ประกาศความเป็นส่วนตัวของแผนกทรัพยากรบุคคลและธุรการ

โรงพยาบาลเอกชัย (“ **โรงพยาบาล** ”) มุ่งมั่นที่จะคุ้มครองข้อมูลส่วนบุคคลของท่านในฐานะที่ท่านเป็นผู้ เข้ารับบริการตรวจรักษาโรค และบริการทางการแพทย์ รวมถึงบริการต่าง ๆ จากโรงพยาบาล ข้อมูลส่วนบุคคลของท่านจะได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุ คคล พ.ศ. 2562 โรงพยาบาลในฐ านะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายในการแจ้งเอกสารฉบับนี้ให้ท่านทราบถึงเหตุผลและวิธีการที่โรงพยาบาลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน รวมถึงแจ้งให้ท่านทราบสิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล

1. คำจำกัดความ

ในนโยบายฉบับนี้ คำหรือข้อความสามารถนิยามได้ดังนี้

คำจำกัดความ	ความหมาย
1. ข้อมูลส่วนบุคคล (Personal data)	หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถกระตุ้นตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม
2. ข้อมูลอ่อนไหว (Sensitive Data)	หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา ข้อมูลจำลองลายนิ้วมือ) หรือข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
3. เจ้าของข้อมูล	หมายถึง บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
4. ประมวลผล	หมายถึง การเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลชองท่านผู้เป็นเจ้าของข้อมูลส่วนบุคคล
5. เว็บไซต์	หมายถึง เว็บไซต์ ซึ่งโรงพยาบาลเป็นเจ้าของหรือให้บริการแล้วแต่กรณี
6. ผู้ควบคุมข้อมูลส่วนบุคคล	หมายถึง บุคคลหรือนิติบุคคลที่มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

7. ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

2. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้ จัดทำขึ้นเพื่อให้การดำเนินการเป็นไปตามกรอบของ พรบ.คุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับองค์กรในด้านการรวบรวมข้อมูล การจำกัดการนำข้อมูลส่วนบุคคลไปใช้ การรักษาความมั่นคงปลอดภัยของข้อมูลหรือการเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามที่กำหนด

3. ขอบเขต (Scope)

ระเบียบงานนี้ใช้สำหรับเจ้าหน้าที่ หน่วยงาน ที่อยู่ในขอบเขตของการควบคุมข้อมูลส่วนบุคคล ทั้งในส่วนงานฝ่ายทรัพยากรบุคคล งานจัดซื้อ งานด้านการตลาด งานด้านบริการ งานด้านสารสนเทศ ตลอดจนผู้ที่มีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

4. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ (Responsible person and responsibility)

4.1 พนักงานทุกคน มีหน้าที่ ให้ข้อมูลที่มีความถูกต้องทันสมัย ให้กับฝ่ายทรัพยากรบุคคลเพื่อไปนำไปใช้ จัดเก็บ เปิดเผย ต่อหน่วยงานหรือการทำงานที่เป็นไปตามสัญญา (สัญญาว่าจ้าง)

4.2 ผู้ควบคุมข้อมูลส่วนบุคคล Data Controller มีหน้าที่

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลโดยไม่มีอำนาจโดยมิชอบ

2. ป้องกันมิให้บุคคล นิติบุคคลซึ่งได้รับข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยข้อมูลนั้นโดยไม่มีอำนาจหรือมิชอบ

3. จัดให้มีการตรวจสอบการลบ หรือทำลายข้อมูล

4. แจ้งเหตุการณ์ละเมิดข้อมูลแก่สำนักงาน ภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ในกรณีการละเมินมีความเสี่ยงสูงอาจกระทบสิทธิ เสรีภาพบุคคล

5. ทำบันทึกรายการข้อมูลส่วนบุคคลเป็นหนังสือ /สื่ออิเล็กทรอนิกส์ เพื่อให้เจ้าของข้อมูล/ สำนักงานตรวจสอบ

4.3 ผู้ประมวลผลข้อมูลส่วนบุคคล Data Processor มีหน้าที่

1. เก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล

2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยไม่มีอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้คุมทราบถึงเหตุการณ์ละเมิดที่เกิดขึ้น

3. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

4.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล Data Protection Officer: DPO มีหน้าที่

1. ให้คำแนะนำแก่ผู้ควบคุมหรือผู้มวล ลูกจ้างหรือผู้รับจ้างในการปฏิบัติตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล

2. ตรวจสอบการดำเนินงานของผู้ควบคุม หรือผู้ประมวลผล ลูกจ้างหรือผู้รับจ้างเกี่ยวกับการรวบรวม ใช้ เปิดเผยข้อมูล

3. ประสานงานและให้ความร่วมมือกับ สำนักงานคณะคุ้มครอง

4. รักษาความลับของข้อมูลส่วนบุคคลที่รู้และได้มาจากการทำหน้าที่

4.5 หน่วยงานที่มีการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลในองค์กร คือ ฝ่ายบุคคล ฝ่ายการตลาด ฝ่ายบัญชีการเงิน ฝ่ายจัดซื้อ ฝ่าย IT สารสนเทศ มีหน้าที่ต้องปฏิบัติตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล และคู่มือฉบับนี้

5. มาตรการความมั่นคงปลอดภัยในการเก็บรักษาข้อมูลส่วนบุคคล

โรงพยาบาลตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของท่าน โรงพยาบาลจึงกำหนดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึงทำลาย ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย เพื่อให้เป็นไปตามที่กำหนดในนโยบายและ /หรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาล โรงพยาบาลจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งครอบคลุมถึงมาตรการป้องกันด้านการ บริหารจัดการ มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล อันประกอบไปด้วยการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย

1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
2) การกำหนดเกี่ยวกับการอนุญาตหรือกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
3) การบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

6. การเปลี่ยนแปลงนโยบายความเป็นส่วนตัว

นโยบายความเป็นส่วนตัวนี้จัดทำขึ้นเพื่อแจ้งรายละเอียดและวิธีการคุ้มครองข้อมูลส่วนบุคคลของท่าน โดยโรงพยาบาลอาจดำเนินการปรับปรุงหรือแก้ไขนโยบายความเป็นส่วนตัวนี้ไม่ว่าบางส่วนหรือทั้งหมดเป็นครั้งคราว เพื่อให้สอดคล้องกับแนวทางและหลักเกณฑ์ของกฎหมายที่มีการเปลี่ยนแปลงไป ดังนั้น ท่านจึงควรติดตามนโยบายความเป็นส่วนตัวที่กำหนดไว้นี้อยู่เสมอ

7. ช่องทางการติดต่อ

หากท่านประสงค์จะติดต่อ หรือมีข้อสงสัย หรือต้องการสอบถามข้อมูลเกี่ยวกับรายละเอียดการประมวลผลข้อมูลส่วนบุคคล รวมถึงสิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคลตามนโยบายฉบับนี้ หรือกรณีที่พบว่ามีการใช้ข้อมูลส่วนบุคคลของท่านไปในทางที่ไม่ชอบ ท่านสามารถติดต่อโรงพยาบาลผ่านทางช่องทางดังต่อไปนี้

โรงพยาบาลเอกชัย ที่อยู่ : 99/9 หมู่ที่ 4 ถ. เอกชัย ตำบล โคกขาม อำเภอเมืองสมุทรสาคร จ. สมุทรสาคร 74000

อีเมล : info@ekachaihospital.com

โทร. 034-417-999

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) : ที่อยู่: 99/9 หมู่ที่ 4 ถ. เอกชัย ตำบล โคกขาม อำเภอเมืองสมุทรสาคร จ. สมุทรสาคร 74000

อีเมล : dpo@ekachaihospital.com

โทร. 034-417-999 ต่อ 9662