

นโยบายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment Policy)

1. หลักการและเหตุผล

โรงพยาบาลเมตตาประชารักษ์ (วัดไร่ขิง) ได้ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และกำหนดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ก่อนเริ่มดำเนินโครงการหรือกิจกรรมที่อาจก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เพื่อให้การประมวลผลข้อมูลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานการกำกับดูแลของหน่วยงาน

2. วัตถุประสงค์

1. ประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล
2. กำหนดมาตรการควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
3. สนับสนุนการออกแบบระบบตามหลัก Privacy by Design และ Privacy by Default
4. สร้างความเชื่อมั่นให้แก่เจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสีย

3. ขอบเขต

นโยบายนี้ใช้กับ

- โครงการใหม่ที่มีการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- การเปลี่ยนแปลงระบบงานหรือเทคโนโลยีที่มีผลต่อข้อมูลส่วนบุคคล
- การใช้ข้อมูลอ่อนไหว
- การใช้เทคโนโลยีใหม่ที่อาจส่งผลกระทบต่อสิทธิของเจ้าของข้อมูล
- การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก

4. กรณีที่ต้องจัดทำ DPIA

ให้ดำเนินการจัดทำ DPIA อย่างน้อยในกรณีดังต่อไปนี้

- มีการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก
- มีการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว
- มีการติดตามหรือเฝ้าสังเกตพฤติกรรมของบุคคลอย่างเป็นระบบ
- มีการใช้ระบบอัตโนมัติในการตัดสินใจที่มีผลกระทบต่อเจ้าของข้อมูล
- มีการใช้เทคโนโลยีหรือวิธีการใหม่ที่อาจเพิ่มความเสี่ยง

5. บทบาทและความรับผิดชอบ

ผู้บริหาร

- อนุมัติผลการประเมิน
- จัดสรรทรัพยากรในการลดความเสี่ยง

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- ให้คำปรึกษาเกี่ยวกับการจัดทำ DPIA
- ตรวจสอบความครบถ้วนของการประเมิน
- เสนอแนะมาตรการลดความเสี่ยง
- ติดตามการดำเนินการตามแผน

เจ้าของโครงการ

- จัดทำ DPIA
- จัดเตรียมข้อมูลประกอบการประเมิน
- ดำเนินมาตรการลดความเสี่ยง

6. ขั้นตอนการดำเนินงาน

1. ระบุโครงการหรือกิจกรรมที่ต้องประเมิน
2. วิเคราะห์ข้อมูลส่วนบุคคลที่เกี่ยวข้อง
3. ประเมินความจำเป็นและความได้สัดส่วน
4. วิเคราะห์ความเสี่ยง
5. กำหนดมาตรการลดความเสี่ยง
6. ขอความเห็นจาก DPO
7. เสนอผู้บริหารอนุมัติ
8. ทบทวน DPIA เมื่อมีการเปลี่ยนแปลงสำคัญหรือน้อยกว่า 12 เดือน

7. การจัดเก็บเอกสาร

รายงาน DPIA และเอกสารประกอบต้องจัดเก็บอย่างปลอดภัย และสามารถตรวจสอบย้อนหลังได้ตามระยะเวลาที่หน่วยงานกำหนด

8. การทบทวน

ให้ทบทวนนโยบายอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย เทคโนโลยี หรือ กระบวนการดำเนินงานที่มีนัยสำคัญ



(นายกิตติวัฒน์ มะโนจันทร์)

ผู้อำนวยการ

โรงพยาบาลเมตตาประชารักษ์ (วัดไร่ขิง)