

# ทีมการจัดการความรู้และสารสนเทศ (KM-IT)



# การพัฒนางานคุณภาพด้านการจัดการความรู้และสารสนเทศ

เพื่อพัฒนาโรงพยาบาลสู่ SMART HOSPITAL

## ทีม KM-IT

**วิสัยทัศน์ :** สร้างและใช้องค์ความรู้ที่มีคุณภาพ เพื่อการพัฒนาโรงพยาบาล

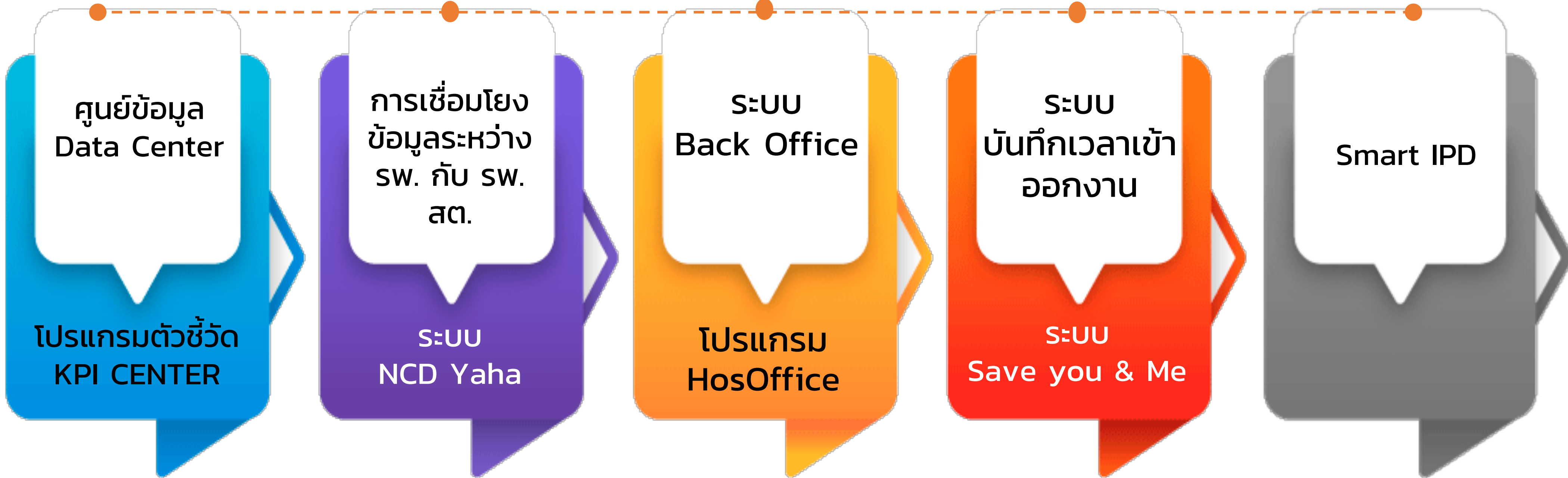
## เป้าประสงค์

1. มีระบบการสร้างการจัดการความรู้ที่มีประสิทธิภาพ
2. มีการนำองค์ความรู้และผลงานไปใช้ประโยชน์
3. เพื่อเป็นองค์กรแห่งนวัตกรรม





# ระบบสารสนเทศของโรงพยาบาล



ศูนย์ข้อมูล  
Data Center

โปรแกรมตัวชี้วัด  
KPI CENTER

การเชื่อมโยง  
ข้อมูลระหว่าง  
sw. กับ sw.  
สต.

ระบบ  
NCD Yaha

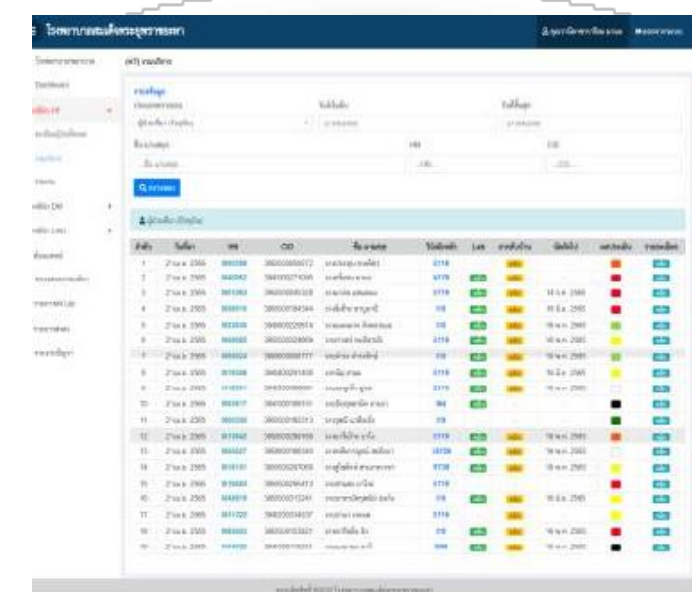
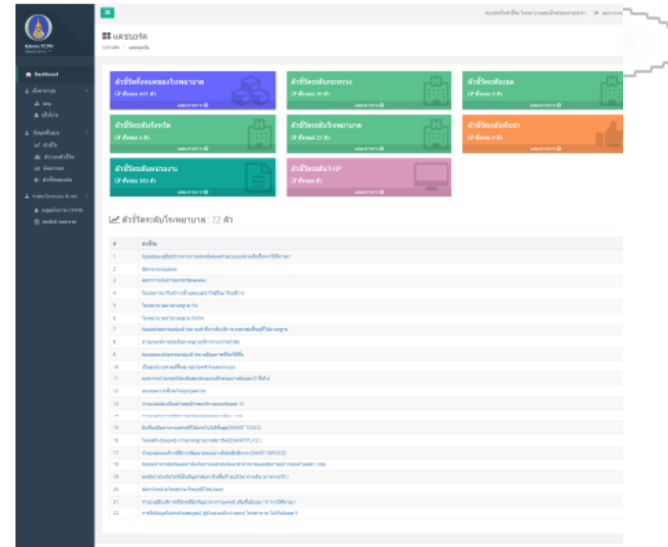
ระบบ  
Back Office

โปรแกรม  
HosOffice

ระบบ  
บันทึกเวลาเข้า  
ออกงาน

ระบบ  
Save you & Me

Smart IPD



ปรับ HOSxP V.3  
เป็น HOSxP V.4 และ  
ระบบ IPD Paperless

+ ตอบเทคโนโลยีอื่นๆที่ใช้ในหน่วยงานทั้งหมด  
ได้ทั้งที่ IT ติดตั้งให้และที่หน่วยงานหาติดตั้งกันเอง (โปรแกรมและ application ต่างๆ)



# การให้บริการของโรงพยาบาล สำหรับผู้รับบริการ

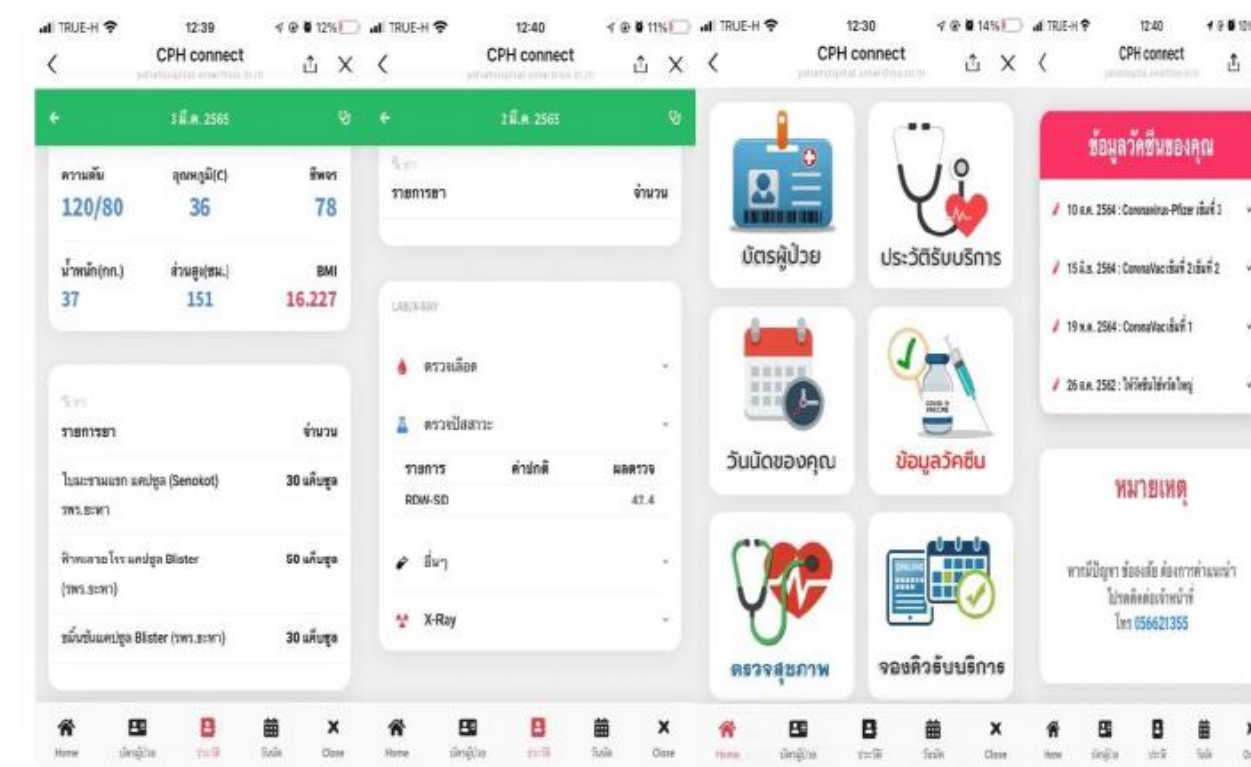
การลงทะเบียนรับบริการผ่าน  
ตู้คิวอัจฉริยะ (ตู้ KIOSK)



หมอรู้จักคุณ  
ระบบการให้บริการสุขภาพระยะ  
ไกลที่รพ. ใช้อยู่ปัจจุบัน

โดยอยู่ขั้นตอนทดลองใช้

LINE YCPH Connect  
ระบบประเมินสุขภาพ  
อิเล็กทรอนิกส์ส่วนบุคคล



เพจ Facebook  
โรงพยาบาล



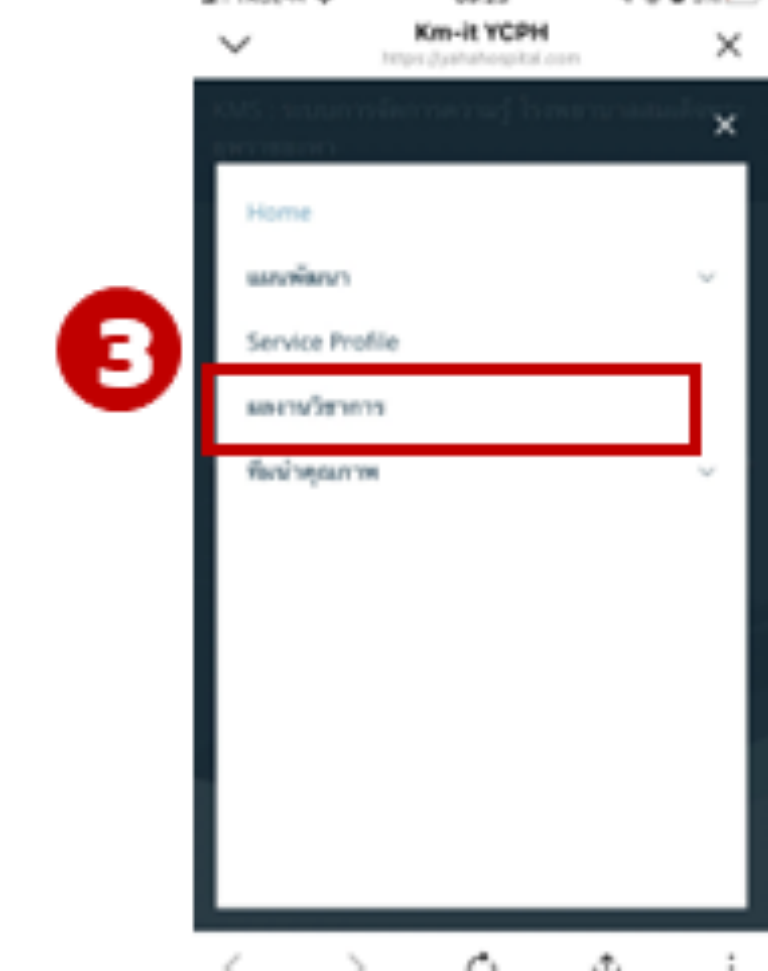
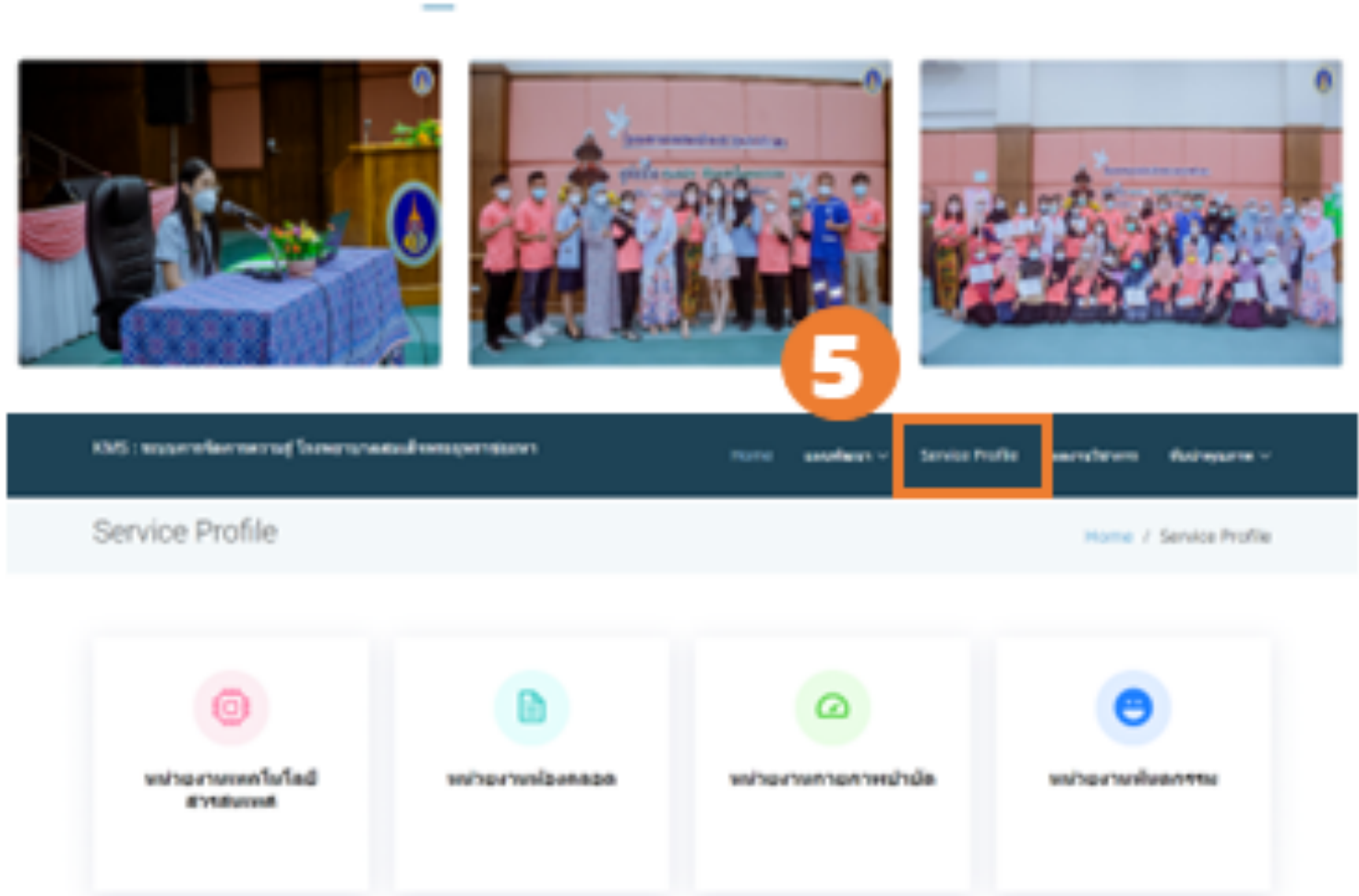
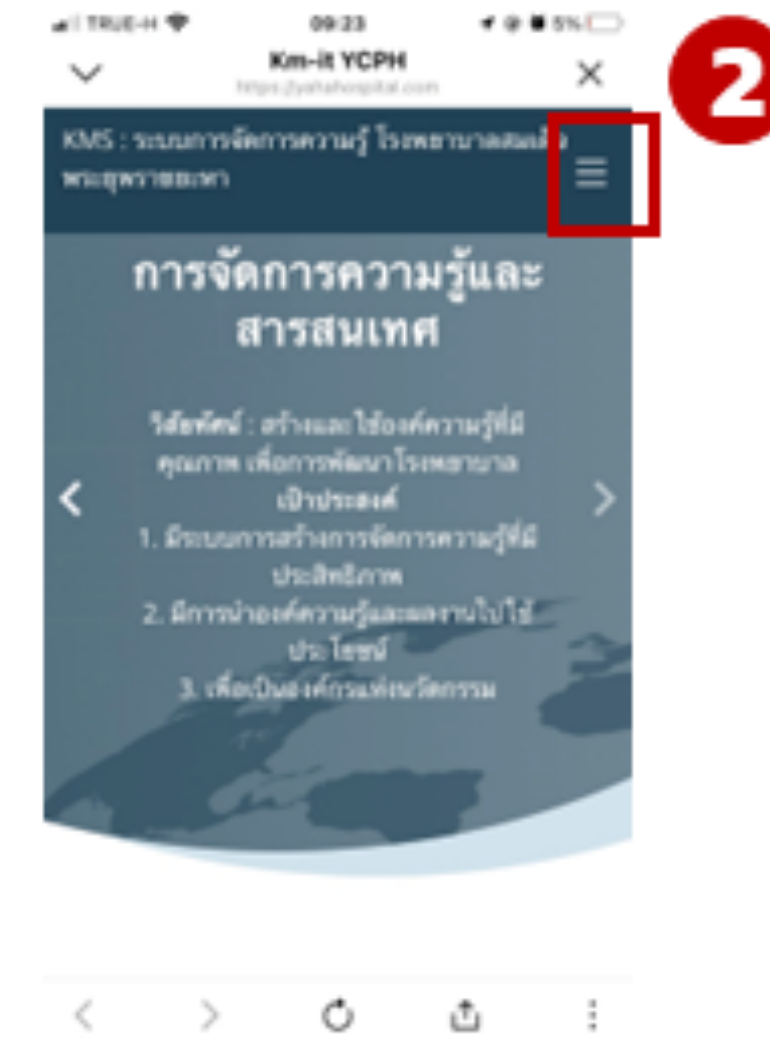
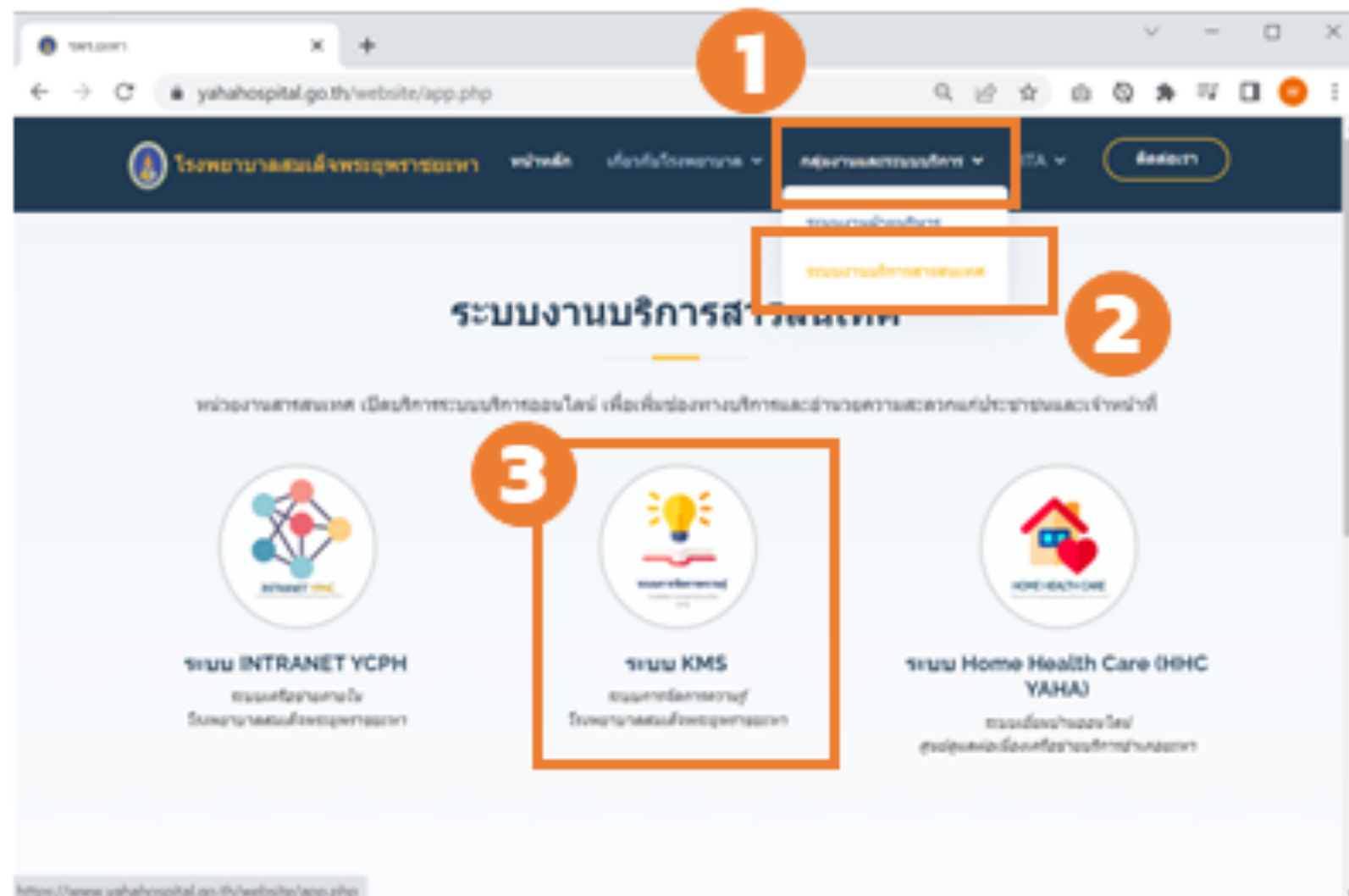




# ขั้นตอนการเข้าใช้ระบบการจัดการความรู้ (KMS)

เข้าผ่านเว็บไซต์โรงพยาบาล <https://www.yahahospital.go.th/>

หรือ เข้าผ่านไลน์ **Save you&me**





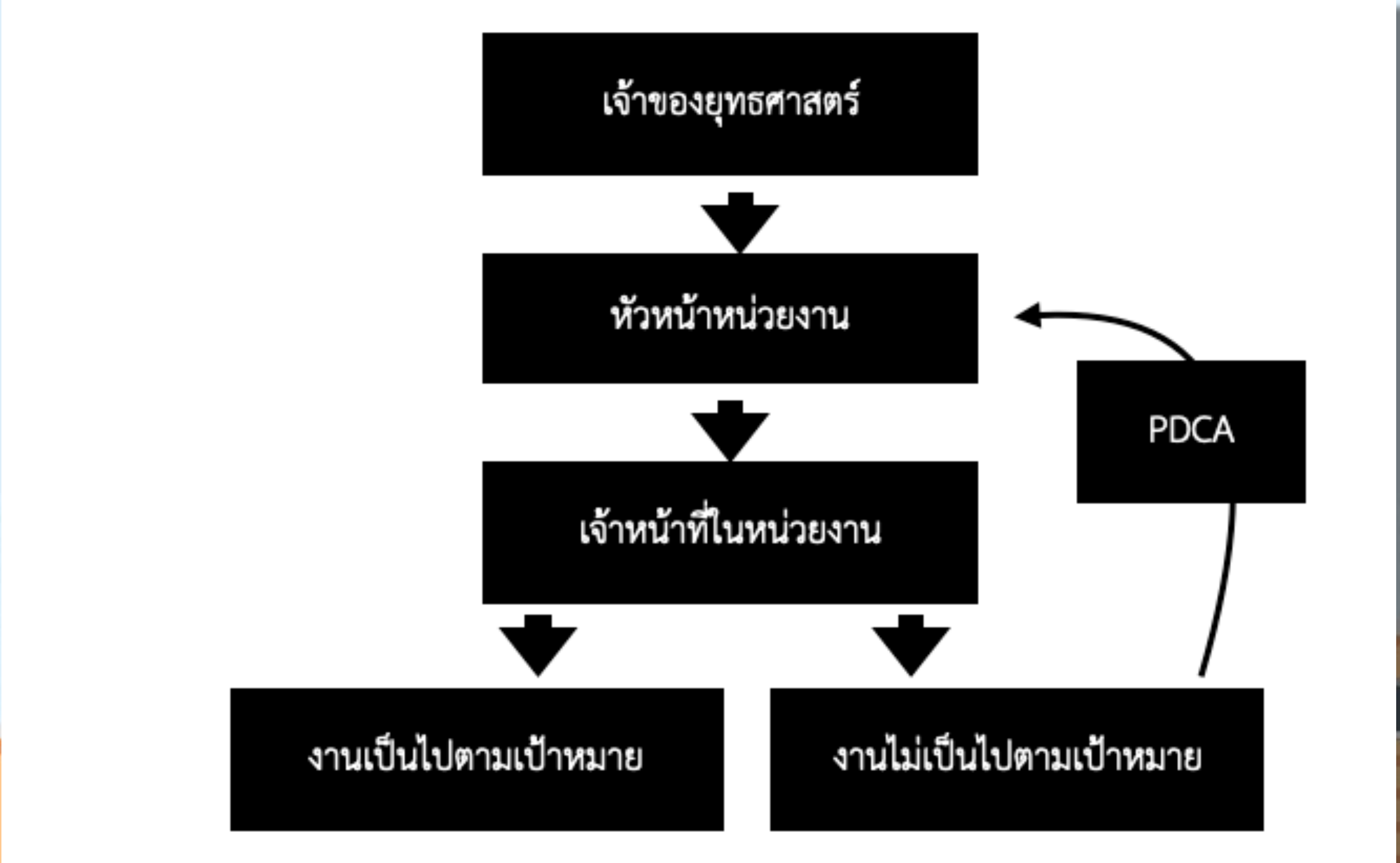
## แนวทางการพัฒนาที่ต้องอาศัยความร่วมมือจากหน่วยงาน

1. เจ้าหน้าที่ในหน่วยงานมีนวัตกรรมส่งประเมินอย่างน้อย 80% ของจำนวนเจ้าหน้าที่ทั้งหมดในหน่วยงาน
2. ทุกหน่วยงานส่ง SP/WI (คู่มือการปฏิบัติงาน/มาตรฐานการปฏิบัติงาน)
3. เตรียมเรื่องที่ภูมิใจในหน่วยงาน ที่มีกระบวนการวิเคราะห์ และแก้ไขปัญหา (เล่าเรื่องเป็นลักษณะ PDCA)
4. ทราบ ตัวชี้วัดสำคัญในหน่วยงานตัวเอง ตัวชี้วัดที่เป็นปัญหาของหน่วยงาน  
ยกตัวอย่างวิธีการแก้ไขปัญหา มีการวิเคราะห์แล้วนำไปใช้ประโยชน์อย่างไร
5. ลงบันทึกผลตัวชี้วัดใน KPI Center ภายในวันที่ 10 ของทุกเดือน





# มีการติดตามตัวชี้วัด และทบทวน



# นโยบายการป้องกันความมั่นคงปลอดภัยด้านไซเบอร์

ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม

## ควรกระทำ

### CHANGE

ต้องตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่  
ทุกๆ 3 เดือน ต้องไม่คาดเดาง่าย

### LOGOUT

ออกจากระบบทุกครั้งหลังใช้งาน



หากผู้ใช้งานไม่ปฏิบัติตามมาตรการที่กำหนดไว้ แล้ว  
เกิดปัญหาในการใช้ระบบตามมา ผู้ใช้งานนั้นๆ ต้อง  
รับผิดชอบในความผิดพลาดของตนเอง

## ห้ามกระทำ

### ACCESS

ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบโดยไม่ได้รับอนุญาตจาก  
แพทย์หรือผู้รับผิดชอบโดยตรง

### SHARE

ห้ามผู้ใช้งานระบบนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผย  
ข้อมูลต่อสาธารณะผ่านทาง LINE, Facebook หรืออื่นๆ Social media หาก  
มีความจำเป็นต้องได้รับการยินยอมจากผู้ป่วยหรือญาติเป็นลายลักษณ์อักษร

### DOWNLOAD

ห้ามดาวน์โหลด โปรแกรมจาก Internet หรือ Update โปรแกรมต่างๆ  
นอกเหนือที่ผู้ดูแลระบบกำหนด

### MOVE

ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือกระทำการใดๆต่ออุปกรณ์  
ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

### INSTALL

ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เช่น Printer, อุปกรณ์  
กระจายสัญญาณต่างๆและอื่นๆมาเชื่อมต่อกับระบบคอมพิวเตอร์หรือระบบ  
เครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต



# นโยบายการป้องกันความมั่นคงปลอดภัยด้านไซเบอร์

## นโยบายการป้องกันความมั่นคง ปลอดภัยด้านไซเบอร์

## ประเมินการรับรู้นโยบาย



**ประกาศโรงพยาบาลสมเด็จพระยุพราชยะหา**  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

การกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของโรงพยาบาลสมเด็จพระยุพราชยะหา มีวัตถุประสงค์สำคัญเพื่อป้องกันมิให้บุคคลภายนอกที่ไม่มีอำนาจหน้าที่ เข้าถึง แก้ไข ปรับปรุง เปลี่ยนแปลง และเพื่อลดความเสี่ยงของกรถูกโจมตีด้วยไวรัสคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดความไม่ปลอดภัยของข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่ายของโรงพยาบาล จึงเห็นสมควรกำหนดข้อปฏิบัติ ดังนี้

**การรักษาความปลอดภัยในการใช้จากระบบอินเตอร์เน็ตของโรงพยาบาล**

1. ให้เจ้าหน้าที่ที่รับผิดชอบ (Password) ของตนเองในการใช้งานระบบคอมพิวเตอร์ของโรงพยาบาล โดยกำหนดให้ทำการเปลี่ยนรหัสผ่านทุก 3 เดือน
2. ผู้ใช้งาน ห้ามใช้รหัสผ่านที่ผู้ใดคาดเดาได้ง่าย เช่น ชื่อเล่น ชื่อหน่วยงาน หมายเลขโทรศัพท์ วันเดือนเกิด เป็นต้น
3. ให้เจ้าหน้าที่ที่รับผิดชอบ ไม่เปิดเผยให้ผู้ใดที่มิใช่พนักงานของโรงพยาบาลใช้
4. ต้องเข้าระบบอินเตอร์เน็ตของโรงพยาบาลหรือโปรแกรม (HCS) ด้วยชื่อที่ใช้จริง (Pseudonym) ของตนเองเท่านั้น
5. ต้องออก (Logout) จากโปรแกรม HCS ทุกครั้งเมื่อเลิกใช้งานแล้ว
6. ไม่อนุญาตให้หน่วยงานรวมใจคอมพิวเตอร์ใช้งานจากอินเตอร์เน็ต (Internet) หรือ ปรับปรุง (update) โปรแกรมต่างๆ ลงสู่คอมพิวเตอร์สำนักงาน นอกเหนือที่ผู้ดูแลระบบกำหนดไว้ในองค์กร
7. ขอให้ผู้ใช้จากระบบอินเตอร์เน็ต Browser : Google Chrome ในการเข้าใช้งานอินเตอร์เน็ตเป็นหลัก เพราะ Google Chrome มีระบบป้องกันที่ค่อนข้างน่าเชื่อถือมากกว่า Browser อื่นๆ ยกเว้น หากมีความจำเป็นต้องใช้ Browser อื่นๆ ขอให้แจ้งงานเทคโนโลยีสารสนเทศ (IT)
8. ไม่ควรคลิกลิ้งค์หรือเปิดไฟล์แนบจากผู้ที่ไม่รู้จัก ที่ใน Email ,line ,facebook
9. ผู้ใช้งานอินเตอร์เน็ต หากเป็นการใช้งานที่ไม่เกี่ยวข้องกับข้อมูลของโรงพยาบาล ขอให้ใช้ผ่านโทรศัพท์หรือแท็บเล็ตส่วนตัวเป็นหลัก เพื่อป้องกันการถูกแฮ็กจากระบบเครื่องคอมพิวเตอร์หน่วยงานของโรงพยาบาล

แบบประเมินการรับรู้และเข้าใจประกาศนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โรงพยาบาลสมเด็จพระยุพราชยะหา

ผู้ดูแลระบบสารสนเทศ (IT) : [wanee.it@gmail.com](mailto:wanee.it@gmail.com) (ส่งไปรษณีย์) **สมัครบัญชี**

\*จำเป็น

ชื่อ-สกุล \*

คำตอบของคุณ

ชื่อหน่วยงาน \*

คำตอบของคุณ

ถัดไป ล้างแบบฟอร์ม

กำลังส่งผ่าน Google ฟอร์ม

ลิงก์ที่ได้อีกครั้งซึ่งส่งให้โดย Google ฟอร์มของคุณคือ - [คลิกที่นี่เพื่อดูการตั้งค่าเพิ่มเติม](https://forms.gle/J8FrwufXkVvFqSKaA) - [ปิดหน้าต่างนี้](#)

Google ฟอร์ม

แบบประเมินการรับรู้และเข้าใจประกาศนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โรงพยาบาลสมเด็จพระยุพราชยะหา

ผู้ดูแลระบบสารสนเทศ (IT) : [wanee.it@gmail.com](mailto:wanee.it@gmail.com) (ส่งไปรษณีย์) **สมัครบัญชี**

\*จำเป็น

ชื่อ-สกุล \*

คำตอบของคุณ

ชื่อหน่วยงาน \*

คำตอบของคุณ

ถัดไป ล้างแบบฟอร์ม

กำลังส่งผ่าน Google ฟอร์ม

ลิงก์ที่ได้อีกครั้งซึ่งส่งให้โดย Google ฟอร์มของคุณคือ - [คลิกที่นี่เพื่อดูการตั้งค่าเพิ่มเติม](https://forms.gle/J8FrwufXkVvFqSKaA) - [ปิดหน้าต่างนี้](#)

Google ฟอร์ม



ลิงก์แบบประเมิน : <https://forms.gle/J8FrwufXkVvFqSKaA>