ประเด็นที่ 6 : Good Governance

หัวข้อ 6.3 การพัฒนาระบบเทคโนโลยีสารสนเทศ (ICT) เป็นศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน

ร้อยละของจังหวัดที่มีการใช้บริการศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน

น.พ.อนันต์ กนกศิลป์

ผอ.ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ

ประชุมชี้แจงแผนการตรวจราชการกระทรวงสาธารณสุข ประจำปี 2565

วันที่ 9 พฤศจิกายน 2564

มิติการดำเนินการกับระบบข้อมูลสุขภาพ

- พรบ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
- กฎกระทรวง แบ่งส่วนราชการสำนักงานปลัดกระทรวง

CIO ,CTO | Data Utilization

5

AI ,Dashboard, Report

CDO | 2 | Data Governance

3 | CCSO

พรบ.ความมั่นคงปลอดภัยไซเบอร์

4 | DPO

- พรบ.คุ้มครองข้อมูลส่วนบุคคล
- พรบ.สุขภาพแห่งชาติ
- ระเบียบกระทรวงสาธารณสุข

ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล

1 | CIO ,CTO

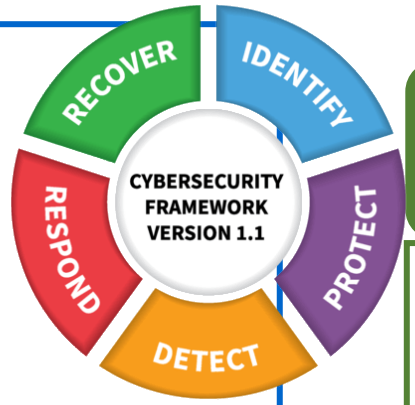
พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

มติครม. เรื่องแนวทางการบริหารจัดการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ

Cyber security Management

Risk Management
มาตราการป้องกัน

1. **Hardening Infrastructure** (สร้างความเข้มแข็งของ Hardware , Software , Network)
   - Vulnerability Assessment (VA)
   - Firewall , License , Patch , Anti Virus
   - Fire Protection , Access
2. **Data Integrity** (การรักษาความมั่นคง ปลอดภัยของข้อมูล)
   - Backup 3 copy ด้วยความถี่ที่เหมาะสม , DR site
3. **User Awareness** (สร้างความตระหนักของผู้ใช้งาน)
   - e-Mail , Thumb Drive , Share file
4. **System Redundant**
   - Active-Active , Active-Passive , Offline Backup
5. **จัดทำ BCP** (แผนรับเหตุฉุกเฉิน/แผนความต่อเนื่อง)
   - Business Contingency Plan
   - Business Continuity Plan



ISO 27799

ISO 27001

Recovery Response
มาตรการเผชิญเหตุ

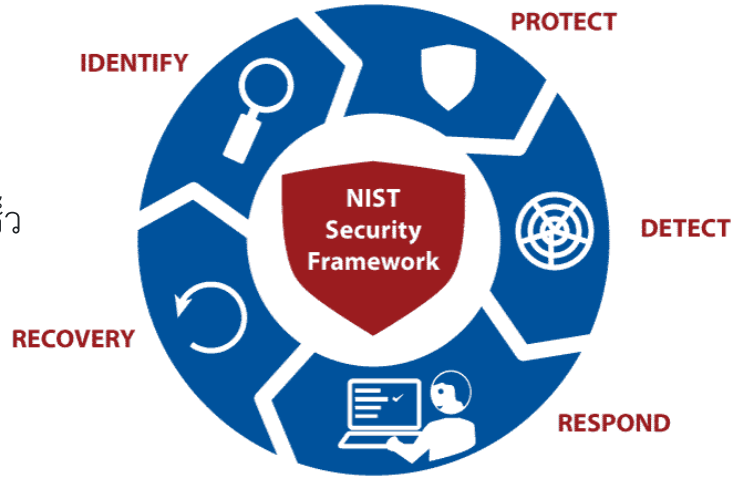
ISO/IEC 27001 Information Security Management

1. **Investigation**
   - หาสาเหตุ
2. **System Recovery**
   - Cleansing OS , HIS , Network , Client
3. **Data Recovery**
   - Backup Restore
4. **Business Recovery**
   - Maunual

NIST Cybersecurity Framework

มีความสอดคล้องกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 13 คณะกรรมการกำกับดูแลฯ มีหน้าที่กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานข้อกำหนดขั้นต่ำ โดยคำนึงถึงหลักการบริหารความเสี่ยง ต้องประกอบด้วย

1. **Identify :** การระบุความเสี่ยง เข้าใจสภาพแวดล้อมของตนเอง ทรัพย์สิน และความเสี่ยงที่มี
2. **Protect :** มาตรการป้องกันความเสี่ยง หาแนวทางที่เหมาะสมในการปกป้องทรัพย์สิน
3. **Detect :** มาตรการตรวจสอบและเฝ้าระวัง ตรวจจับและเฝ้าระวังภัยคุกคามที่อาจจะเกิดขึ้น
4. **Response :** มาตรการเผชิญเหตุ ตอบสนองได้ทันท่วงที เพื่อลดผลกระทบหรือจำกัดความเสียหายให้อยู่ในวงแคบ
5. **Recovery :** มาตรการรักษาและฟื้นฟู สามารถกู้คืน ระบบขึ้นมาให้บริการตามปกติได้อย่างรวดเร็วภายใต้งบประมาณและหลักการบริหารความเสี่ยงขององค์กร



สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology : NIST) ของสหรัฐอเมริกา

กระบวนการ PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. กำหนดให้บุคคลหรือนิติบุคคล เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตาม มาตรา 6 และ 19 ทำหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2. ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer หรือ DPO) ตาม มาตรา 41
3. ต้องมีการแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลและแจ้งความเป็นส่วนตัว (Privacy Notice) ให้แก่เจ้าของข้อมูลส่วนบุคคลนั้นๆ ทราบโดยชัดเจน
4. กรณีกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลไม่ใช่ภารกิจโดยตรงตามฐานอำนาจทางกฎหมาย จำเป็นต้องมีกระบวนการให้เจ้าของข้อมูลส่วนบุคคลแสดงความยินยอมโดยชัดแจ้ง
5. ต้องมีมาตรการแสดงความรับผิดชอบ และมาตรการเยียวยาให้กับเจ้าของข้อมูลส่วนบุคคล หากเกิดความผิดพลาดหรือมีการรั่วไหลของข้อมูลนั้นๆ
6. ต้องมีกระบวนการ Implementation and Monitoring อย่างเป็นรูปธรรม และต่อเนื่อง

ธรรมาภิบาลข้อมูลภาครัฐ

ในระดับหน่วยงาน ต้องประกอบด้วยเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้

(1) การ**กำหนดสิทธิ หน้าที่ และความรับผิดชอบ**ของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน

(2) การ**วางแผนการดำเนินงาน การปฏิบัติ**ตามแผนการดำเนินงาน **การตรวจสอบ**และ**การรายงานผล**การดำเนินงาน และ**การปรับปรุงแผน**การดำเนินงานอย่างต่อเนื่อง เพื่อให้ระบบบริหารและกระบวนการจัดการข้อมูลมีประสิทธิภาพสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันทั้งภายในและภายนอกหน่วยงาน และคุ้มครองข้อมูลให้มีประสิทธิภาพ

(3) การ**กำหนดมาตรการควบคุมและพัฒนาคุณภาพข้อมูล** เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ถูกละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

(4) การ**วัดผลการบริหารจัดการข้อมูล** โดยอย่างน้อยประกอบด้วย การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล

(5) การ**จำแนกหมวดหมู่ของข้อมูล** เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่างๆ ภายในหน่วยงาน สาหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

(6) การ**จัดทำคำอธิบายชุดข้อมูลดิจิทัล**ของภาครัฐและ**บัญชีข้อมูล**ให้มีความ**ถูกต้อง ครบถ้วนและเป็นปัจจุบัน**

คำนิยาม

ร้อยละของจังหวัดที่มีการใช้บริการศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน

ศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน หมายถึง **แหล่งข้อมูลด้านสุขภาพที่บริหารจัดการจากศูนย์กลาง**ให้มีมั่นคงปลอดภัยทางไซเบอร์ และมีความพร้อมใช้**ให้บริการแก่เจ้าของข้อมูลในรูปแบบของ PHR** (Personal Health Record) และความรู้สุขภาพเฉพาะบุคคล (Personal Health Literacy) **และพร้อมให้บริการข้อมูลแก่หน่วยงานต่างๆ ที่เกี่ยวข้องเพื่อประโยชน์ในการดูแลรักษาชีวิตและสุขภาพของเจ้าของข้อมูล** และเพื่อประโยชน์แก่วงการสุขภาพและสาธารณสุขของประเทศไทย

การใช้บริการศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน หมายถึง **โรงพยาบาลเชื่อมโยงข้อมูลตามชุดข้อมูลที่กำหนด ระหว่างกันได้สำเร็จผ่าน HIS Gateway** และ**จังหวัดมีมาตรการในการกำกับดูแลด้านธรรมาภิบาล** มีการแต่งตั้งคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ

โรงพยาบาล หมายถึง โรงพยาบาลใน**สังกัดสำนักงานปลัด**กระทรวงสาธารณสุข สังกัด**กรมการแพทย์** สังกัด**กรมสุขภาพจิต** สังกัด**กรมควบคุมโรค**

คณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ ประกอบด้วย ผู้แทนจากสำนักงานสาธารณสุขจังหวัด (**สสจ.**) สำนักงานสาธารณสุขอำเภอ (**สสอ.**) โรงพยาบาลศูนย์ (**รพศ.**) โรงพยาบาลทั่วไป (**รพท.**) โรงพยาบาลชุมชน (**รพช.**) โดย**มีหน้าที่**ในการ**กำหนดนโยบาย กำกับติดตาม** ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การคุ้มครองข้อมูลส่วนบุคคล (PDPA) การใช้ประโยชน์ข้อมูลสุขภาพส่วนบุคคลภายใต้กฎหมายที่เกี่ยวข้อง การรับส่งข้อมูลตามมาตรฐานที่ตกลงร่วมกัน และการนำข้อมูลสุขภาพไปใช้ประโยชน์ในการให้บริการแก่ประชาชนในรูปแบบต่างๆ (Data Governance)

Small Success

ร้อยละของจังหวัดที่มีการใช้บริการศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน

3 เดือน	6 เดือน	9 เดือน	12 เดือน
ทุกจังหวัด มีการแต่งตั้งคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ	รพ. ที่ติดตั้ง HIS Gateway และมีผลการเชื่อมโยงข้อมูลสำเร็จ มีจำนวนไม่น้อยกว่าร้อยละ 20 ของจำนวน รพ.* ทั้งจังหวัด	-	รพ. ที่ติดตั้ง HIS Gateway และมีผลการเชื่อมโยงข้อมูลสำเร็จ มีจำนวนไม่น้อยกว่าร้อยละ 60 ของจำนวน รพ.* ทั้งจังหวัด

* โรงพยาบาล หมายถึง โรงพยาบาลในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข สังกัดกรมการแพทย์ สังกัดกรมสุขภาพจิต สังกัดกรมควบคุมโรค

ประเด็นการตรวจราชการที่มุ่งเน้น

ร้อยละของจังหวัดที่มีการใช้บริการศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน

เป้าหมาย	มาตรการที่ดำเนินงานในพื้นที่	แนวทางการตรวจ ติดตาม	ผลลัพธ์ที่ต้องการ
ทุกจังหวัด	แต่งตั้งคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพในระดับจังหวัด	ส่งข้อมูลให้ ศทส.สป.	ทุกจังหวัดมีการประชุมกำกับติดตามการดำเนินงานด้านธรรมาภิบาลอย่างสม่ำเสมอ
โรงพยาบาลทุกแห่ง	เชิญชวนให้โรงพยาบาลทุกแห่งเข้าร่วมอบรมการติดตั้งใช้งาน HIS Gateway รุ่นปัจจุบัน	ดูผลลัพธ์การเข้าร่วมอบรมและผลทดสอบ	รพ. ทุกแห่งทั่วประเทศ เข้าร่วมอบรม
หน่วยงานทุกแห่ง	กำกับติดตามให้หน่วยงานตอบแบบสอบถามสถานะความพร้อมด้านไซเบอร์ ออนไลน์	ศทส.สป. สรุปผลการตอบ	มีสถานะความพร้อมด้านไซเบอร์ในภาพรวม สธ.
โรงพยาบาลทุกแห่ง	กำกับติดตามให้โรงพยาบาลทุกแห่งติดตั้ง HIS Gateway และใช้ประโยชน์อย่างสม่ำเสมอเพื่อคุณภาพของข้อมูลที่ประชาชนจะได้รับ	ศทส. ดู Log การใช้ HIS Gateway จาก Server http://hisgateway.moph.go.th/	รพ. อื่นๆ ที่ ประชาชน เจ้าของข้อมูลเข้ารับบริการ เรียกใช้ข้อมูลของผู้รับบริการรายนั้นจาก โรงพยาบาลอื่นได้อย่างมีคุณภาพ

แบบสอบถามด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Survey)
เพื่อใช้ในการปรับปรุงระบบและเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์
สำหรับหน่วยงานสาธารณสุข (Health Sector) ปี 2565

วัตถุประสงค์ เพื่อนำผลวิเคราะห์ไปใช้ประกอบการจัดทำแผนเสนอขอรับงบประมาณด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกระทรวงสาธารณสุข

ข้อมูลระบบสารสนเทศภายในหน่วยงาน (IT system detail)

หมายเหตุ ข้อมูลจะถูกจัดเก็บและปกปิดเป็นความลับเฉพาะหน่วยงานผู้ตอบแบบสอบถาม และ ศทส.สป.สธ. ซึ่งเป็นผู้รวบรวมเท่านั้น

12. แผนผังระบบเครือข่าย และ ระบบงาน (Network and System diagram) *

แนบไฟล์

13. จำนวน IP Address ที่เป็น Private IP ที่ใช้ภายในหน่วยงาน (ระบุเป็น Subnet Mask หรือ ชุดไอพี เช่น 192.168.1.0/24) *

.....

https://ops-service.moph.go.th/

14. ประเภทสายสื่อสัญญาณในการเชื่อมโยงเครือข่ายอินเทอร์เน็ตของหน่วยงาน (Link Internet) *

- ☐ MPLS (อินทราเน็ตที่ สป.สธ. โดย ศทส. จัดสรรให้)
- ☐ MPLS (อินทราเน็ตที่หน่วยงานเช่าใช้บริการเอง)
- ☐ Leased Line internet
- ☐ FTTX Home use
- ☐ อื่นๆ: .....

15. จำนวน IP Address ที่เป็น Public IP สำหรับใช้ในการเข้าถึงจากเครือข่ายอินเทอร์เน็ต *

- ☐ 1
- ☐ 2-5
- ☐ มากกว่า 5 หมายเลข
- ☐ ไม่มี Public IP ใช้งาน

รายละเอียดข้อมูลด้าน Cyber Security)

26. จำนวนอุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย (Firewall) ของหน่วยงานทั้งหมด*

- ☐ ไม่มี
- ☐ 1 เครื่อง
- ☐ 1 ระบบ (2 เครื่องทำ HA)
- ☐ 2 เครื่อง
- ☐ 2 ระบบ (4 เครื่อง ทำ HA)
- ☐ มากกว่า 2 เครื่อง
- ☐ อื่นๆ โปรดระบุ : .....

27. ยี่ห้อและรุ่นของ firmware ของอุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย (Firewall) *

.....

28. หน่วยงานมีการใช้ Proxy หรือ Application Gateway หรือไม่ ในการใช้งานอินเทอร์เน็ต *

- ☐ ใช้
- ☐ ไม่ใช้

29. หน่วยงานมีการใช้ Software ประเภท endpoint security (antivirus) ยี่ห้อใด ภายในหน่วยงาน (สามารถตอบได้มากกว่า 1) *

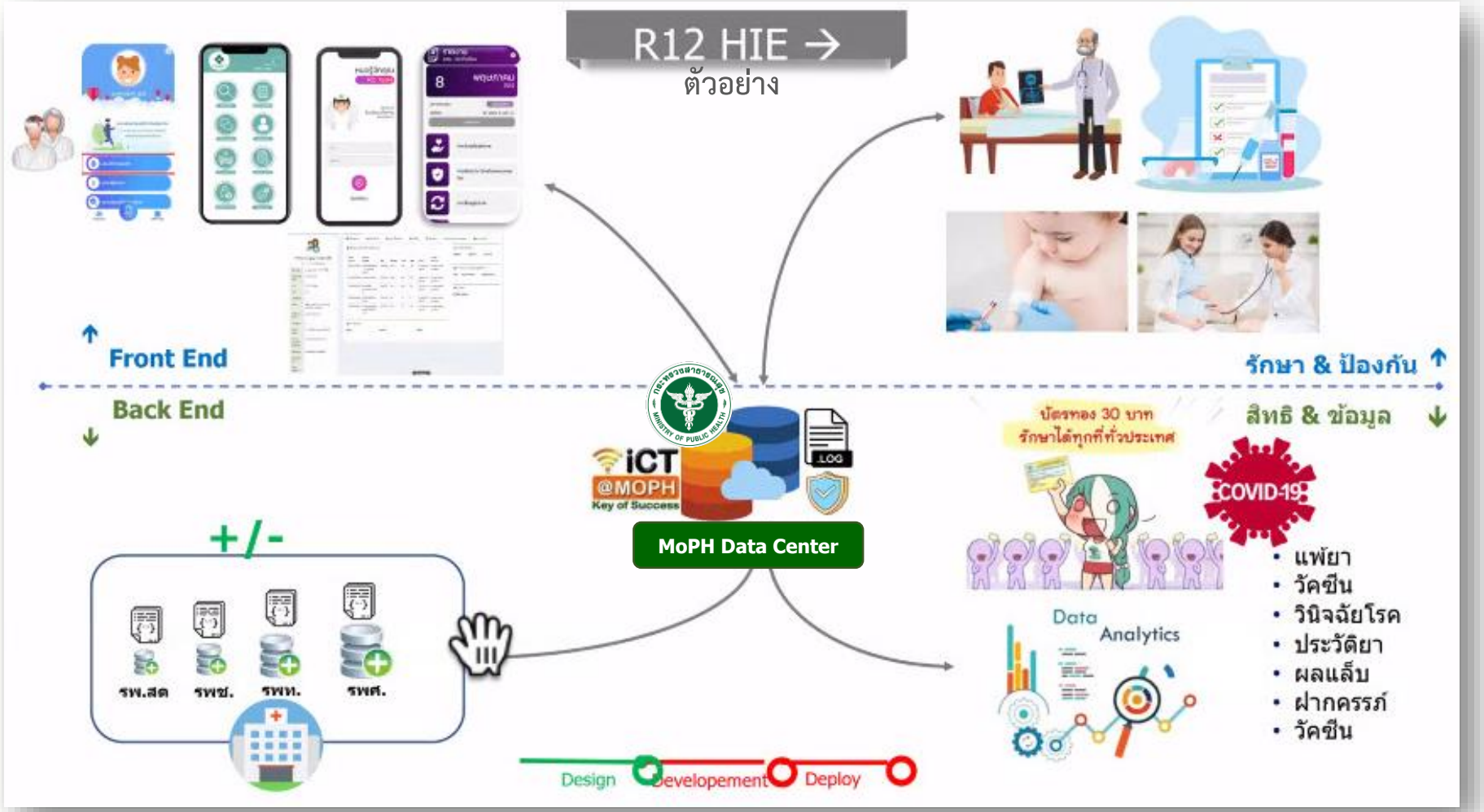
.....

30. ชนิดของ Software ประเภท endpoint security (antivirus) ที่ใช้ภายในหน่วยงาน *

- ☐ commercial grade
- ☐ Cloud Base

HIS Gateway

เครื่องมือกลางเชื่อมโยงข้อมูลสุขภาพเพื่อคุณภาพการให้บริการประชาชนได้อย่างไร้รอยต่อ
บนแพลตฟอร์มระบบสุขภาพดิจิทัล (NDHP : National Digital Health Platform)
http://hisgateway.moph.go.th/



ผลการดำเนินงาน : *(ณ ต.ค.64)*
จำนวนหน่วยงานที่ติดตั้ง HIS Gateway

เขต 1 : 20 รพ. คิดเป็น 20%
เขต 4 : 27 รพ. คิดเป็น 38%
เขต 9 : 30 รพ. คิดเป็น 33%
เขต 12 : 56 รพ. คิดเป็น 71%

แผนการอบรมภาคปฏิบัติ :

เขต 1 : 30 พ.ย. - 3 ธ.ค. 64 (เชียงใหม่)
เขต 4 : 8 - 9 ธ.ค. 64 (นนทบุรี)
เขต 9 : 13 - 14 ธ.ค. 64 (โคราช)
เขต 12 : 16 - 17 ธ.ค. 64 (ออนไลน์)


Thank You