจ้าของข้อมูลไม่ว่าทางตรงหรือทางอ้อมได้ โรงพยาบาลจึงกำหนด ให้มีคู่มือระบบบริหารจัดการคุ้มครอง ข้อมูลส่วนบุคคล ดังนี้

1. นโยบายการคุ้มครองข้อมูลส่วนบุคคล

โรงพยาบาลให้ความสำคัญต่อการรักษาข้อมูลส่วนบุคคล ทั้งของพนักงานและผู้ที่เกี่ยวข้องทั้งหมด อาทิเช่น ลูกค้า คู่ค้าคู่สัญญา ผู้รับจ้างเหมา ผู้ให้บริการ ผู้เข้าเยี่ยมชมโรงพยาบาล ผู้มาติดต่อ เป็นต้น ที่ต้อง ได้รับความคุ้มครองทางกฎหมาย และแนวปฏิบัติมาโดยตลอด ซึ่งการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์ โดยมิชอบหรือเปิดเผยข้อมูลที่อาจทำให้เกิดความเสียหายหรือทำให้สามารถระบุถึงตัวบุคคล โดยไม่ได้รับความ ยินยอมเป็นการกระทำการละเมิด ผิดกฎหมายและข้อบังคับการทำงาน โรงพยาบาลจึงได้กำหนดนโยบายการ คุ้มครองข้อมูลส่วนบุคคล ดังนี้

"โรงพยาบาลจะบริหารจัดการ กำหนดให้มีมาตรการและแนวทางปฏิบัติที่จำเป็นที่เป็นการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและควบคุมการปฏิบัติงานภายในองค์กรให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูล บุคคลพ.ศ.2562 และกฎหมายที่เกี่ยวข้องเพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะได้รับความคุ้มครองตามที่กฎหมายกำหนด "

โรงพยาบาลจะรักษาคุ้มครองข้อมูลส่วนบุคคล และกำหนดให้มีมาตรการและแนวทางปฏิบัติที่จำเป็น เพื่อคุ้มครองข้อมลส่วนบุคคลที่ถูกเก็บรวบรวมใช้และเปิดเผย โดยบริษัทให้เป็นไปตามที่กฎหมายกำหนด

2. วัตถุประสงค์ของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

2.1 เพื่อรักษามาตรฐานความรับผิดขอบที่องค์กรมีต่อพนักงานและผู้ที่เกี่ยวข้องทั้งหมดลูกค้าคู่ค้า คู่สัญญาผู้รับจ้างเหมาผู้ให้บริการผู้เข้าเยี่ยมชมโรงพยาบาลหรือเว็บไซด์ ผู้มาติดต่อให้ได้รับการเก็บรักษา อย่างถูกต้อง ปลอดภัย และใช้งานโดยสุจริต รวมถึงเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วน บุคคล พ.ศ.2562

2.2 เพื่อเป็นแนวปฏิบัติในการบริหารจัดการได้แก่การเก็บรวบรวม การนำข้อมูลเพื่อประมวลผล การ เปิดเผย การจัดการข้อมูลและการนำข้อมูลไปใช้เพื่อกิจการโรงพยาบาล มีความมั่นคงปลอดภัย น่าเชื่อถือ มีการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว

2.3 เพื่อป้องกันความเสียหายที่เกิดจากการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์โดยมิชอบด้วยกฎหมาย

3. กฎหมายที่บังคับใช้

โรงพยาบาลได้กำหนดระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อเป็นแนวปฏิบัติของ พนักงานทุกคน ในการกำหนดมาตรฐาน1ขั้นต่ำสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผย ซึ่งอยู่ในบังคับของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ตลอดจนกฎหมายและประกาศ และระเบียบอื่นที่ เกี่ยวข้อง

ระบบการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลนี้ ประกอบด้วยนโยบายคุ้มครองข้อมูลส่วนบุคคล คู่มือระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล ข้อกำหนด ระเบียบปฏิบัติ และเอกสารแนบท้ายในกรณีที่ เอกสารใดมีข้อความที่ขัดหรือแย้งกันให้บังคับตามคู่มือระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้

4. ขอบเขตการใช้บังคับ

4.1 การบังคับใช้ให้ครอบคลุมกับคณะกรรมการ กรรมการ ผู้บริหาร และพนักงาน ทุกระดับ รวมถึง คู่ค้า คู่สัญญา และผู้มีส่วนได้เสียกับโรงพยาบาล

4.2 การบังคับใช้ให้ครอบคลุมกับทุกกิจกรรมการดำเนินงานของโรงพยาบาลที่เกี่ยวข้องกับข้อมูลส่วน บุคคล ได้แก่ วิธีการจัดเก็บข้อมูล ประเภท และรูปแบบของข้อมูลที่จัดเก็บ วัตถุประสงค์ของโรงพยาบาล ใน การนำข้อมูลส่วนบุคคลไปใช้ การแบ่งเป็นข้อมูลดังกล่าวให้กับบุคคลอื่น ตลอดจนวิธีการที่โรงพยาบาล ดำเนินการปกป้องข้อมูลส่วนบุคคลของลูกค้า

4.3 การคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ครอบคลุมการประมวลผลข้อมูลทั้งหมด ตั้งแต่การเก็บ รวบรวม ใช้ เปิดเผย

4.4 การคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลทุกคนประกอบด้วย

(1) คณะกรรมการบริษัท ผู้บริหารทุกระดับ

(2) ผู้สมัครงาน

(3) พนักงาน

(4) ลูกจ้างชั่วคราว และนักศึกษาฝึ)กงาน

(5) ลูกค้า

(6) คู่ค้า คู่สัญญา

(7) ผู้รับจ้างเหมา ผู้ให้บริการ

(8) ผู้เข้าเยี่ยมชมโรงพยาบาล หรือเว็บ,ไซด์

(9) ข้อมูลส่วนบุคคลที่ได้รับมาจากการรับจ้างประมวลผลข้อมูล

(10) ผู้มาติดต่อ

4.5 ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศผู้รับโอนมีมาตรฐานคุ้มครอง ข้อมูลส่วนบุคคลสูงกว่าที่กำหนดในเอกสารฉบับนี้ให้โรงพยาบาลปฏิบัติตามกฎหมายดังกล่าว

4.6 ในกรณีที่ไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศผู้รับโอนใช้บังคับกับการ ประมวลผลข้อมูลส่วนบุคคล หรือเป็นกรณีที่กฎหมายชองประเทศบั้นมีมาตรฐานต่ำกว่าที่กำหนดในเอกสารฉบับนี้โรงพยาบาลจะต้องปฏิบัติตามเงื่อนไขที่กำหนดไว้ในเอกสารฉบับนี้

5. ความหมายและนิยาม

5.1 โรงพยาบาล หมายถึง บริษัท

5.2 ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

5.3 เจ้าของข้อมูลส่วนบุคคล หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล แต่ไม่ใช่กรณีที่บุคคลที่ ครอบครองข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลจะหมายถึง บุคคลธรรมดาเท่านั้น และไม่รวมถึงนิติบุคคล

5.4 ประเภทของเจ้าของข้อมูลส่วนบุคคล หมายถึง เจ้าของข้อมูลส่วนบุคคลที่โรงพยาบาลเก็บและ ประมวลผลข้อมูลส่วน บุคคล ได้แก่ ลูกค้า นักลงทุน คู่ค้า คู่สัญญา ที่ปรึกษา ผู้ประกอบวิชาชีพ พนักงาน เจ้าหน้าที่ ลูกจ้าง ตัวแทน ผู้สมัคร งาน ผู้ใช้บริการเว็บไซต์และบุคคลใดๆ ที่เกี่ยวข้องกับกิจกรรม การดำเนิน ธุรกิจและการ ดำเนินงานต่างๆ ของโรงพยาบาล

5.5 ข้อมูลอ่อนไหว ได้แก่ ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ พันธุกรรม ข้อมูลชีวภาพข้อมูลภาพจำลองใบหน้าม่านตาหรือลายนิ้วมือข้อมูลสหภาพแรงงานหรือข้อมูล อื่นใดซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ประกาศ ให้เป็นข้อมูลข้อมูลส่วนบุคคลที่มีความอ่อนไหว

5.6 คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล หมายถึง พนักงานของโรงพยาบาล ที่ได้รับ การมอบหมายให้ทำหน้าที่ให้ความรู้ ขับเคลื่อนนโยบาย และกำกับดูแลนโยบายและแนวปฏิบัติในการคุ้มครอง ข้อมูลส่วนบุคคลของพนักงาน ลูกค้า คู่ค้า คู่สัญญาและผู้เกี่ยวข้อง

5.7 ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller หมายถึงผู้ที่ได้รับมอบหมายให้มีอำนาจหน้าที่ เก็บรักษา ประมวลผลใช้ควบคุมและตรวจสอบข้อมูลส่วนบุคคล ที่ใช้ในการวิเคราะห์ รายงาน และหรือสรุป เพื่อใช้ในกิจการของโรงพยาบาลโดยสุจริต

5.8 ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง ผู้ที่ได้รับมอบหมายให้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล โดยบุคคลหรือ นิติบุคคลดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

5.9 เจ้าหน้าที่คุมครองข้อมูลส่วนบุคคลหรือData Protection Officer : DPO) หมายถึงผู้ที่ดูแล รักษาข้อมูลส่วนบุคคลทั้งหมด ในองค์กรไม่ว่าจะเป็นองค์กรข้อมูลภายใน (ข้อมูลบุคลากร) หรือภายนอก (ข้อมูลลูกค้า และคู่ค้า คู่สัญญา) ตั้งแต่ตรวจสอบการรวบรวมข้อมูลจนถึงนำไปใช้ เผยแพร่ จัดเก็บ และ ประลานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

5.10 การละเมิดข้อมูลส่วนบุคคล หมายถึง ข้อมูลส่วนบุคคลที่โรงพยาบาล เก็บไว้อยู่ภายใต้การเข้าถึง หรือเปิดเผยโดยไม่ได้รับอนุญาตหรือสูญหาย

6. หน้าที่และความรับผิดชอบ

โรงพยาบาลได้กำหนดผู้รับผิดชอบ และอำนาจหน้าที่พร้อมทั้งการติดต่อโรงพยาบาลไว้ เพื่อเพื่อให้ได้ มั่นใจว่าการคุ้มครองข้อมูลส่วนบุคคลจะได้รับการปฏิบัติ และมีการติดตามตรวจสอบ รวมถึงการใช้สิทธิของ เจ้าของข้อมูลเป็นไปตามที่กำหนด

6.1 คณะกรรมการบริษัท

6.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลบุคคลและความเป็นส่วนตัว

6.1.2 กำกับดูแลให้มีการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

6.2 ผู้บริหารทุกระดับ

6.2.1 จัดให้มีระเบียบปฏิบัติและมาตรการในการจัดเก็บข้อมูลส่วนบุคคลให้เหมาะสมกับ บริบทของแต่ละโรงพยาบาล โดยให้สอดคล้องกับนโยบาย แนวปฏิบัติ กฎหมาย และมาตรฐานสากล

6.2.2 จัดให้มีผู้รับผิดชอบ เช่น หน่วยงานหรือบุคลากรที่รับผิดชอบ เพื่อดูแลการดำเนินงาน ให้เป็นไปตามระเบียบปฏิบัติ

6.2.3 ในกรณีที่โรงพยาบาลว่าจ้างบุคคลธรรมดาหรือนิติบุคคลจากภายนอก เพื่อให้ ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ต้องมีระบบการคัดลอกที่มีการวางระบบการคุ้มครองข้อมูลที่ได้ มาตรฐาน

6.2.4 กำกับดูแลให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติ และระเบียบปฏิบัติ ตลอดจน หาแนวทางพัฒนาปรับปรุงเพื่อให้การนาไปปฏิบัติมีประสิทธิภาพมากขึ้น รวมทั้งมั่นใจว่ามีการรายงานผลการ ปฏิบัติงานตามนโยบายและแนวปฏิบัติและระเบียบปฏิบัติ

6.3 ผู้ควบคุมข้อมูลส่วนบุคคล /ผู้ที่ได้รับมอบหมายให้เป็นผู้เก็บรวบรวมข้อมูล

6.3.1 ดำเนินการและควบคุมการดำเนินการเกี่ยวกับการประมวลข้อมูลทั้งการแจ้ง ขอความ ยินยอม เก็บรวม รวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามระเบียบปฏิบัติการคุ้มครองข้อมูลส่วน บุคคล และกฎหมายที่กำหนด

6.3.2 ดำเนินการและควบคุมการดำเนินมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือ โดยมิชอบตามที่กำหนดไว้ในระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วน บุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

6.3.3 ดำเนินการและควบคุมการลบหรือทำลายข้อมูลเมื่อพ้นกำหนดระยะเวลาการเก็บ รักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือตามที่เจ้าของข้อมูล ส่วนบุคคลได้ร้องขอ

6.3.4 ตรวจสอบ และควบคุม ปรับปรุงข้อมูลส่วนบุคคลให้มีความถูกต้องและเป็นปัจจุบัน

6.3.5 เมื่อพบการรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคลต้องแจ้งสำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคุลเพื่อคุ้มครองข้อมูลส่วนบุคคลทราบทันที

6.3.6 ดำเนินการควบคุมการบันทึกข้อมูลและรายงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่รับผิดชอบ

6.3.7 ประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ตนรับผิดชอบ บริหารจัดการและ ดำเนินตามมาตรการที่กำหนดเพื่อลดความเสี่ยง

6.4 ผู้ประมวลผลข้อมูลส่วนบุคคล /ผู้ที่ได้รับมอบหมายให้ประมวลผลข้อมูลส่วนบุคคล

6.4.1 ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจาก ผู้ควบคุมข้อมูลส่วนบุคคล และตามระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย

6.4.2 ดำเนินการตามาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบตามที่กำหนดไว้ตามที่กฎมายกำหนด

6.4 ผู้บังคับบัญชาฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่

6.1.1 ดำเนินการเกี่ยวกับหารออกแบบ ติดตาม ตรวจสอบ และเสนอแนะระบบการป้องกันข้อมูลส่วนบุคคล

แจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วน บุคคล ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ร่วมกันดำเนินการแก้ไขการสูญหาย รั่วไหล และการละเมิดข้อมูลส่วนบุคคล

6.5 คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล

6.5.1 ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้ง พนักงานที่เกี่ยวข้องกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

6.5.2 ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วน บุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามที่กฎหมายกำหนด

6.5.3 ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วน บุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วน บุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

6.5.4 รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

6.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ดังนี้

6.6.1 ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้ง พนักงาน หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

6.6.2 ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วน บุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามที่กฎหมายดกำหนด

6.6.3 ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ ประมวลผลข้อมูลส่วนบุคคล

6.6.4 ประสานงานกับคณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล เพื่อดำเนินการ ตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การเข้าถึงข้อมูลส่วนบุคคล การโอนย้ายข้อมูลส่วนบุคคล การคัดค้านการ ประมวลผลข้อมูลส่วนบุคคล การลบข้อมูลส่วนบุคคล การระงับการใช้ข้อมูลส่วนบุคคล การ แก้ไขข้อมูล ส่วนบุคคลให้ถูกต้อง เพิกถอนความยินยอม การยื่นข้อร้องเรียนตามที่เจ้าของข้อมูลส่วนบุคคลร้อง ขอ พร้อมทั้งบันทึกรายการและจัดเก็บหลักฐานในการทำธุรกรรมดังกล่าวไว้อย่างครบถ้วน

6.6.5 รับผิดชอบในการประสานงานเรื่องการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ ที่โรงพยาบาลได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคลหรือที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความ ยินยอม ทั้งนี้ ตามที่กำหนดไว้ในนโยบายและคู่มือฉบับนี้ รวมทั้งแนวทางและคู่มือปฏิบัติงานที่เกี่ยวข้อง

6.6.6 รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่

6.6.7 ให้คำแนะนำแก่พนักงาน/หน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ในการปฏิบัติตาม นโยบาย แนวทางปฏิบัติและคู่มือฉบับนี้

7. หลักการและแนวปฏิบัติในการประมวลผลข้อมูลส่วนบุคคล

โรงพยาบาล ได้กำหนดหลักการและแนวปฏิบัติในการประมวลผลข้อมูลส่วนบุคคล เพื่อใช้เป็น แนวทางให้พนักงานปฏิบัติ เพื่อให้มั่นใจว่าการประมวลผลข้อมูลส่วนบุคคลจะเป็นไปตามที่กฎหมายกำหนด

7.1 หลักการในการประมวลผลข้อมูลส่วนบุคคล แบ่งเป็น

7.1.1 หลักการ Fairness and lawfulness เป็นการประมวลผลข้อมูลและการส่งหรือโอนข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วย กฎหมาย และ เป็นไปตามที่กำหนดโดยชัดแจ้งและเป็นธรรม

7.1.2 หลักการ Restriction to a specific purpose (Purpose Limitation) เป็นการประมวลผลข้อมูลส่วนบุคคลจะกระทำเฉพาะวัตถุประสงค์ที่ได้มีการแจ้งไว้การ เปลี่ยนวัตถุประสงค์หรือเพิ่มวัตถุประสงค์จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน ยกเว้นเป็นไปตามที่ กฎหมายกำหนด

7.1.3 หลักการ Transparency (Accountability) โรงพยาบาลมีหน้าที่ต้องแจ้งวัตถุประสงค์ ผู้ควบคุมข้อมูล การส่งหรือโอนข้อมูลให้บุคคลที่ สาม (ถ้ามี) และสิทธิแก่เจ้าของข้อมูลส่วนบุคคลก่อนหรือในเวลาที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลโรงพยาบาลจะเผยแพร่นโยบายการคุ้มครองข้อมูลส่วนบุคคล เอกสารระบบบริหารจัดการ คุ้มครองข้อมูลส่วนบุคคลและระเบียบปฏิบัติที่เกี่ยวข้องไว้ในเว็บไซต์ของโรงพยาบาลเพื่อให้เพื่อให้พนักงาน ทุกคนสามารถเข้าไปดูข้อมูลได้

7.1.4 หลักการ Necessity (Data Minimization) โรงพยาบาล จะเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็น ตามวัตถุประสงค์ที่ ข้อมูลส่วนบุคคลถูกเก็บรวบรวม

7.1.5 หลักการ Deletion (Storage Minimization) ข้อมูลส่วนบุคคลที,เกินระยะเวลาที่โรงพยาบาลกำหนดในการจัดเก็บ หรือโรงพยาบาล'ไม่มี สิทธิหรือไม่สามารถอ้างฐานในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลแล้ว โรงพยาบาลจะดำเนินการทำลายข้อมูลส่วนบุคคลนี้น

7.1.6 หลักการ Accuracy, up to date of data โรงพยาบาลจะใช้มาตรการตามสมควรในการเก็บรักษาข้อมูลส่วนบุคคลให้มีความถูกต้อง เป็นปัจจุบันและเชื่อถือได้

7.1.7 หลักการ Confidentiality and data security โรงพยาบาลจะกำหนดความมั่นคงและปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมทั้งระบบ การจัดการและเทคนิค เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลจะได้รับการคุ้มครองบีองกันตามที่กฎหมายกำหนด ทั้งการบีองกันการสูญหาย รั่วไหล การละเมิดจากผู้ที่ไม่มีอำนาจ รวมถึงการประมวลหรือส่งโอนโดยไม่ขอบด้วยกฎหมาย รวมถึงการสูญหายจากอุบัติเหตุ

7.2 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและการประมวลผลข้อมูลส่วนบุคคลการกำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล จะกำหนดแบ่งไปตามประเภทของ เจ้าของข้อมูลและต้องครอบคลุมกระบวนการประมวลตั้งแต่ต้นกระบวนการในการแจ้งสิทธิ การเก็บ รวบรวม การใช้เปิดเผย จนถึงการทำลายและการขอใช้สิทธิ โดยต้องมีองค์ประกอบอย่างน้อย ดังนี้

1) ข้อมูลที่เก็บ
2) แหล่งที่มา
3) การเก็บรวบรวม
4) การใช้
5) การเปิดเผย
6) การส่งหรือโอน
7) การป้องกัน
8) การแจ้งสิทธิ
9) การปรับปรุงข้อมูล
10) ผู้รับผิดชอบ
11) ช่องทางการติดต่อ

7.2.1 การเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล

(1)เก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็น (need to know) สำหรับ การดำเนินการ ตามวัตถุประสงค์ที่เกี่ยวข้องตามที่โรงพยาบาลกำหนด ซึ่งเป็นไปตามหลักเกณฑ์ที่กฎหมาย คุ้มครองข้อมูลส่วนบุคคลระบุไว้เช่น ก. จำเป็นเพื่อปฏิบัติตามสัญญาหรือคำขอของเจ้าของข้อมูลส่วนบุคคล ข. จำเป็นเพื่อปฏิบัติตามกฎหมาย ค. จำเป็นเพื่อประโยชน์โดยขอบด้วยกฎหมาย ง. จำเป็นเพื่อประโยชน์สาธารณะ
จ. จำเป็นเพื่อระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล
ฉ. ความยินยอมของเจ้าของข้อมูลส่วนบุคคลเท่านั้น

(2)แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลให้ เจ้าของข้อมูลส่วน บุคคลรับทราบก่อน หรือขณะเก็บรวบรวม หรือเมื่อมีการแก้ไขข้อมูลส่วนบุคคลตาม นโยบายความเป็น ส่วนตัว

(3)ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน หากจำเป็นต้องเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลอ่อนไหว

(4)ในกรณีที่โรงพยาบาลว่าจ้างบุคคลภายนอกให้ดำเนินการใดๆ ที่เกี่ยวข้องกับข้อมูลส่วน บุคคล โรงพยาบาลจะคัดเลือกบุคคลที่มีหลักเกณฑ์หรือแนวทางในการคุ้มครองข้อมูลส่วนบุคคลไม่น้อยกว่า หลักเกณฑ์ที่กำหนดไว้ในนโยบายและคู่มือฉบับนี้รวมถึงต้องจัดให้มีข้อตกลงเกี่ยวกับการคุ้มครองข้อมูลส่วน บุคคลตามที่เห็นสมควร

(5)ต้องแจ้งการส่งต่อหรือโอนข้อมูลให้กับบุคคลที่สาม หรือต่างประเทศ

(6)กรณีมีการเปลี่ยนแปลงวัตถุประสงค์ หรือมีการเพิ่มวัตถุประสงค์จะต้องแจ้งให้เจ้าของ ข้อมูลทราบ ยกเว้นที่กฎหมายกำหนด

(5)วิธีการเก็บรวบรวมและการรับข้อมูลส่วนบุคคล

ก. ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลให้ไว้กับโรงพยาบาล โดยตรง กรณีนี้ เกิดขึ้นเมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อกับโรงพยาบาลเพื่อสอบถาม กรอกแบบฟอร์มต่างๆ โดยทาง ออนไลน์ หรือ โดยทางเอกสาร เพื่อใช้บริการสอบถามข้อมูล สมัครงาน เข้าเป็นคู่สัญญากับ หรือรับการ ติดต่อ โดยตรง หรือให้ความคิดเห็น/คำติชมแก่โรงพยาบาล เป็นต้น

ข. ข้อมูลส่วนบุคคลที่โรงพยาบาลเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดย อัตโนมัติ โรงพยาบาลอาจเก็บรวบรวมข้อมูลทางเทคนิคบางอย่างเกี่ยวกับอุปกรณ์ กิจกรรมและรูปแบบการ เข้าชม/ดูงานข้อมูลประวัติการใช้งานเว็ปไซต์โดยอัตโนมัติและเทคโนโลยีอื่นๆที่คล้ายคลึงกัน

ค. ข้อมูลส่วนบุคคลที่โรงพยาบาลได้รับจากบุคคลภายนอก เช่น ตัวแทน นายหน้า ผู้ ให้บริการ นายหน้าจัดหางาน หน่วยงานของรัฐ คู่สัญญาและผู้ประกอบวิชาชีพ เป็นต้น

7.2.2 ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวบ ได้แก่

(1)ข้อมูลส่วนตัว อาทิ ชื่อนามสกุล วัน/เดือน/ปีเกิด อายุ เพศ รูปถ่าย หมายเลขและสำเนา หนังสือเดินทาง (Passport) หรือบัตรประจำตัวประชาชน ลายมือชื่อ สัญชาติ สถานภาพสมรสและข้อมูล บุคคลใน ครอบครัว

(2)ข้อมูลส่วนบุคคลที่มีความอ่อนไหว อาทิ ศาสนา ประวัติอาชญากรรม ข้อมูลสุขภาพ ผล ตรวจสุขภาพ ความ พิการและข้อมูลชีวภาพ

(3)ข้อมูลการติดต่อ อาทิที่อยู่อาศัย หมายเลขโทรศัพท์ อีเมล์ ข้อมูลการติดต่อทางโซเชียล มีเดียและ รายละเอียดบุคคลที่ติดต่อได้ในกรณีฉุกเฉิน

(4)ข้อมูลเกี่ยวกับการเงิน อาทิ หมายเลขบัญชีธนาคารและข้อมูลเกี่ยวกับภาษีอากรต่างๆ

(5)ข้อมูลเกี่ยวกับการใช้งานระบบต่างๆ ของโรงพยาบาล เช่น ข้อมูลลงทะเบียนสมัครใช้ บริการระบบของโรงพยาบาล ชื่อบัญชีใช้งาน (Account) ข้อมูลบัญชีผู้ใช้งาน รหัสประจำตัว (Username) รหัสผ่าน (Password) และ รหัสลับ (PIN) (ถ้ามี) ข้อมูลที่แสดงบนหน้าประวัติผู้ใช้งานและหน้าการสมัคร บริการต่างๆ ข้อมูลที่เจ้าของข้อมูลส่วนบุคคลได้แก้ไขปรับปรุงในข้อมูลบัญชีผู้ใช้งาน (Account) ของเจ้าของ ข้อมูลส่วนบุคคล ข้อมูลที่ได้จากบัญชีผู้ใช้งาน (Account) อื่นๆ ที่โรงพยาบาลมีเหตุอันควรเชื่อได้ว่าเจ้าของ ข้อมูลส่วนบุคคลดูแลอยู่ ข้อมูลการใช้บริการ ความสนใจและความเห็นทุกอย่างที่

เจ้าของข้อมูลส่วนบุคคลได้ แสดงผ่านระบบของโรงพยาบาล (ถ้ามี) ข้อมูลการร่วมกิจกรรมต่างๆ ของเจ้าของข้อมูลส่วนบุคคลในระบบของ โรงพยาบาล ข้อมูลการ ทำแบบสอบถาม ข้อมูลที่ได้จากการที่เจ้าของข้อมูลส่วนบุคคลติดต่อกับโรงพยาบาล หรือทีมงานของโรงพยาบาล

(6)ข้อมูลด้านเทคนิค เช่น ข้อมูลการเข้าใช้งานเว็บไซต์และระบบต่างๆ ของโรงพยาบาล ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ข้อมูลการติดต่อและสื่อสารระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ใช้งาน รายอื่น ข้อมูลจากการบันทึกการใช้งานเช่นตัวระบุอุปกรณ์ หมายเลข IP ของคอมพิวเตอร์ รหัสประจำอุปกรณ์ ประเภทอุปกรณ์ ข้อมูลเครือข่ายมือถือ ข้อมูลการเชื่อมต่อ ข้อมูลตำแหน่งที่ตั้งทางภูมิศาสตร์ ประเภทของ เบราว์เซอร์(Browser) ข้อมูลบันทึกการเข้าออกระบบ ข้อมูลแอปพลิเคชั่นหรือเว็บไซต์ที่เจ้าของข้อมูล ส่วน บุคคลเข้าถึงก่อนและหลัง (Referring Website) ข้อมูลบันทึกประวัติการใช้ระบบ ข้อมูลบันทึกการ เข้าสู่ระบบ (Login Log) ข้อมูลรายการทำธุรกรรม (Transaction Log) พฤติกรรมการใช้งาน สถิติการใช้ ระบบ เวลาที่เยี่ยมชมระบบ (Access Time) ข้อมูลที่เจ้าของข้อมูลส่วนบุคคลค้นหา การใช้ฟังก์ชั่นต่างๆ ในระบบ และข้อมูลที่โรงพยาบาล ได้เก็บรวบรวมผ่านคุกกี้ (Cookies) หรือเทคโนโลยีอื่นที่คล้ายกัน

(7)ข้อมูลเกี่ยวกับการศึกษา การฝึกอบรมและการทำงาน อาทิ ประวัติการศึกษาและการ 13กอบรม หนังสือ รับรองคุณวุฒิหรือใบแสดงผลการศึกษา ผลคะแนนหรือระดับคะแนน ระดับการศึกษา ความสามารถทาง ภาษา ข้อมูลใบอนุญาตในการประกอบวิชาชีพ เลขทะเบียน วันที่เริ่มอายุทะเบียน วันที่เห มดอายุทะเบียน วันที่ต่ออายุทะเบียน ข้อมูลการปฏิบัติหน้าที่ วันที่เริ่มงาน ข้อมูลการอบรมและข้อมูลการ ทดสอบซึ่งจัด โดยโรงพยาบาลหรือหน่วยงานอื่นที่เกี่ยวข้อง วุฒิบัตรหรือประกาศนียบัตร ประวัติการทำงาน เงินเดือนหรือ ค่าจ้าง

(8)ข้อมูลอื่นๆ เช่น บันทึกภาพและ/หรือเสียงผ่านกล้องวงจรปิด (CCTV) ภาพถ่าย บันทึกภาพและเสียง บันทึกเสียงสนทนา (ถ้ามี)

7.2.3 การเก็บรักษาและระยะเวลาใบการเก็บรักษาข้อมูลส่วนบุคคล

(1)จัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่ กฎหมายกำหนด เพื่อป้องกันการทำลาย การแก้ไขและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(2)เก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์ที่เก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ตามที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลจนกว่าเจ้าของข้อมูลส่วนบุคคลจะสิ้นสุดความสัมพันธ์ กับโรงพยาบาล ทั้งนี้โรงพยาบาล อาจจะต้องเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลต่อไป ตามระยะเวลาที่ กฎหมายกำหนด

7.3 การลบหรือทำลายข้อมูลส่วนบุคคล

โรงพยาบาลจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลของ เจ้าของข้อมูลส่วนบุคคล เมื่อ

7.3.1 พันระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล 7.3.2ไม่จำเป็นในการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์

7.3.3 เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล และโรงพยาบาลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ ต่อไป

7.3.4 เป็นการรวบรวมข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

8. สัญญาการประมวลผลข้อมูล

โรงพยาบาลได้กำหนดแนวทางปฏิบัติในการทำสัญญาจ้าง หรือรับจ้างประมวลผลข้อมูลส่วนบุคคล ดังนี้

8.1 กรณีโรงพยาบาลว่าจ้างผู้ประมวลข้อมูล

8.1.1 ก่อนทำการว่าจ้างผู้ประมวลผลข้อมูล โรงพยาบาลต้องประเมินระบบการคุ้มครอง ข้อมูลส่วนบุคคลของผู้รับจ้างก่อน หากผู้รับจ้างประมวลผลไม่มีระบบการป้องกันหรือไม่เพียงพอ การทำ สัญญาจ้างผู้ประมวลผลต้องให้ผู้ประมวลผลปฏิบัติตามระเบียบปฏิบัติที่โรงพยาบาลกำหนด

8.1.2 ในสัญญาจ้างต้องระบุวัตถุประสงค์ วิธีการเก็บข้อมูล การแจ้งเจ้าของข้อมูล การใช้ การส่ง การโอนข้อมูล และการกำจัดข้อมูล

8.1.3 คู่สัญญาต้องลงนามคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายหรือระเบียบ ปฏิบัติที่โรงพยาบาลกำหนด

8.1.4 เมื่อมีการว่าจ้างผู้ประมวลผล ต้องทำการควบคุมการประมวลผลตามที่จ้างและการ ควบคุมการปฏิบัติให้เป็นไปตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่กำหนด

8.1.5 เมื่อครบกำหนดการเก็บรักษาข้อมูล ต้องติดตามและควบคุมให้ผู้รับจ้างประมวลผลทำ การทำลายข้อมูลตามที่กำหนด

8.2 กรณีโรงพยาบาลรับจ้างประมวลผลข้อมูล

8.2.1 การรับจ้างประมวลผลข้อมูล ต้องมีการกำหนดหลักเกณฑ์ที่เกี่ยวข้องอย่างชัดเจน ต้อง ปฏิบัติให้เป็นไปตามวัตถุประสงค์อย่างเคร่งครัด ไม่เก็บ ใช้หรือเปิดเผยเกินความจำเป็นหรือนอกเหนือ วัตถุประสงค์

8.2.2 การนำเสนองานเพื่อรับจ้าง และการทำสัญญารับจ้างที่มีการประมวลผลข้อมูลจะต้อง มีการจัดทำหนังสือแจ้งความรับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคลระหว่างคู่สัญญา

8.2.3 ถ้าผู้ว่าจ้างไม่ได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ผู้รับผิดขอบต้อง ปฏิบัติตามกฎระเบียบปฏิบัติของโรงพยาบาลที่กำหนด

8.2.4 เมื่อมีการส่งข้อมูลส่วนบุคคลต้องแจ้งให้ผู้ว่าจ้างทราบด้วย

8.2.5 เมื่อครบกำหนดการเก็บรักษาข้อมูล ต้องทำการทำลายข้อมูลตามกำหนด และแจ้งให้ผู้ว่าจ้างทราบ

9. การโอนเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก หรือการส่งหรือโอนข้อมูลส่วนบุคคลไป หน่วยงาบต่างประเทศ

โรงพยาบาลอาจมีความจำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานในการ คุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามประกาศกำหนด หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วน บุคคลที่ส่งหรือโอนไปยังต่างประเทศ ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โรงพยาบาลสามารถทำใน กรณีดังต่อไปนี้

9.1 ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอ

แนวการพิจารณาความเพียงพอของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่รับโอน ข้อมูลส่วนบุคคลสามารถพิจารณาได้โดย

1) พิจารณาจากกฎหมายของประเทศดังกล่าวว่ามีความคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐาน จากกฎหมายที่เกี่ยวข้องทั้งในภาพรวมหรือกฎหมายเฉพาะรวมถึงการรักษาความมั่นคงของขาติกฎหมายอาญา การเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานรัฐการบังคับใช้กฎหมายกฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล กฎเกณฑ์ของผู้ประกอบวิชาชีพมาตรการในการรักษาความปลอดภัยของข้อมูลกฎเกณฑ์ในการโอนข้อมูลส่วน บุคคล,ไปยังต่างประเทศหรือองค์การระหว่างประเทศเพราะมีประสิทธิภาพ'ในการบังคับ'ใช้สิ,ทธิ,ของเจ้า1ของ ข้อมูลส่วนบุคคลมาตรการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลหากข้อมูลส่วนบุคคลที่โอนนั้นถูกละเมิด

2) การมีอยู่และการทำงานขององค์กรหน่วยงานอิสระในต่างประเทศหรือหน่วยงานระหว่างประเทศ ที่รับโอนข้อมูลส่วนบุคคลว่ามีอำนาจหน้าที่ในการบังคันใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วน บุคคลและอำนาจหน้าที่ในการให้ความช่วยเหลือของเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิ์ของเจ้าของข้อมูล ส่วนบุคคลและอำนาจหน้าที่ในการร่วมมือกับคพะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

3) ข้อผูกพันระดับนานาชาติของประเทศหรือองค์กรระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคลเกิด จากการที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันทางกฎหมายแต่เฉพาะที่เกี่ยวข้องกับการ คุ้มครองข้อมูลส่วนบุคคลเช่นอนุสัญญาที่มีผลบังคับผูกพันทางกฎหมายหรือการเข้าร่วมระบบพหุภาคีหรือ ภูมิภาค

9.2 กรณีได้รับการยกเว้นตามกฎหมาย

โรงพยาบาลสามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศได้แม้ว่า มาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางไม่เพียงพอหากเข้ากรณียกเว้นตามกฎหมาย ดังต่อไปนี้

1) เป็นการปฏิบัติตามกฎหมาย

2) ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดย โรงพยาบาลได้รับแจ้งให้เจ้าของข้อมูลส่วน บุคคลทราบถึงมาตรการในการคุ้มครองของข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทาง หรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ใน การดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อ ประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5) เพื่อน่องกันหรือระงับอันตรายต่อชีวิตร่างกายหรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคล อื่นเมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6) เป็นการจำเป็นเพื่อการดำเนินภารกิจ เพื่อประโยชน์สาธารณะที่สำคัญในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทาง หรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้โรงพยาบาลเสนอปัญหาต่อคณะกรรมการคุ้มครองข้อมูล ส่วนบุคคลเป็นผู้วินิจฉัย

10. สิทธิของเจ้าของข้อมูล

10.1 โรงพยาบาล มีหน้าที่ในการรับรองและคุ้มครองสิทธิของเจ้าของข้อมูล ดังต่อไปนี้

(1) สิทธิขอถอนความยินยอม

(2) สิทธิขอเข้าถึง ขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของ โรงพยาบาล หรือ ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่เจ้าของข้อมูลส่วนบุคคลบันไม่ได้ให้ ความยินยอม

(3) สิทธิขอรับหรือให้ส่งข้อมูลส่วนบุคคลไปยังผู้อื่นด้วยวิธีอัตโนมัติ

(4) สิทธิขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล

(5) สิทธิขอแก้!ข หรือเปลี่ยนแปลงข้อมูลให้ถูกต้อง สมบูรณ์ หรือเป็นปีจจุบัน

(6) สิทธิขอระงับการใช้ข้อมูลส่วนบุคคลได้

(7) สิทธิขอลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้

10.2 จัดทำบันทึกรายการข้อใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงเหตุปฏิเสธในการกรณีที่ ไม่ดำเนินการตามคำร้องขอของเจ้าของสิทธิส่วนบุคคล เพื่อเป็นหลักฐานตามที่กฎหมายกำหนด

10.3 การบริหารจัดการขอใช้สิทธิของเจ้าของข้อมูล โรงพยาบาลได้กำหนดหลักเกณฑ์การขอใช้สิทธิ ทั้งกระบวนการตั้งแต่การขอใช้ การพิสูจน์ ตัวตน การพิจารณาอนุมัติการแจ้งผลดำเนินการ เพื่อให้มั่นใจว่าเจ้าของข้อมูลจะสามารถใช้สิทธิตามเจตนา

11. มาตรการคุ้มครองข้อมูลส่วนบุคคลและแผนรับมือการละเมิดข้อมูลส่วนบุคคล

โรงพยาบาล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยพิจารณาตามความ เสี่ยง เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากการใช้ อำนาจหรือโดยมีขอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามที่โรงพยาบาลกำหนด

12. การตรวจสอบ

โรงพยาบาลได้ทำการแต่งตั้งคณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล และกำหนดระเบียบ ปฏิบัติในการตรวจสอบภายใน รวมทั้งควบคุมและตรวจสอบการดำเนินการให้เป็นไปตามระบบที่กำหนด นอกจากนี้ยังแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อทำการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ โรงพยาบาลเสมือนเป็นผู้ตรวจสอบภายนอกระบบอีกครั้ง และรายงานให้ผู้บริหารทราบตามระเบียบ ปฏิบัติการทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

13. แผนรับมือการละเมิดข้อมูลส่วนบุคคล

13.1 การเตรียมแผนรับมือเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล จัดการเหตุตั้งแต่ต้นจนจบ ครอบคลุม ข้อกำหนดทางกฎหมาย กำหนดบทบาทและหน้าที่

13.2 แผนการรับมือเมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล แบ่งเป็นขั้นตอน ได้แก่

- จำกัดความเสียหาย
- ประเมินผลกระทบ
- กำหนดผู้รับผิดชอบรวมทั้งบทบาทและหน้าที่
- จัดการเหตุตั้งแต่ต้นจนจบ ครอบคลุมข้อกำหนดทางกฎหมาย
- แจ้งผู้ที่ได้รับผลกระทบและหน่วยงานกำกับที่เกี่ยวข้อง
- ทบทวนแนวทางการรับมือและหาวิธีป้องกันไม่ให้เกิดขึ้นอีก

14. การอบรมให้ความรู้

14.1 เพื่อให้พนักงานทุกคนได้รับข้อมูลและความรู้ที่เพียงพอ โรงพยาบาลจะดำเนินการสื่อสารเพื่อให้พนักงานได้รับทราบและตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

14.2 พนักงานของโรงพยาบาล ซึ่งมีหน้าที่ต้องประมวลข้อมูลส่วนบุคคล จะต้องได้รับการอบรมและ ลร้างความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดตามระเบียบการพัฒนาอบรมพนักงาบตาม ระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลที่โรงพยาบาลกำหนด

15. การควบคุมเอกสาร

โรงพยาบาลมีหน้าที่เก็บบันทึกรายการกิจกรรมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และจัดส่งให้ เจ้าหน้าที่ผู้มีอำนาจตรวจสอบในกรณีที่มีการเรียกให้ส่งมอบบันทึกดังกล่าว

16. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

กรณีหากมีการละเมิดข้อมูลส่วนบุคคล ให้โรงพยาบาลแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ สำนักงานคพะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 (เจ็ดสิบสอง) ชั่วโมง นับแต่ทราบ เหตุเท่าที่สามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คพาะกรรมการประกาศกำหนด

17. กระบวนการร้องเรียนและขั้นตอนที่เกี่ยวข้อง

17.1 กรณีที่เจ้าของข้อมูลเชื่อว่า ข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยฝ่าผิน กฎหมายหรือระเบียบปฏิบัติการคุ้มครองข้อมูลของโรงพยาบาลที่กำหนด และมีความประสงค์ที่จะใช้สิทธิของ ตน สามารถยื่นคำร้องต่อเจ้าหน้าที่ควบคุมข้อมูลส่วนบุคคลของบริษัท หรือคณะกรรมการดำเนินงานคุ้มครอง ข้อมูลส่วนบุคคลตามที่อยู่ที่กำหนด หรือเจ้าพนักงานคุ้มครองข้อมูล สำนักงานคุ้มครองข้อมูลส่วนบุคคล โดยตรงได้

17.2 พนักงานของโรงพยาบาลซึ่งเชื่อว่าข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผยอย่าง ไม่เหมาะสม สามารถขอใช้สิทธิ์ได้ที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท

17.3 บุคคลผู้รับคำร้องจะพิจารณาเพื่อที่จะส่งคำร้องต่อไปยังเจ้าพนักงานควบคุมข้อมูลส่วนบุคคล เพื่อการพิจารณาตามที่เห็นว่าเหมาะสมก็ได้

17.4 คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะต้องตอบสนองต่อคำร้องโดยไม่ชักช้า และไม่เกิน 30 วัน นับทั้งแต่วันที่ได้รับคำร้อง และต้องรายงานการ ดำเนินงานต่อประธานเจ้าหน้าที่ฝ่ายบริหาร

17.5 ในกรณีที่ผู้ร้องไม่เห็นด้วยกับการพิจารณาของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ร้องสามารถ อุทธรณ์การพิจารณาต่อเจ้าพนักงานคุ้มครองต่อไปได้

18. ความรับผิด

โรงพยาบาล หรือ พนักงานที่ทำการละเมิดกฎหมายมีหน้าที่รับผิดชอบต่อการฝ่าเป็นบทบัญญัติที่ พระราชบัญญัติคุ้มครองข้อมูลส่วน พ.ศ. 2562 กำหนดไว้และถือเป็นการกระทำที่ผิดวินัยของโรงพยาบาล อย่างร้ายแรง

19. การปรับปรุงระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

19.1 ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล หรือพนักงานที่ปีหน้าที่เกี่ยวข้องในระบบบริหารจัดการ คุ้มครองข้อมูลส่วนบุคคล สามารถเสนอการปรับปรุงแก้ไขคู่มือ ข้อกำหนด ระเบียบปฏิบัติ แบบฟอร์ม หรือ ประกาศอื่นใดที่ตนพิจารณาว่าจะทำให้ระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพที่สูงขึ้น หรือเหมาะสมกับการดาเนินงานของโรงพยาบาล โดยสามารถเสนอต่อคณะกรรมการดำเนินงานคุ้มครองข้อมูล ส่วนบุคคล

19.2 ให้คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคลมีอำนาจนำเสนอการแก้ไขปรับปรุงระบบ บริหารจัดการคุ้มครองข้อมูลส่วนบุคคลโดยให้คำนึงถึงความถูกต้อง เหมาะสม เพียงพอ และเพิ่มประสิทธิภาพ ของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประธานเจ้าหน้าที่บริหารพิจารณาอนุมัติให้ดำเนิน แก้ไข และแจ้งประกาศให้ผู้เกี่ยวข้องทราบและปฏิบัติตามที่ปรับปรุง

20. กฎหมาย ข้อกำหนดที่เกี่ยวข้องกับคู่มือฉบับนี้

โรงพยาบาล ได้กำหนดระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ เพื่อเป็นแนวปฏิบัติของ พนักงานทุกคนในการกำหนดมาตรฐานขึ้นพื้นฐานสำหรับการเก็บรวบรวม ใช้หรือเปิดเผย ซึ่งอยู่ในบังคับของ พระราชบัญญัติคุ้มครอง' ข้อมูลส่วนบุคคล พ.ศ.2562 ตลอดจนกฎหมาย คำสั่ง ประกาศ แนวปฏิบัติ และ ระเบียบอื่นที่เกี่ยวข้อง

20.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายที่เกี่ยวข้อง

20.2 นโยบายรักษาความปลอดภัยข้อมูล (Information security policy)

21. การทบทวนนโยบาย

คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้อง จะทบทวนนโยบายฉบับ นี้อย่างน้อยปีละหนึ่งครั้ง หรือ เมื่อกฎหมายมีการแก้ไขหรือเปลี่ยนแปลงหรือ จำเป็นต้องเปลี่ยนแปลง หลักเกณฑ์ที่เป็นสาระสำคัญที่กำหนดไว้ในนโยบาย แนวทางปฏิบัติและคู่มือระบบบริหารจัดการ คุ้มครอง ข้อมูลส่วนบุคคลฉบับนี้

22. ช่องทางการติดต่อ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ/หรือผู้ควบคุมข้อมูลส่วนบุคคล

ไปรษณีย์: บริษัท รพ.ศุภมิตร จำกัด (มหาชน) จำกัด
เลขที่ 76 ถนนเณรแก้ว ตำบลท่าพี่เลี้ยง อ.เมือง จังหวัดสุพรรณบุรี 72000
อีเมล: DPO@supamitrhospital.com
โทรศัพท์: 035-523777 ต่อ 2441
เว็บไซต์: https://www.supamitrhospital.com/

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 1 มิถุนายน 2565
บริษัท โรงพยาบาลศุภมิตร จำกัด (มหาชน)

(ทันตแพทย์อนุศักดิ์ คงมาลัย)
กรรมการผู้จัดการและประธานกรรมการบริหาร

คู่มือการออกแบบการคุ้มครองป้องกันข้อมูลส่วนบุคคล

โรงพยาบาลได้กำหนดคู่มือการออกแบบการคุ้มครองป้องกันข้อมูลส่วนบุคคลเพื่อใช้เป็นแนวทางของ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในการกำหนดการคุ้มครองป้องกับข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบ อย่างเหมาะสมสอดคล้องกับการพิจารณาความเสี่ยง (Risk Based Approach) ตั้งแต่การป้องกันข้อมูล อาทิ การเก็บรักษาข้อมูลการจัดส่งและการใช้หรือเปิดเผย เป็นต้น จนกงการป้องกันอุปกรณ์ต่างๆ การตรวจสอบและทดสอบระบบเพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลของโรงพยาบาล ที่งการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบเป็นไปอย่างมีประสิทธิภาพเพียงพอและเหมาะสมในการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

1.1 เพื่อให้มั่นใจว่าผู้ควบคุมข้อมูลและผู้ประมวลผลจากกำหนดการคุ้มครองป้องกันข้อมูลส่วนบุคคล ได้ตามข้อกำหนดที่กำหนด

1.2 เพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลมีความเพียงพอและเหมาะสม

1.3 เพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลได้มีการควบคุมการปฏิบัติงานได้อยาก เหมาะสมและเป็นไปตามวัตถุประสงค์ของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

2. การออกแบบคุ้มครองป้องกันข้อมูลส่วนบุคคล

โรงพยาบาลได้กำหนดแนวทางในการออกแบบคุ้มครองป้องกันข้อมูลส่วนบุคคลขั้นต่ำที่จะทำให้ ผู้ควบคุมและผู้ประมวลผลนำไปปรับใช้ในการคุ้มครองป้องกันข้อมูลให้ครอบคลุมทั้งข้อมูลและอุปกรณ์ ตลอดจนการตรวจสอบและทดสอบระบบเพื่อให้มั่นใจถึงความเพียงพอและเหมาะสมในการคุ้มครองป้องกัน ข้อมูลส่วนบุคคลโดยต้องคำนึงถึงความเสี่ยงในแต่ละข้อมูลส่วนบุคคลด้วยซึ่งผู้ควบคุมข้อมูลและผู้ประมวลผล สามารถกำหนดมาตรการใดใดที่เหมาะสมและเพียงพอในการคุ้มครองป้องกันข้อมูลที่ตนรับผิดชอบดังนี้

2.1 การป้องกับข้อมูลการออกแบบการป้องกันข้อมูลกำหนดไว้เป็น 2 รูปแบบตามลักษณะของข้อมูล คือ ข้อมูลที่เป็นเอกสาร (Physical Document) และ ข้อมูลที่เป็นข้อมูลในระบบอิเล็กทรอนิกส์ (Electronics Data) ดังนี้

2.1.1 การป้องกันข้อมูลที่เป็นเอกสารการป้องกันข้อมูลที่เป็นเอกสารประกอบด้วย

2.1.1.1 การป้องกันเอกสารข้อมูลส่วนบุคคล

1) ผู้ควบคุมหรือผู้ประมวลผลจะต้องเป็นผู้จัดการเอกสารข้อมูลส่วนบุคคลเท่านั้น

2) ผู้ควบคุมหรือผู้ประมวลผลจะต้องมีการป้องกันข้อมูลในการแก้ไขพิมพ์หรือคัดลอกข้อมูล ยกเว้นข้อมูลที่ต้องพิมพ์ออกมาเพื่อไช้ประกอบการดำเนินการที่เป็นไปตามข้อกำหนดหรือกฎหมายและต้อง ทำลายเอกสารข้อมูลที่สำเนาออกไปทันทีเมื่อหมดความจำเป็นในการไช้งาน

2.1.1.2 การป้องกันที่เก็บรักษา (Storage)

1) การเก็บรักษาเอกสารข้อมูลส่วนบุคคลจะต้องเก็บไว้เป็นสัดส่วนและต้องเป็น อุปกรณ์ที่มีการปิดล็อกการเข้าถึงได้

2) ผู้ควบคุมจะเป็นผู้เก็บรักษากุญแจ

2.1.1.3 การส่งต่อข้อมูล

1) การส่งต่อเอกสารข้อมูลส่วนบุคคลต้องส่งโดยตรงให้กับเฉพาะผู้มีอำนาจเข้าถึงข้อมูลได้เท่านั้น

2) การส่งต่อเอกสารข้อมูลส่วนบุคคลต้องมีการพิมพ์ข้อความสับหรือ confidential

2.1.2 การป้องกันข้อมูลที่เป็นข้อมูลในระบบอิเล็กทรอนิกส์การป้องกันข้อมูลที่เป็นข้อมูลระบบอิเล็กทรอนิกส์ประกอบด้วย

2.1.2.1 การป้องกันไฟล์ข้อมูล

1) ไฟล์ข้อมูลส่วนบุคคลต้องกำหนดรหัสการเข้าถึงไฟล์ข้อมูล โดยรหัสข้อมูลการ เข้าถึงจะมีรูปแบบการเข้าถึงข้อมูลตามที่แผนกเทคโนโลยีสารสนเทศกำหนดไว้

2) ไฟล์ข้อมูลจะต้องมีการป้องกันข้อมูลในการแก้ไขพิมพ์หรือคัดลอกข้อมูลยกเว้น ข้อมูลที่พิมพ์ออกมาเพื่อใช้ประกอบการดำเนินการที่เป็นไปตามข้อกำหนดหรือกฎหมาย

3) รหัสผ่าน (password) ต้องเก็บเป็นความสับ

4) ข้อมูลประเภทรหัสผ่าน (password) ต้องทำการ Hash ข้อมูลรหัสผ่าน(password) ก่อนการจัดเก็บลงในฐานข้อมูลทุกครั้ง

5) ไฟล์ข้อมูลส่วนบุคคลสามารถเปิดใช้งานได้แค่ในส่วนที่โรงพยาบาลกำหนดไว้ เท่านั้นห้ามนำไฟล์ข้อมูลส่วนบุคคลออกไปใช้งานนอกเหนือจากงานที่โรงพยาบาลกำหนดไว้

2.1.2.2 การป้องกันที่เก็บรักษาและ การ Back up ข้อมูล (Storage & Backup)

1) การเก็บรักษาไฟล์ข้อมูลส่วนบุคคลจะต้องเก็บไว้ และกำหนดสิทธิในการเข้าถึง ข้อมูลนั้น (Access Control) เฉพาะผู้ที่ได้รับสิทธิเข้าถึงเท่านั้น

2) กรณีที่เป็นข้อมูลของลูกค้าหรือการรับจ้างประมวลผลจะต้องเก็บโฟลเดอร์หรือ ฐานข้อมูลไว้แยกต่างหากของแต่ละลูกค้าหรือการรับจ้างประมวลผล

3) ข้อมูลส่วนบุคคลข้อมูลของลูกค้าหรือข้อมูลที่รับจ้างประมวลผลจะต้องจัดเก็บไว้ ใบไดรพิกลางของโรงพยาบาลที่กำหนดไว้เท่านั้นและจะเก็บไว้ใน Server ของโรงพยาบาล โดยแยกข้อมูลของ แต่ละลูกค้าไว้

4) โรงพยาบาลจะทำการ Back up ข้อมูลทุกวัน

5) โรงพยาบาลมีการกำหนด Firewall ในการป้องกันการเข้าถึงระบบ Server ของ โรงพยาบาลโดยจะมีแต่ผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าใช้งานได้

2.1.2.3 การส่งต่อข้อมูล

1) การส่งต่อไฟล์ข้อมูลส่วนบุคคลต้องผ่านอีเมล์ของบริษัทเท่านั้น

2) การส่งไฟล์ข้อมูลส่วนบุคคลต้องไม่ส่งไปพร้อมกับรหัสการเปิดไฟล์ข้อมูลในอีเมล์ ฉบับเดียวกัน โดยอาจพิจารณาการส่งรหัสเข้าไฟล์ข้อมูลไปอีเมล์อีกฉบับหรือช่องทางอื่นๆตามความเหมาะสม

3) ให้พิจารณาการลดขั้นตอนการส่งไฟล์ข้อมูลผ่านอีเมล์ให้น้อยที่สุดโดยอาจใช้ การเข้าถึงไฟล์ที่จัดเก็บไว้ที่ไดร์กลางแทน

2.1.2.4 การแปลข้อมูลก่อนการส่งต่อนำไปใช้

1) ควรพิจารณาการแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymous Data) หรือ ข้อมูลนิรนาม (Anonymous Data) ก่อนการจัดส่งข้อมูลให้ผู้ใช้หรือเปิดเผยข้อมูลเพื่อให้ไม่สามารถพิสูจน์ตัว บุคคลของเจ้าของข้อมูลได้

2.2 การควบคุมอุปกรณ์อิเล็คทรอนิกส์

2.2.1 ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบบริหารจัดการทรัพย์สินอุปกรณ์ อิเล็กทรอนิกส์ของบริษัท และจะทำการจัดเก็บและระบุผู้ควบคุมและใช้รวมถึงเปลี่ยนแปลงอุปกรณ์ อิเล็กทรอนิกส์

2.2.2 จะต้องมีการกำหนดรหัสการใช้งานอุปกรณ์อิเล็คทรอนิกส์

2.2.3 รหัสการใช้งานอุปกรณ์อิเล็คทรอนิกส์จะมีรูปแบบรหัสผ่านตามที่ฝ่ายเทคโนโลยี สารสนเทศเป็นผู้กำหนด

2.2.4 ผู้ควบคุมข้อมูลและผู้ประเมินผลจะต้องเปลี่ยนรหัสการใช้งานอุปกรณ์อิเล็กทรอนิกส์ ตามที่โรงพยาบาลกำหนด

2.2.5 ผู้ควบคุมข้อมูลและผู้ประมวลผลจะต้องเตรียมอุปกรณ์อิเล็กทรอนิกส์ที่ใหม่ใช้งานได้ ระยะเวลาตามที่โรงพยาบาลกำหนด

2.2.6 ผู้ควบคุมข้อมูลและผู้ประมวลผลห้ามติด หรือเขียนรหัสการใช้อุปกรณ์ติดไว้ที่อุปกรณ์อิเล็กทรอนิกส์

2.2.7 ฝ่ายเทคโนโลยีสารสนเทศจะจำกัดอุปกรณ์อิเล็กทรอนิกส์ ที่ไม่ได้รับอนุญาตในการ เข้าถึงข้อมูลส่วนบุคคล

2.2.8 ฝ่ายเทคโนโลยีสารสนเทศมีอำนาจในการเข้าถึงอุปกรณ์อิเล็กทรอนิกส์เพื่อจัดการ การใช้งานที่ผิดประเภทได้

2.3 ความปลอดภัยของอุปกรณ์มือถือ

2.3.1 ฝ่ายเทคโนโลยีสารสนเทศจะป้องกันการเข้าถึงโฟลเดอร์และไฟล์ข้อมูลในไดร์กลาง ของโรงพยาบาลผ่านอุปกรณ์มือถือทั้งหมด ยกเว้นมีเหตุจำเป็นที่จะต้องมีการขออนุมัติตามข้อปฏิบัติที่ โรงพยาบาลกำหนด

2.4 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลจะแบ่งออกตามลักษณะของข้อมูลดังนี้

2.4.1 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลที่เป็นเอกสาร

1) ผู้ควบคุมข้อมูลจะต้องทำการตรวจสอบที่จัดเก็บเอกสารข้อมูลส่วนบุคคลว่ามีการ ปิดล็อกตามปกติ หรือมีการเข้าถึงเอกสารหรือไม่

2) หากพบการละเมิดต้องทำการแจ้งให้คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคลทราบทันที

2.4.2 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลที่เป็นไฟล์อิเล็กทรอนิกส์

1) ฝ่ายเทคโนโลยีสารสนเทศจะทำการตรวจสอบ log ในการเข้าถึงว่ามีผู้ไม่มีอำนาจ พยายามเข้าถึงโฟลเดอร์หรือไฟล์ข้อมูลส่วนบุคคลนั้นหรือไม่

2) ฝ่ายเทคโนโลยีสารสนเทศจัดทำการตรวจสอบ log ว่ามีผู้ไม่มีอำนาจเข้าถึง โฟลเดอร์หรือไฟล์ข้อมูลส่วนบุคคลหรือไม่

2.5 การควบคุมการทำลายหรือลบข้อมูลส่วนบุคคล

2.5.1 การทำลายหรือลบข้อมูลส่วนบุคคล เป็นส่วนหนึ่งของการป้องกันข้อมูลด้านการเก็บ รักษา (Storage) โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลที่ ตบเองรับผิดขอบตามความจำเป็นของการใช้งานหรือตามที่มีกฎหมายอื่นใดกำหนด และเมื่อพ้นระยะเวลา จัดเก็บแล้ว หรือโรงพยาบาลไม่มีสิทธิ์หรือไม่สามารถอ้างฐานในการประมวลผลข้อมูลส่วนบุคคลแล้ว ผู้ควบคุม ข้อมูลส่วนบุคคลจะต้องดำเนินการทำลายข้อมูลส่วนบุคคลนั้นภายใน 30 วันทำการ

2.6 การทดสอบการคุ้มครองป้องกับข้อมูลส่วนบุคคล

1) ฝ่ายเทคโนโลยีสารสนเทศจะทำการทดสอบการเข้าถึงโฟลเดอร์ที่จัดเก็บข้อมูลส่วนบุคคล

2) หากพบว่าสามารถเข้าถึงโฟลเดอร์นั้นได้ฝ่ายเทคโนโลยีสารสนเทศจะต้องแจ้งให้ คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบทันทีพร้อม ทำการแก้ไข

3) ให้ฝ่ายเทคโนโลยีสารสนเทศทำการเสนอและระบบที่เหมาะสมเพียงพอในการคุ้มครอง ข้อมูลส่วนบุคคลให้คณะกรรมการดำเนินงานคุ้มครองข้อมูลส่วนบุคคลทราบ

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 1 มิถุนายน 2565
บริษัท โรงพยาบาลศุภมิตร จำกัด (มหาชน)

(ทันตแพทย์อนุศักดิ์ คงมาลัย)
กรรมการผู้จัดการและประธานกรรมการบริหาร