



9.3.2 มีนโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

Cybersecurity Management Policy

PDPA Policy



บันทึกข้อความ

ส่วนราชการ...โรงพยาบาลปรางค์กู่ กลุ่มงานสุขภาพดิจิทัล โทร.๐ ๔๕๖๙ ๗๑๖๗ ต่อ.๑๕๘.....

ที่ ศก ๐๐๓๓.๓๑๔/ ๑๐๐๕ วันที่ ๑ เมษายน ๒๕๖๙.....

เรื่อง ขอแจ้งเวียนแผนการรับมือภัยคุกคามทางไซเบอร์ นโยบาย ระเบียบปฏิบัติต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

เรียน หัวหน้ากลุ่มงาน/หัวหน้างาน และผู้ที่เกี่ยวข้อง

ด้วยโรงพยาบาลปรางค์กู่ ได้มีคำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานประจำโรงพยาบาลปรางค์กู่ ให้เป็นไปตามกฎหมาย มาตรฐาน และแนวทางปฏิบัติที่เกี่ยวข้อง อันได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ทั้งนี้เพื่อยกระดับด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศให้สามารถ ป้องกัน รับมือ ลดความเสี่ยงภัยคุกคามทางด้านไซเบอร์

ในการนี้โรงพยาบาลปรางค์กู่ จึงขอแจ้งเวียนแผนการรับมือภัยคุกคามทางไซเบอร์ นโยบาย ระเบียบปฏิบัติต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งโรงพยาบาลปรางค์กู่ได้ปรับปรุงขึ้น รายละเอียดตามเอกสารที่แนบมาพร้อมหนังสือนี้

จึงเรียนมาเพื่อโปรดทราบและแจ้งให้ผู้มีส่วนเกี่ยวข้องทราบโดยทั่วกันถือปฏิบัติ

(นายอัครเดช บุญเย็น)

นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลปรางค์กู่





เอกสารแนบ

กลุ่มงาน/งาน	รับทราบ	กลุ่มงาน/งาน	รับทราบ
๑. กลุ่มงานการแพทย์		๘. กลุ่มงานทันตสาธารณสุข	
๒. กลุ่มงานการพยาบาล		๙. กลุ่มงานบริการด้านปฐมภูมิ	
๓. กลุ่มงานบริหารทั่วไป		๑๐. กลุ่มงานโภชนศาสตร์	
๔. กลุ่มงานเภสัชกรรมฯ		๑๑. กลุ่มงานประกันสุขภาพฯ	
๕. กลุ่มงานเทคนิคการแพทย์		๑๒. กลุ่มงานจิตเวชและยาเสพติด	
๖. กลุ่มงานรังสีการแพทย์		๑๓. กลุ่มงานแพทย์แผนไทย	
๗. กลุ่มงานเวชกรรมฟื้นฟู		๑๔. กลุ่มงานสุขภาพดิจิทัล	

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายกาญจนศักดิ์ โสตา	นายสันต์ สิงห์ไกร	นายแพทย์อัครเดช บุญเย็น
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	เจ้าพนักงานเวชสถิติชำนาญงาน (Lead Implementer)	ผู้อำนวยการโรงพยาบาลปรางค์กู (CISO)
วันเดือนปี	16 มีนาคม 2569	20 มีนาคม 2569	23 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	23 มีนาคม 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรางค์กู ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)

1. วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดหลักเกณฑ์ แนวทาง และมาตรการในการเก็บรวบรวม ใช้เปิดเผย และคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลปราγκู ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) รวมถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และสร้างความเชื่อมั่นในการดำเนินงานของโรงพยาบาลปราγκู

2. ขอบเขตการบังคับใช้

นโยบายนี้ครอบคลุมข้อมูลส่วนบุคคลทุกประเภทที่โรงพยาบาลปราγκู เก็บรวบรวม ใช้ หรือเปิดเผย ซึ่งรวมถึงข้อมูลของ

- ผู้ป่วยและญาติ
- บุคลากร พนักงาน ลูกจ้าง
- ผู้รับจ้าง ผู้ให้บริการภายนอก
- ผู้มาติดต่อหรือผู้มีส่วนได้ส่วนเสียอื่นใด

รวมถึงการประมวลผลข้อมูลผ่านระบบสารสนเทศ เอกสาร และสื่อทุกรูปแบบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปราγκู ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปราγκู เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

3. คำจำกัดความ

- **ข้อมูลส่วนบุคคล (Personal Data)** : ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะทางตรงหรือทางอ้อม
- **ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)** : ข้อมูลตามที่กฎหมายกำหนด เช่น ข้อมูลสุขภาพ ประวัติการรักษา
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** : โรงพยาบาลปรางค์กู
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** : บุคคลหรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่งของโรงพยาบาลปรางค์กู
- **เจ้าของข้อมูลส่วนบุคคล (Data Subject)**: บุคคลเจ้าของข้อมูลส่วนบุคคล

4. บทบาทและความรับผิดชอบ

4.1 โรงพยาบาลปรางค์กู ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่กำหนดนโยบาย มาตรการ และกำกับดูแลให้การประมวลผลข้อมูลเป็นไปตามกฎหมาย

4.2 ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตามคำสั่งของโรงพยาบาลปรางค์กู และมีมาตรการคุ้มครองข้อมูลที่เหมาะสม

4.3 โรงพยาบาลปรางค์กู จะแต่งตั้ง **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)** ตามหลักเกณฑ์ของกฎหมาย

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้เป็นสมบัติของ โรงพยาบาลปรางค์กู ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

5. ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

โรงพยาบาลปรางค์กู จะประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานกฎหมายที่เหมาะสม เช่น

- เพื่อการรักษาพยาบาลและการสาธารณสุข
- เพื่อปฏิบัติตามกฎหมาย
- เพื่อประโยชน์โดยชอบด้วยกฎหมายของโรงพยาบาลปรางค์กู
- โดยได้รับความยินยอมจากเจ้าของข้อมูล (กรณีที่ถูกกฎหมายกำหนด)

6. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิตามกฎหมาย ดังนี้

- สิทธิขอเข้าถึงและขอรับสำเนาข้อมูล
- สิทธิขอแก้ไขข้อมูลให้ถูกต้อง
- สิทธิขอลบหรือทำลายข้อมูล
- สิทธิขอจำกัดหรือคัดค้านการประมวลผล
- สิทธิถอนความยินยอม

โรงพยาบาลปรางค์กู จะดำเนินการตามคำร้องขอภายในระยะเวลาที่กฎหมายกำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรางค์กู ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

7. การเก็บรักษาและระยะเวลาในการเก็บข้อมูล

โรงพยาบาลปราγκุ จะเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์และข้อกำหนดของกฎหมาย เมื่อพ้นระยะเวลาที่จำเป็น จะดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

8. การเปิดเผยและการโอนข้อมูลส่วนบุคคล

การเปิดเผยหรือโอนข้อมูลส่วนบุคคลให้บุคคลที่สาม จะกระทำเท่าที่จำเป็นและเป็นไปตามกฎหมาย โดยต้องมีมาตรการคุ้มครองข้อมูลที่เหมาะสม และกรณีการโอนข้อมูลไปต่างประเทศต้องเป็นไปตามหลักเกณฑ์ PDPA

9. มาตรการคุ้มครองข้อมูลส่วนบุคคล

โรงพยาบาลปราγκุ กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในด้าน

- มาตรการทางเทคนิค เช่น การควบคุมการเข้าถึง การเข้ารหัสข้อมูล
- มาตรการทางการบริหารจัดการ เช่น นโยบาย การกำหนดสิทธิ์ การอบรมบุคลากร
- มาตรการทางกายภาพ เช่น การควบคุมพื้นที่จัดเก็บข้อมูล

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้เป็นสมบัติของ โรงพยาบาลปราγκุ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปราγκุ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)	รหัสเอกสาร	PKH MOPH Audit Plan -07
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

10. การจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach)

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล โรงพยาบาลปรางค์กู๋ จะดำเนินการตรวจสอบ ประเมินผลกระทบ และแจ้งหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลตามระยะเวลาที่กฎหมายกำหนด

11. ช่องทางการติดต่อ

เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลได้ที่

- ชื่อเจ้าหน้าที่ DPO : นายสันต์ สิงห์ไกร [เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)]
- อีเมล: suntpkh@gmail.com
- โทรศัพท์: 0 4569 7167 ต่อ 158

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรางค์กู๋ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู๋ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ