



ประเมินการรับรู้และการละเมิดแนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

VIRUS

โรงพยาบาลเมืองจันทร์

งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์



โรงพยาบาลเมืองจันทร์

ประกาศนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคีรัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเมืองจันทร์ ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลเมืองจันทร์ จึงกำหนดนโยบาย ดังนี้

๑. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร
๒. มีหน้าที่ควบคุม ดูแล ระวังเบี่ยงเบนสิทธิ หรือบดบังโทษตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติในกรณีสำคัญ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ รายงานการฝ่าฝืนให้ต้นสังกัด หรือโรงพยาบาลเพื่อพิจารณาลงโทษ
๓. สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
๔. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้ และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๓

(นายแพทย์จิระวัตร วิเศษสังข์)

ผู้อำนวยการโรงพยาบาลเมืองจันทร์



โรงพยาบาลเมืองจันทร์

ประกาศระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเมืองจันทร์ ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลเมืองจันทร์ จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHIMPRO ทุกๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHIMPRO ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของู้ใช้งาน(User Account) และรหัสผ่าน(Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
๔	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นเตอร์, อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
๕	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัพเดทซอฟต์แวร์อื่นใดในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
๖	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
๗	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
๘	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
๙	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้อินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
๑๐	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๓

(นายแพทย์จรัสวัตร วิเศษสังข์)

ผู้อำนวยการโรงพยาบาลเมืองจันทร์

**ประเมินการรับรู้และการละเมิดแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ**

กิจกรรมที่ 1

ร่างนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
1	ผ่านมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ	✓
2	ผ่านมติที่ประชุมคณะกรรมการระบบเวชระเบียน (MRS)	✓
3	ผ่านมติที่ประชุมคณะกรรมการบริหารโรงพยาบาล (กกบ)	✓

กิจกรรมที่ 2

ประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
1	ประกาศใช้ วันที่ 1 ตุลาคม 2563	✓
2	เวียนหนังสือแจ้งประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ทุกหน่วยงานพร้อมกับเซ็นต์รับทราบทุกคน ส่งรายชื่อกลับงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เพื่อติดตามประเมินผลต่อไป	✓

กิจกรรมที่ 3

ประเมินการรับรู้นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
1	ประเมินการรับรู้ ผู้ใช้งานทุกคน จำนวน 116 คน ทั้งหมด 13 หน่วยงาน	100%
2	วิธีการประเมินการรับรู้ โดยแบบสอบถาม	100%
3	หัวหน้ากลุ่มงานควบคุม กำกับ ติดตามผล	✓
4	งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ สรุปผลการประเมิน และหาแนวทางพัฒนาต่อไป	✓

กิจกรรมที่ 4

ประเมินการละเมิดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
1	ประเมินการรับรู้ ผู้ใช้งานทุกคน จำนวน 116 คน ทั้งหมด 13 หน่วยงาน	100%
2	วิธีการประเมินการรับรู้ โดยแบบสอบถาม	100%
3	หัวหน้ากลุ่มงานควบคุม กำกับ ติดตามผล	✓
4	งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ สรุปผลการประเมินและหาแนวทางพัฒนาต่อไป	✓

กิจกรรมที่ 5 สรุปผลการประเมินการรับรู้ และการละเมิดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

ลำดับ	แนวปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ/แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HIMPRO ทุกๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	116	100	0	0	3	2.58	113	97.41	• ผู้ใช้งานต้องติดต่อขอเปิดใช้งานใหม่
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม HIMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	116	100	0	0	3	2.58	113	97.41	• งานประกันสุขภาพฯ ประเมินทุกราย เมื่อพบให้แจ้งดำเนินการแก้ไขทันที
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (User Account) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม	116	100	0	0	1	0.86	115	99.13	• เตือน แนะนำผู้ละเมิด และประเมินผลซ้ำ • เพิ่มบัญชีผู้ใช้งานให้แก่บุคคลที่ยังไม่มี
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	116	100	0	0	1	0.86	115	99.13	• เตือน แนะนำผู้ละเมิด และประเมินผลซ้ำ
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	116	100	0	0	2	1.72	114	98.27	• ติดตั้งโปรแกรม Winlock ผู้ใช้งานจะไม่สามารถติดตั้งซอฟต์แวร์อื่นได้ยกเว้นผู้ดูแลระบบเท่านั้น
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	116	100	0	0	9	7.75	107	92.27	• เตือน แนะนำ ผู้ละเมิด และประเมินผลซ้ำ

ลำดับ	แนวปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ/แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom)กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	116	100	0	0	3	2.58	113	97.41	• เตือน แนะนำ ผู้ละเมิด และประเมินผลซ้ำ
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	116	100	0	0	2	1.72	114	98.27	• เตือน แนะนำ ผู้ละเมิด และประเมินผลซ้ำ
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	116	100	0	0	1	0.86	115	99.13	• เตือน แนะนำ ผู้ละเมิด ให้ดำเนินการลบข้อมูล และประเมินผลซ้ำ
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	116	100	0	0	0	0	116	100	• กำหนดสิทธิ์การเข้าถึงข้อมูล
หมายเหตุ : ผู้ใช้งานทั้งหมด จำนวน 116 คน										



ภาคผนวก



สื่อประชาสัมพันธ์

* แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ *

โรงพยาบาลเมืองจันทร์

3 Do

- ควรทำการเปลี่ยนรหัสผ่านทุกๆ 90 วัน
- รหัสผ่านมีความยาวอย่างน้อย 6 ตัวอักษร (มีตัวอักษรผสมตัวเลข)
- เก็บรักษารหัสผ่านให้เป็นความลับ ห้ามให้ผู้อื่นใช้

5 Don't

- ห้าม กระทำการเลื่อนย้าย ดิสก์พ่นเมฆ หรือทำการใดๆ ต่อคอมพิวเตอร์และอุปกรณ์
- ห้าม ผู้ใดนำอุปกรณ์ราคาสัญญาต่างๆ มาเชื่อมต่อระบบเครือข่าย
- ห้าม ดาวน์โหลด ดิสก์ อีเมลขยะฟิชเวิร์ก ซอฟต์แวร์
- ห้าม แชนแนลข้อมูลผู้เกี่ยวข้องสาธารณะผ่านสื่อออนไลน์หรือโซเชียลมีเดียต่างๆ
- ห้าม เช้าข้อมูลผู้เกี่ยวข้องในฐานความรับผิดชอบ

แนวปฏิบัติ ไซเบอร์ให้แก่มหาวิทยาลัยขอนแก่น

- 1 **ไม่เปิดเผยข้อมูล ส่วนบุคคลของผู้ป่วย**
เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เติง ฯลฯ
- 2 **ชี้แจง ให้ผู้ป่วยเข้าใจ**
ตระหนักในความเสี่ยง ของการแชร์ข้อมูลในไลน์กลุ่ม ฯลฯ
- 3 **หากจำเป็น**
ต้องระบุข้อมูลส่วนบุคคล ให้ใช้โดยส่วนตัว
- 4 **ระบุตัวตนได้**
ใช้ชื่อ และรูปโปรไฟล์ของตนเอง

สื่อ/ความรู้

เรื่องควรรู้ พ.ร.บ. ...

เรื่องควรรู้ พ.ร.บ. คอม ๕0

health station. แนวทางปฏิบัติใน...

10 ข้อควรระวัง PDPA

- 01 ข้อมูลส่วนบุคคล
- 02 สิทธิของผู้เสียหาย
- 03 การขอข้อมูล
- 04 สิทธิในการลบข้อมูล
- 05 การแจ้งเหตุ
- 06 การแจ้งเหตุ
- 07 การแจ้งเหตุ
- 08 การแจ้งเหตุ
- 09 การแจ้งเหตุ
- 10 การแจ้งเหตุ

4 เรื่องไม่จริง เกี่ยวกับ PDPA

1. PDPA ไม่เกี่ยวกับข้อมูลสุขภาพ
2. PDPA ไม่เกี่ยวกับข้อมูลสุขภาพ
3. PDPA ไม่เกี่ยวกับข้อมูลสุขภาพ
4. PDPA ไม่เกี่ยวกับข้อมูลสุขภาพ

แนวทาง การใช้งานสื่อสังคมออนไลน์

วัตถุประสงค์

- 1. เพื่อใช้ในการสื่อสารและประชาสัมพันธ์
- 2. เพื่อใช้ในการประชาสัมพันธ์
- 3. เพื่อใช้ในการประชาสัมพันธ์
- 4. เพื่อใช้ในการประชาสัมพันธ์

ข้อควรระวัง

- 1. ไม่ควรเปิดเผยข้อมูลส่วนตัว
- 2. ไม่ควรเปิดเผยข้อมูลทางการแพทย์
- 3. ไม่ควรเปิดเผยข้อมูลที่เกี่ยวข้องกับผู้ป่วย

แนวทางปฏิบัติ ในการใช้งานสื่อสังคมออนไลน์

วัตถุประสงค์

- 1. เพื่อใช้ในการสื่อสารและประชาสัมพันธ์
- 2. เพื่อใช้ในการประชาสัมพันธ์
- 3. เพื่อใช้ในการประชาสัมพันธ์
- 4. เพื่อใช้ในการประชาสัมพันธ์

ข้อควรระวัง

- 1. ไม่ควรเปิดเผยข้อมูลส่วนตัว
- 2. ไม่ควรเปิดเผยข้อมูลทางการแพทย์
- 3. ไม่ควรเปิดเผยข้อมูลที่เกี่ยวข้องกับผู้ป่วย



ภาคผนวก ข

แบบสอบถามประเมินการรับรู้และการละเมิดแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ



**แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564**

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อ - สกุล.....ตำแหน่ง.....

หน่วยงาน / กลุ่มงาน.....

ตอนที่ 2 การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ฯ

ข้อ	เรื่อง	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHIMPRO ทุกๆ 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน				
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHIMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร				
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน(Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม				
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล				
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ				
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น				
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ				
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ				
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้อินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ				
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน				



ภาคผนวก ค

แบบสอบถามประเมินการรับรู้และการละเมิดแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
(ตัวอย่างการประเมิน)



**แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564**

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อ - สกุล นางสาวอรุณี ภูผา ตำแหน่ง ผู้จัดการงานทั่วไป/ปฏิบัติการ
 หน่วยงาน / กลุ่มงาน บริหารฯ

ตอนที่ 2 การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ฯ

ข้อ	เรื่อง	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHIMPRO ทุกๆ 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	/			/
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHIMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	/			/
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (User Account) ไม่ว่าจะการกระทำนั้นเกิดจากผู้ใช้งานหรือไม่ก็ตาม	/			/
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	/			/
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	/			/
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	/			/
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	/		/	/
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	/		/	
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	/			/
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	/			/



แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อ - สกุล.....นางสาว รัชชานันท์.....ตำแหน่ง.....อภ. - ๔๕๒ แพทย์ประจำบ้าน
หน่วยงาน / กลุ่มงาน.....กลุ่มเวชศาสตร์.....ศัลยกรรมศัลยกรรม

ตอนที่ 2 การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ฯ

ข้อ	เรื่อง	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHIMPRO ทุกๆ 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	✓			✓
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHIMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	✓			✓
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (User Account) ไม่ว่าจะการกระทำนั้นเกิดจากผู้ใช้งานหรือไม่ก็ตาม	✓			✓
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	✓			✓
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	✓			✓
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	✓			✓
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive, CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้ โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้อินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	✓			✓
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	✓			✓



**แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564**

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อ - สกุล..... ทพ.กวีพงษ์ มงคลพรหม ตำแหน่ง..... นักวิชาการสาธารณสุขปฏิบัติการ
 หน่วยงาน / กลุ่มงาน..... กศ.๑๓ สาธารณสุข

ตอนที่ 2 การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ฯ

ข้อ	เรื่อง	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHIMPRO ทุกๆ 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	/			/
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHIMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	/			/
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน(Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม	/			/
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	/			/
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	/			/
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	/			/
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้ โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	/			/
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	/			/
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	/			/
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	/			/


สรุปประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

หน่วยงาน	หัวหน้ากลุ่มงาน	ลายมือชื่อ	จำนวนรับ	จำนวนส่ง	หมายเหตุ
กลุ่มงานการแพทย์	นายจิระวัตร วิเศษสังข์	✓	4	4	
กลุ่มงานการพยาบาล	ดร.บุษบา บุญเกษมพันธ์	leg	2	2	
งานการพยาบาลผู้ป่วยนอก (OPD)	นางจุไรรัตน์ ศรีดี	ac	7	7	
งานการพยาบาลผู้ป่วยอุบัติเหตุ ฉุกเฉิน (ER)	นายสรารุท ท้าวนิล	✓	12	12	
งานการพยาบาลผู้ป่วยใน (IPD)	นายวรุต พุฒิกรเมธากุล	✓	15	15	
งานคลินิกโรคไม่ติดต่อเรื้อรัง (NCD)	นางสาวพัชนี ศิริจันทร์	พัชนี	4	4	
งานการพยาบาลหน่วยควบคุมการ ติดเชื้และงานจ่ายกลาง	นางสาวปิยะภรณ์ เพ็งมะดัน	Ahr	5	5	
กลุ่มบริหารงานทั่วไป	นางสาวรชิตา มุลลา	รชิตา	20	20	
กลุ่มงานทันตกรรม	นางสาวมณีนรัตน์ จันทพา	มณีนรัตน์	5	5	
กลุ่มงานรังสีวิทยา	นายจิโรจน์ จันทร์สนิทศรี	จิโรจน์	1	1	
กลุ่มงานโภชนศาสตร์	นางณัฐกานต์ ลาสิงหาญ	ณัฐกานต์	4	4	
กลุ่มงานเทคนิคการแพทย์	นางสาวกรภัทร์นิชา พิมพ์	พิมพ์	5	5	
กลุ่มงานจิตเวชและยาเสพติด	นางศิรดา ประรัมย์	ศิรดา	3	3	
กลุ่มงานเภสัชกรรมและคุ้มครอง ผู้บริโภค	นางสาววันชนก แก้วคะตา	วันชนก	9	6	
กลุ่มงานเวชศาสตร์ฟื้นฟู (กายภาพบำบัด)	นางสาวศุภรัตน์า จิตรรัก	ศุภรัตน์า	2	2	
กลุ่มงานบริการด้านปฐมภูมิและ องค์กรวม	นางดวงตะวัน ภูมิสี	ดวงตะวัน	8	8	
กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการ	นางสาวธัญญ์จิรา ปัญโญพิพัฒน์	ธัญญ์จิรา	7	7	
กลุ่มงานการแพทย์แผนไทยและ การแพทย์ทางเลือก	นางสาวศุภฤติกา สิงห์กุล	ศุภฤติกา	3	3	
รวม			116		



เช็คประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

ที่	ชื่อ - สกุล	ประเมินแล้ว	การละเมิด
กลุ่มงานการแพทย์			
1	นายจิระวัตร วิเศษสังข์	✓	
2	น.ส.อริยาพร เกษกุล	✓	
3	นายธนสันตชัย พรหมบุตร	✓	
4	นางสาวรัชนิกร บุตรรัตน์	✓	
กลุ่มงานการพยาบาล			
5	นางบุษบา บุญเกษมพันธ์	✓	
6	นายสำราญ งามหอม	✓	
งานการพยาบาลผู้ป่วยนอก (OPD)			
7	นางจุไรรัตน์ ศรีดี	✓	2
8	น.ส.อุทัยวรรณ จันทร์	✓	
9	น.ส.พรพรรณภัส นามวงศ์	✓	
10	นางโสภา รันทร	✓	
11	นายวัลลภ พันธุ์ขาว	✓	
12	นายณรงค์ศักดิ์ ทัตระสา	✓	
13	น.ส.ภัทราพร ไชยรัตน์	✓	
งานการพยาบาลผู้ป่วยอุบัติเหตุฉุกเฉิน (ER)			
14	นายสรารัฐ ท้าวนิล	✓	b
15	น.ส.สุจินันท์ สายสินธุ์	✓	
16	น.ส.จิรัฐติกาล วิเศษสังข์	✓	b
17	น.ส.พรศร นีรวรรณ	✓	b
18	นางสุธาสินี หนองกก	✓	
19	น.ส.ภาณุชนาถ เต็มใจ	✓	
20	น.ส.อาภาภรณ์ บุญปลุก	✓	
21	น.ส.วรัญญา สมัย	✓	9
22	น.ส.ปิยนุช บุญอินทร์	✓	b
23	นางผลนพร รุนพงษ์	✓	
24	นายปาริวัฒน์ คำสุข	✓	
25	น.ส.สมศรี คุณสาร	✓	
งานการพยาบาลผู้ป่วยใน (IPD)			
26	นายวรุฒ พุฒิกรเมธากุล	✓	
27	น.ส.ยุวลิ ไชโย	✓	


 แผนกพยาบาลประเมินการรับรู้และการละเมิด
 แนวปฏิบัติรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อ - สกุล: วิมลรัตน์ คุ้มสาร ตำแหน่ง: วิสัญญีพยาบาลทั่วไปผู้ปฏิบัติการ

หน่วยงาน / ภาควิชา: วิสัญญีฯ

ตอนที่ 2 การประเมินการรับรู้และการละเมิดแนวปฏิบัติรักษาความมั่นคงปลอดภัยฯ

ข้อ	เรื่อง	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HMPRO ทุกๆ 90 วัน หรือถูกครีมีมีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม HMPRO ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (User Account) ไม่ทำการกระทำนั้นหรือเกิดจากผู้ใช้งานหรือไม่ก็ตาม	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	ห้ามผู้ใช้งานนำอุปกรณ์กระจายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดในโรงพยาบาล โดยไม่อนุญาตจากผู้ดูแลระบบ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติงานราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive, CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากที่ตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่ เชื่อมต่อกับ อินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป้อนให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>



สรุปประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.2564

หน่วยงาน	หัวหน้ากลุ่มงาน	ลายมือชื่อ	จำนวนรับ	จำนวนส่ง	หมายเหตุ
กลุ่มงานการแพทย์	นายจิระวัตร วิเศษสังข์	✓	4	4	
กลุ่มงานการพยาบาล	ดร.บุษบา บุญเกษมพันธ์	✓	2	2	
งานการพยาบาลผู้ป่วยนอก (OPD)	นางจุไรรัตน์ ศรีดี	✓	7	7	
งานการพยาบาลผู้ป่วยอุบัติเหตุ ฉุกเฉิน (ER)	นายสรารุช ท้าวนิล	✓	12	12	
งานการพยาบาลผู้ป่วยใน (IPD)	นายวรุฒ พุฒิกรเมธากุล	✓	15	15	
งานคลินิกโรคไม่ติดต่อเรื้อรัง (NCD)	นางสาวพัชนี ศิริจันทร์	พัชนี	4	4	
งานการพยาบาลหน่วยควบคุมการ ติดเชื้และงานจ่ายกลาง	นางสาวปิยะภรณ์ เพ็งมะดัน	ปิยะ	5	5	
กลุ่มบริหารงานทั่วไป	นางสาวธิดา มุลลา	ธิดา	20	20	
กลุ่มงานทันตกรรม	นางสาวณัฏฐ์รัตน์ จันทพา	ณัฏฐ์	5	5	
กลุ่มงานรังสีวิทยา	นายจิโรจน์ จันทรสุนทรศรี	จิโรจน์	1	1	
กลุ่มงานโภชนศาสตร์	นางณัฐกานต์ ลาสิงหาญ	ณัฐกานต์	4	4	
กลุ่มงานเทคนิคการแพทย์	นางสาวกรภัทร์นิชา พิมพร	กรภัทร์	5	5	
กลุ่มงานจิตเวชและยาเสพติด	นางศรिता ประรัมย์ย์	ศรिता	3	3	
กลุ่มงานเภสัชกรรมและคุ้มครอง ผู้บริโภค	นางสาววันชนก แก้วคะตา	วันชนก	9	6	
กลุ่มงานเวชศาสตร์ฟื้นฟู (กายภาพบำบัด)	นางสาวศุภรัตน์า จิตรัก	ศุภรัตน์	2	2	
กลุ่มงานบริการด้านปฐมภูมิและ องค์กรวม	นางดวงตะวัน ภูมิลี	ดวงตะวัน	8	4	
กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการ	นางสาวธัญญ์จิรา ปัญญาพิพัฒน์	ธัญญ์จิรา	7	7	
กลุ่มงานการแพทย์แผนไทยและ การแพทย์ทางเลือก	นางสาวศุภธิดา สิงห์กุล	ศุภธิดา	3	3	
รวม			116		

