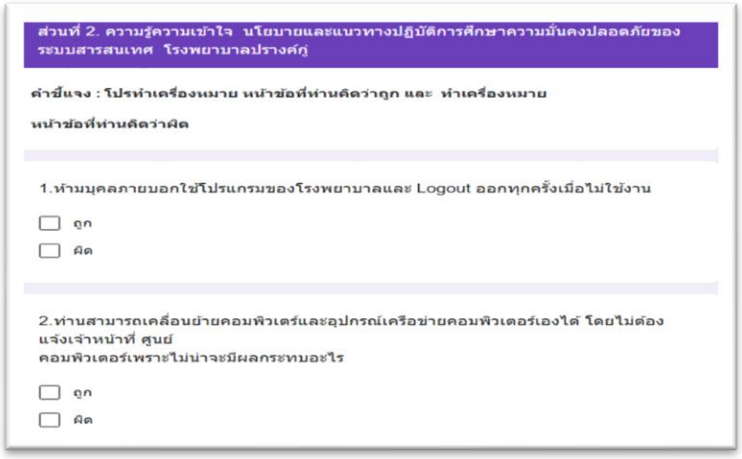
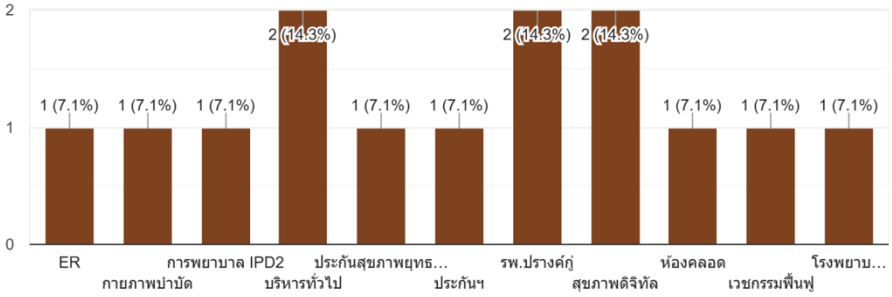
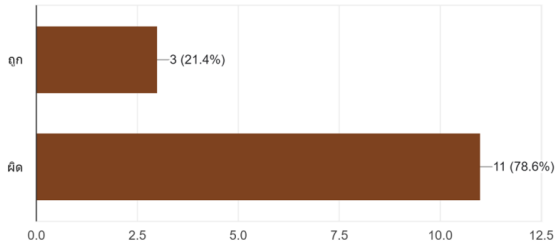
9.3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติ อย่างต่อเนื่อง





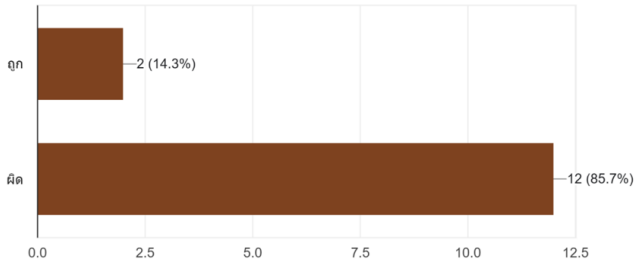
7. สามกรถส่งมูลผู้ป่วยผ่าน social media เช่น Line, Message เพื่อปรึกษา(Consult) ไม่ต้องให้ผู้ป่วยเซ็นยินยอม

ค่าตอบ 14 ข้อ



8.ท่านสามารถเชื่อมต่ออุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อื่น...อร์ได้เองโดยไม่ต้อง ติดต่อเจ้าหน้าที่ศูนย์คอมพิวเตอร์

ค่าตอบ 14 ข้อ



จากแบบประเมินความเข้าใจในนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่ายังมีความเข้าใจผิดบ้างในกรณีการเชื่อมต่ออุปกรณ์คอมพิวเตอร์อื่นโดยไม่แจ้งเจ้าหน้าที่จึงได้ออกนโยบายมาเพื่อสร้างความเข้าใจและปฏิบัติได้ถูกต้อง

	นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)	**รหัสเอกสาร**	PKH MOPH Policy-05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

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

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	23 มีนาคม 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 2.4.1, ข้อ 22.4.2]

1. วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรการและแนวปฏิบัติสำหรับการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ เช่น USB, External Hard Drive, SD Card และอุปกรณ์จัดเก็บข้อมูลอื่น ๆ เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและการรั่วไหลของข้อมูลสำคัญขององค์กร

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงพนักงานทุกระดับ ผู้รับเหมา และบุคคลภายนอกที่ต้องการใช้งานหรือเชื่อมต่ออุปกรณ์บันทึกข้อมูลแบบถอดได้กับระบบสารสนเทศขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management):** กำกับดูแลให้มีการปฏิบัติตามนโยบายและสนับสนุนมาตรการด้านความมั่นคงปลอดภัย
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team):** บังคับใช้และตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้ พร้อมดำเนินมาตรการรักษาความมั่นคงปลอดภัย
- **พนักงานและผู้ใช้งาน (Employees & Users):** ปฏิบัติตามแนวทางของนโยบายนี้ และรายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการใช้งานสื่อบันทึกข้อมูลแบบถอดได้

4. แนวปฏิบัติในการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Guidelines)

4.1 การอนุญาตและข้อจำกัด

- อุปกรณ์บันทึกข้อมูลแบบถอดได้ต้องได้รับการอนุมัติจากฝ่าย IT ก่อนใช้งาน
- ห้ามใช้อุปกรณ์ส่วนตัวในการถ่ายโอนหรือจัดเก็บข้อมูลขององค์กร เว้นแต่ได้รับอนุญาตเป็นกรณีพิเศษ
- ต้องมีการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลสำคัญที่จัดเก็บในอุปกรณ์บันทึกข้อมูลแบบถอดได้

4.2 การควบคุมการเข้าถึงและการใช้งาน

- จำกัดสิทธิ์การเข้าถึงสื่อบันทึกข้อมูลแบบถอดได้เฉพาะผู้ที่มีความจำเป็นต้องใช้งานเท่านั้น
- ระบบที่รองรับการใช้งานอุปกรณ์แบบถอดได้ต้องมีการเปิดใช้ **Read-Only Mode** เป็นค่าเริ่มต้น และอนุญาตให้เขียนข้อมูลได้เฉพาะอุปกรณ์ที่ได้รับอนุญาต
- ห้ามใช้อุปกรณ์บันทึกข้อมูลแบบถอดได้ที่ไม่มีการตรวจสอบหรือมีแหล่งที่มาไม่แน่ชัด

4.3 มาตรการรักษาความมั่นคงปลอดภัย

- ต้องใช้ซอฟต์แวร์ป้องกันมัลแวร์เพื่อตรวจสอบอุปกรณ์ทุกครั้งก่อนใช้งาน
- อุปกรณ์ที่ไม่ได้ใช้งานเป็นเวลานานต้องถูกลบข้อมูลทั้งหมดก่อนนำมาใช้อีกครั้ง
- ต้องมีระบบบันทึกการใช้งานสื่อบันทึกข้อมูลแบบถอดได้เพื่อให้สามารถตรวจสอบย้อนหลังได้

4.4 การนำออกและการทำลายข้อมูล

- เมื่อเลิกใช้งานอุปกรณ์ ต้องมีการลบข้อมูลอย่างปลอดภัย (Secure Erasure) ตามมาตรฐานขององค์กร
- อุปกรณ์ที่ชำรุดหรือหมดอายุการใช้งานต้องถูกทำลายอย่างปลอดภัย โดยใช้เทคนิคการลบข้อมูลที่ไม่สามารถกู้คืนได้ เช่น **Data Wiping หรือ Physical Destruction**

5. การตรวจสอบและบังคับใช้ (Monitoring and Enforcement)

5.1 การตรวจสอบและติดตาม

- ทีม IT Security ต้องมีระบบเฝ้าระวังและตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้
- ต้องมีการตรวจสอบบันทึกการใช้งานเป็นระยะ และดำเนินมาตรการตอบสนองหากพบพฤติกรรมที่ผิดปกติ

5.2 การตอบสนองต่อเหตุการณ์ (Incident Response)

- หากพบการใช้งานที่ไม่ได้รับอนุญาต ระบบต้องแจ้งเตือนฝ่าย IT Security ทันที
- ทีม IT มีอำนาจในการยกเลิกสิทธิ์การใช้งานของผู้ใช้ที่ละเมิดนโยบาย

5.3 การบังคับใช้ข้อกำหนด

- ผู้ใช้ที่ฝ่าฝืนนโยบายนี้อาจถูกระงับสิทธิ์การใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้ และอาจได้รับโทษทางวินัยตามระเบียบขององค์กร
- องค์กรมีสิทธิ์ปรับปรุงนโยบายและกระบวนการนี้ให้สอดคล้องกับภัยคุกคามและกฎหมายที่เปลี่ยนแปลง

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

	กระบวนการเชื่อมต่อระยะไกล **(Remote Connection Procedure)**	**รหัสเอกสาร**	**PKH MOPH Protect -03**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้ **ชั้นความลับ** **ของเอกสาร**	**23 มี.ค. 2569** **ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

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

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**23 มีนาคม 2569**	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

	กระบวนการเชื่อมต่อระยะไกล **(Remote Connection Procedure)**	**รหัสเอกสาร**	PKH MOPH Protect -03
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ **ชั้นความลับ** **ของเอกสาร**	**23 มี.ค. 2569** **ใช้ภายในเท่านั้น**

สารบัญ

กระบวนการเชื่อมต่อระยะไกล (Remote Connection Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.3.1, ข้อ 22.3.2]

1. วัตถุประสงค์

กระบวนการนี้จัดทำขึ้นเพื่อควบคุมและรักษาความมั่นคงปลอดภัยของการเชื่อมต่อระยะไกลมายัง บริการที่สำคัญของหน่วยงาน โดยให้แน่ใจว่ามีมาตรการที่เพียงพอในการป้องกันและตรวจจับการเข้าถึงที่ไม่ได้รับอนุญาต

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อ ระยะไกลมายังบริการที่สำคัญ รวมถึงการกำหนดแนวทางปฏิบัติสำหรับการเชื่อมต่อและการควบคุมการไหล ของข้อมูล

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	ผู้ใช้งานระบบ	เจ้าหน้าที่ของหน่วยงานต่าง ๆ โรงพยาบาลปรางค์กู่ที่เป็นผู้ใช้งานระบบ
2	IT/IST/Security Team	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ทำหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
3	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นปลอดภัยสารสนเทศขององค์กร

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	รับผิดชอบในการอนุมัติและตรวจสอบมาตรการความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกล
2	IT/IST/Security Team	รับผิดชอบในการกำหนดและบังคับใช้ นโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล
3	ผู้ใช้งานระบบ	มีหน้าที่ในการปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการใช้งานระบบตามมาตรฐานที่กำหนด

5. ขั้นตอนปฏิบัติ

5.1 การรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล (Remote Connection Security)

1) มาตรการรักษาความมั่นคงปลอดภัย

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลมายังบริการที่สำคัญมีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ เช่น มีการเข้ารหัสข้อมูล การพิสูจน์ยืนยันตัวตนที่แข็งแกร่ง และการ ควบคุมการไหลของข้อมูล โดยมีการใช้ VPN ที่เข้ารหัสการเชื่อมต่อและการยืนยันตัวตนด้วยสองปัจจัย (2FA) สำหรับการเข้าถึงระบบจากระยะไกล

2) การเปิดใช้งานการเชื่อมต่อ

ขั้นตอน: เปิดใช้งานการเชื่อมต่อระยะไกลเมื่อมีความจำเป็นเท่านั้น และปิดการเชื่อมต่อเมื่อไม่ใช้งาน โดยการตั้งค่าให้เซิร์ฟเวอร์เปิดใช้งานการเชื่อมต่อระยะไกลเฉพาะในช่วงเวลาทำงานเท่านั้น

3) การใช้เทคนิคการพิสูจน์ตัวตนที่แข็งแกร่ง

ขั้นตอน: ใช้เทคนิคการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยในการส่งข้อมูลที่มีความอ่อนไหว เช่น การใช้โปรโตคอลที่ปลอดภัย SSH สำหรับการเชื่อมต่อระยะไกล เพื่อป้องกันการโจมตีแบบ Man-in-the-Middle

4) การเข้ารหัสการเชื่อมต่อ

ขั้นตอน: ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมดเพื่อป้องกันการดักฟังข้อมูลระหว่างทาง เช่น การใช้ HTTPS สำหรับการเข้าถึงเว็บไซต์ภายในองค์กรจากระยะไกล

5) ข้อจำกัดในการใช้คำสั่งระบบ (System Commands)

ขั้นตอน: ไม่อนุญาตให้เชื่อมต่อระยะไกลเพื่อใช้งานคำสั่งระบบที่จะส่งผลกระทบต่อการดำเนินงานของบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน โดยการจำกัดสิทธิ์ในการใช้คำสั่งที่เกี่ยวข้องกับการจัดการเซิร์ฟเวอร์ผ่านการเชื่อมต่อระยะไกล เว้นแต่จะได้รับการอนุมัติจากผู้บริหาร

6) การจำกัดการไหลของข้อมูล

ขั้นตอน: จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ เพื่อป้องกัน การรั่วไหลของข้อมูลที่ไม่จำเป็น โดยการกำหนดให้สามารถถ่ายโอนข้อมูลเฉพาะไฟล์ที่จำเป็น สำหรับการทำงานเท่านั้นในระหว่างการเชื่อมต่อระยะไกล

7) การขอเชื่อมต่อระยะไกลจากผู้บริการภายนอก

ขั้นตอน: ทางผู้บริการภายนอกจำเป็นต้องร้องขอการเชื่อมต่อระยะไกล โดยการส่งข้อความอย่สงเป็นทางการ เช่น EMAIL หรือแบบฟอร์มที่กำหนด มายังหน่วยงาน IT ที่รับผิดชอบ พร้อมทั้งระบุวันเวลาที่ต้องการเชื่อมต่อระยะไกล จากนั้นทางหน่วยงาน IT ที่รับผิดชอบต้องทำการตรวจสอบกิจกรรมที่ทำ จนกระทั่งเสร็จสิ้นการทำงาน

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร
1	NDA	NDA – Non Disclosure Agreement

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) - การเชื่อมต่อระยะไกล (Remote Connection)
2	นโยบาย แนวปฏิบัติในการเชื่อมต่อระยะไกล
3	หลักฐานการขออนุญาตเชื่อมต่อระยะไกล
4	รายงานการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ

	กระบวนการเชื่อมต่อระยะไกล **(Remote Connection Procedure)**	**รหัสเอกสาร**	**PKH MOPH Protect -03**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้ **ชั้นความลับ** **ของเอกสาร**	**23 มี.ค. 2569** **ใช้ภายในเท่านั้น**

โรงพยาบาลปรางค์กู่ จังหวัดศรีสะเกษ		หน้า: 1
ระเบียบปฏิบัติเลขที่ SP-IM-385-00		ฉบับที่: 2
เรื่อง: แนวทางการใช้งานสื่อสังคมออนไลน์	วันที่: 20 มีนาคม 2569	
แผนก: งานเวชระเบียนและเทคโนโลยีสารสนเทศฯ	แผนกที่เกี่ยวข้อง เจ้าหน้าที่ทุกคน	
ผู้จัดทำ: นายกาญจนศักดิ์ โสดา	ผู้อนุมัติ นายแพทย์อัครเดช บุญเย็น	

1 วัตถุประสงค์

๑.เพื่อให้เจ้าหน้าที่สามารถปฏิบัติตามแนวปฏิบัติ การใช้งานสื่อสังคมออนไลน์เป็นแนวทางเดียวกันและปฏิบัติได้ถูกต้อง

๒.เพื่อป้องกันการเปิดเผยข้อมูลอันเป็นความลับของผู้ป่วยในสื่อสังคมออนไลน์

๓.เพื่อป้องกันข้อร้องเรียนหรือการฟ้องร้องในการเปิดเผยความลับของผู้ป่วย

2 .ขอบข่าย

เจ้าหน้าที่โรงพยาบาลปรางค์กู่ต้องปฏิบัติและสอดคล้องตามแนวนโยบายภายใต้กฎหมาย ได้แก่ พรบ. ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) กฎหมายว่าด้วยสถานพยาบาล กฎหมายว่าด้วยสุขภาพแห่งชาติ กฎหมายวิชาชีพ ระเบียบต่างๆ เป็นต้น

3.คำนิยามศัพท์

๑.สื่อสังคมออนไลน์ (Social media) หมายถึง สื่อหรือช่องทางการติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูลระหว่างบุคคลโดยใช้เทคโนโลยีสารสนเทศ ที่เน้นการสร้างและเผยแพร่เนื้อหาระหว่างผู้ใช้งานด้วยกันหรือสนับสนุนการสื่อสารสองทาง หรือการนำเสนอและเผยแพร่เนื้อหาในวงกว้างได้ด้วยตนเองซึ่งนิยมเรียกว่า Social Media หรือ Social network ซึ่งรวมถึงสื่อดังต่อไปนี้

(๑) กระดานข่าว (Web board หรือ Online forums)

(๒) เครือข่ายสังคมออนไลน์ (Social networking services) เช่น Facebook Google Plus, Myspace, Linkedln, LINE, WhatsApp, Viber, Skype

(๓) สื่อสำหรับเผยแพร่และแลกเปลี่ยนที่เป็นภาพนิ่ง เสียง วิดิทัศน์ หรือ แฟ้มข้อมูล หรือให้บริการเนื้อที่เก็บข้อมูลบนอินเทอร์เน็ต เช่น Flicker, Podcast, YouTube, Instargram, Dropbox, Google Drive,

(๔) บล็อก (Blogs) เช่น WordPress, Blogger และไมโครบล็อก เช่น Twitter

(๕) เว็ปไซต์สำหรับสร้างและแก้ไขเนื้อหาร่วมกัน เช่น Wikipedia

(๖) เกมออนไลน์หรือโลกเสมือนที่มีผู้ใช้งานหลายคน

(๗) สื่ออิเล็กทรอนิกส์หรือสื่อออนไลน์อื่นในลักษณะเดียวกันหรือคล้ายคลึงกันที่เปิดให้ใช้งานเพื่อเป็นช่องทางสื่อสารระหว่างบุคคล ระหว่างกลุ่มบุคคล หรือกับสาธารณะ

๒. องค์กร/หน่วยงาน หมายถึง กลุ่มงาน แผนก งาน ในโรงพยาบาลปรางค์กู่

๓. บุคคล บุคลากร ผู้ใช้งาน เจ้าหน้าที่ หมายถึง บุคลกรในโรงพยาบาลปรางค์กู่ ได้แก่ ข้าราชการ ลูกจ้างประจำ พนักงานกระทรวงสาธารณสุข ลูกจ้างเงินบำรุง พนักงานราชการ และลูกจ้างอื่นของโรงพยาบาล

๔.โพสต์ (Post) หมายถึง การส่งข้อความตัวอักษร ภาพ หรือวิดิทัศน์ เข้าสู่สื่อออนไลน์

๕.ผู้ป่วย หมายถึง ผู้ป่วยตามกฎหมายว่าด้วยสถานพยาบาลและหมายความรวมถึงผู้ที่รับบริการด้านสุขภาพจากสถานพยาบาลหรือจากผู้ประกอบวิชาชีพด้านสุขภาพด้วย

4.เอกสารอ้างอิง

ประกาศของคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ.๒๕๕๙ ประกาศในราชกิจจานุเบกษา เล่ม ๑๓๔ ตอนพิเศษ ๘๘ ง ๒๔ มีนาคม ๒๕๖๐

ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ.๒๕๖๑ ประกาศในราชกิจจานุเบกษา เล่ม ๑๓๕ ตอนพิเศษ ๑๒๔ ง ๓๑ พฤษภาคม ๒๕๖๑

พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ (PDPA)

5.นโยบาย

เพื่อให้การใช้งานสื่อสังคมออนไลน์ของเจ้าหน้าที่โรงพยาบาลปรางค์กู่เป็นไปด้วยความเรียบร้อย เหมาะสมและมีจริยธรรมอันจะเป็นการธำรงรักษาเกียรติภูมิและความเชื่อมั่นศรัทธาที่ประชาชนมีต่อวิชาชีพและการทำงานของเจ้าหน้าที่

6. ความรับผิดชอบ

หากพบเห็นการใช้งานสื่อสังคมออนไลน์ที่ไม่เหมาะสมอย่างร้ายแรงให้แจ้งบุคคลนั้นหยุดการกระทำและแก้ไขหรือรายงานให้ผู้อำนวยการโรงพยาบาลปรางค์กู่พิจารณาดำเนินการตามอำนาจหน้าที่ ทั้งนี้ตามความรุนแรงของการกระทำ ความเหมาะสมของสถานการณ์และวิสัยและพฤติการณ์ที่เกี่ยวข้อง

หากมีการฟ้องร้องหรือร้องเรียนผู้เปิดเผยข้อมูลจะต้องรับผิดชอบหรือร่วมรับผิดชอบตามที่กฎหมายกำหนด

7. วิธีปฏิบัติ

๑. องค์กรอนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์เว็ปไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และจรรยาบรรณวิชาชีพ

๒. ระมัดระวังการแสดงความคิดเห็นบนสื่อสังคมออนไลน์ที่เป็นข้อถกเถียงหรือสุ่มเสี่ยงเกี่ยวกับสถาบันชาติ ศาสนา พระมหากษัตริย์

๓. คิดก่อนแชร์ ให้ตรวจสอบความถูกต้อง เหมาะสม น่าเชื่อถือ ไม่ผิดกฎหมายก่อนแชร์ข้อมูล

๔. คิดก่อนโพสต์ เจ้าหน้าที่ต้องรับผิดชอบต่อการกระทำทั้งในด้านกฎหมาย วินัย จริยธรรม และสังคม ต้องระมัดระวังการแสดงความคิดเห็นในลักษณะบ่น ระบายอารมณ์หรือนินทาบนสื่อออนไลน์

๕. ต้องเคารพศักดิ์ศรีความเป็นมนุษย์หลีกเลี่ยงการกระทำหรือเผยแพร่เนื้อหาที่ทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เหยียดหยาม ถูกเกลียดชัง ถูกคุกคามหรือถูกกลั่นแกล้ง เป็นต้น

๖. หลีกเลี่ยงการใช้ถ้อยคำ การถ่ายภาพ ที่ไม่สุภาพ ไม่เหมาะสม ลามกอนาจาร หรือรุนแรง

๗. ต้องเคารพในจริยธรรมแห่งวิชาชีพ ตลอดจนข้อบังคับ ระเบียบและประกาศที่เกี่ยวข้อง

๘. ไม่เปิดเผยข้อมูลส่วนบุคคลที่เป็นความลับของผู้ป่วยหรือบุคคลอื่นเว้นแต่ได้รับความยินยอมโดยต้องแจ้งวัตถุประสงค์ รูปแบบ ช่องทาง ผลดีผลเสียให้ทราบและเข้าใจ หรือเป็นไปตามกฎหมายบัญญัติ

๙.การแลกเปลี่ยนเรียนรู้ระหว่างผู้ปฏิบัติงานด้านสุขภาพด้วยกัน การแลกเปลี่ยนความเห็นทางวิชาการโดยไม่ได้รับความยินยอมจากผู้ป่วย ให้ลบข้อมูลที่ระบุตัวตนของผู้ป่วยทั้งหมด หรือข้อมูลที่อาจระบุตัวผู้ป่วยได้ เช่น หอผู้ป่วย หมายเลขเตียง เป็นต้น และให้ลบหรือยกเลิกการส่งข้อความภายใน ๑ วัน เมื่อได้รับหรือส่งคำปรึกษาทางวิชาการแล้ว

๑๐.ห้ามโฆษณาหรือยินยอมให้ผู้อื่นโฆษณาผลิตภัณฑ์สุขภาพในลักษณะที่เป็นความผิดตามกฎหมาย

๑๑.ให้ข้อมูลบนสังคมออนไลน์ได้ตามอำนาจหน้าที่ของตนเท่านั้น

๑๒.การให้คำปรึกษาด้านสุขภาพออนไลน์ให้พิจารณาถึงผลดีผลเสีย เลือกใช้ตามความจำเป็นและเหมาะสมอย่างระมัดระวัง หลีกเลี่ยงการให้คำปรึกษาในลักษณะที่แสดงถึงความมั่นใจ ชัดเจน แน่นอน โดยไม่คำนึงถึงโอกาสการเกิดปัญหาอาจนำไปสู่การฟ้องร้องได้

๑๓.การใช้สื่อสังคมออนไลน์เพื่อติดต่อสื่อสารกับผู้ป่วยให้บันทึกรายละเอียดของการให้คำปรึกษาไว้ในเวชระเบียนผู้ป่วยเพื่อความต่อเนื่องในการให้บริการผู้ป่วย

๑๔.ห้ามเผยแพร่ภาพถ่ายในหอผู้ป่วย ห้องคลอด ห้องผ่าตัดขณะมีการดูแลหรือทำหัตถการกับผู้ป่วยหรือขณะให้การดูแลรักษาผู้บาดเจ็บหรือเสียชีวิต

๑๕.ใช้รหัสผ่านที่คาดเดาได้ยากในการเข้าใช้งานเครือข่ายคอมพิวเตอร์โรงพยาบาล

๑๖.ไม่คลิกลิงก์หรือเปิดไฟล์ที่ไม่แน่ใจว่ามีความปลอดภัยต่อระบบคอมพิวเตอร์

๑๗.พบปัญหาในการใช้งานให้แจ้งเจ้าหน้าที่งานเวชระเบียนและสารสนเทศทางการแพทย์

๑๘.หากพบเห็นการใช้งานสื่อสังคมออนไลน์ที่ไม่เหมาะสมอย่างร้ายแรงให้แจ้งบุคคลนั้นหยุดการกระทำและแก้ไขหรือรายงานให้ผู้อำนวยการโรงพยาบาลปรางค์กู่พิจารณาดำเนินการตามอำนาจหน้าที่ต่อไป ทั้งนี้ตามความรุนแรงของการกระทำ ความเหมาะสมของสถานการณ์วิสัยและพฤติการณ์ที่เกี่ยวข้อง

ผู้จัดทำ .....

(นายกาญจนศักดิ์ โสดา)

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ผู้ทบทวน.....

(นายสันต์ สิงห์ไกร)

เจ้าพนักงานเวชสถิติชำนาญงาน

ผู้อนุมัติ

(นายอัครเดช บุญเย็น)

นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลปรางค์กู่