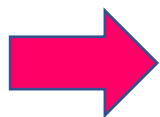


# PDPA & Cyber security in office

วัชร รุ่งอรุณย์นันท์  
ศูนย์เฝ้าระวังความปลอดภัยด้านผลิตภัณฑ์สุขภาพ (HPVC)  
สำนักงานคณะกรรมการอาหารและยา

# 1. แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร

- ศูนย์เฝ้าระวังความปลอดภัยด้านผลิตภัณฑ์สุขภาพ (Health Product Vigilance Center: HPVC) สำนักงานคณะกรรมการอาหารและยา (อย.) มีฐานข้อมูลรายงานเหตุการณ์ไม่พึงประสงค์จากการใช้ผลิตภัณฑ์สุขภาพ (Thai Vigibase) โดยเป็นฐานข้อมูลที่เก็บรายงานเหตุการณ์ไม่พึงประสงค์จากการใช้ผลิตภัณฑ์สุขภาพ (adverse event: AE) ของผู้ป่วยเฉพาะราย (โดยรายงานมีข้อมูลที่จำเป็นต่อการประเมินความปลอดภัยจากการใช้ผลิตภัณฑ์สุขภาพ ยกตัวอย่าง เช่น ข้อมูลผู้ป่วย ประวัติโรค AE ผลทางห้องปฏิบัติการ ผู้รายงาน) โดยรายงานนี้ได้มาจากหน่วยงานเครือข่าย เช่น โรงพยาบาล ร้านยา ผู้ประกอบการ



# 1. แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร (ต่อ)

การดำเนินการ เพื่อรักษาความลับของผู้ป่วยที่ถูกบันทึกในรายงาน AE ที่อยู่ในฐานข้อมูล Thai Vigibase มีดังนี้

HPVC Form – 8

1. เจ้าหน้าที่จากหน่วยงานที่ต้องการส่งรายงาน AE เพื่อเข้าสู่ฐานข้อมูล Thai Vigibase ผ่านระบบ AE Online reporting หรือต้องการเข้าถึงรายงาน AE ต้องดำเนินการ ดังนี้

1.1 สร้างบัญชีผู้ใช้งาน OpenID ที่เว็บไซต์ของสำนักงานรัฐบาล อิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งจะระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

1.2 หน่วยงานต้นสังกัดต้องมีหนังสือส่งรายชื่อผู้ต้องการขอสิทธิเข้าใช้งานระบบ AE Online reporting มาที่ อย โดยแนบเอกสารประกอบตามที่กำหนด เช่น กรณีบริษัทฯ ต้องส่งหนังสือมอบอำนาจจากบริษัท บัตรประชาชนผู้เข้าใช้ระบบ ใบอนุญาตฯ

1.3 เจ้าหน้าที่ HPVC ตรวจสอบเอกสาร และเปิดสิทธิให้เข้าใช้งาน ทั้งนี้ผู้ใช้งานระบบ AE Online reporting มีสิทธิใช้เป็นระยะเวลา 1 ปี อย่างไรก็ตามหน่วยงานต้นสังกัด สามารถทำหนังสือแจ้งยกเลิกรายชื่อเจ้าหน้าที่ที่เข้าถึงข้อมูลหน่วยงานนั้นๆ หรือเจ้าหน้าที่ผู้ใช้ระบบสามารถแจ้งความประสงค์ไม่ต้องการเข้าถึงระบบก่อนครบ 1 ปีได้

แบบคำขอลิขสิทธิ์เพื่อเข้าใช้งานระบบสารสนเทศศูนย์เฝ้าระวังความปลอดภัยด้านผลิตภัณฑ์สุขภาพ  
สำนักงานคณะกรรมการอาหารและยา

<b>ส่วนที่ 1 ประวัติส่วนบุคคลหรือข้อมูลของผู้ขอสิทธิเข้าใช้งานระบบสารสนเทศ</b>		
หมายเลขบัตรประชาชน _____		
คำนำหน้า-ชื่อ-นามสกุล.....		
ตำแหน่ง.....		
อีเมล.....เบอร์โทรศัพท์มือถือ.....		
<b>ส่วนที่ 2 ข้อมูลหน่วยงาน</b>		
ประเภทผู้ประกอบการ ( <input type="checkbox"/> ยานยนต์ <input type="checkbox"/> ยา <input type="checkbox"/> เครื่องมือแพทย์ <input type="checkbox"/> อาหาร <input type="checkbox"/> สมุนไพร <input type="checkbox"/> เครื่องสำอาง)		
ชื่อหน่วยงาน.....		
เลขนิติบุคคลของหน่วยงาน.....		
กลุ่มงาน.....แผนก/ฝ่าย.....		
โทรศัพท์.....โทรสาร.....		
ที่อยู่เลขที่.....หมู่ที่.....ซอย.....ถนน.....ตำบล/แขวง.....		
อำเภอ/เขต.....จังหวัด.....รหัสไปรษณีย์.....		
<b>ส่วนที่ 3 จุดประสงค์การยื่นแบบคำขอลิขสิทธิ์เข้าใช้งานระบบสารสนเทศ</b>		
<input type="checkbox"/> ขอครั้งแรก <input type="checkbox"/> ต่ออายุ <input type="checkbox"/> แก้ไขประเภทสิทธิ <input type="checkbox"/> ยกเลิกสิทธิ		
<b>ส่วนที่ 4 ประเภทสิทธิที่มีความประสงค์ขอสิทธิการใช้งาน</b>		
<input type="checkbox"/> AE Reporting <input type="checkbox"/> AE CEM Program <input type="checkbox"/> AE Search <input type="checkbox"/> AE-Service		
<b>เอกสารแนบ</b>		
1. หนังสือมอบอำนาจให้เป็นผู้รับผิดชอบในการเฝ้าระวังความปลอดภัยด้านผลิตภัณฑ์สุขภาพจากหน่วยงาน (ตัวจริง) พร้อมติดอากรแสตมป์ 30 บาท 2. สำเนาบัตรประชาชนของผู้ขอและผู้ให้มอบอำนาจ อย่างละ 1 ฉบับ 3. สำเนาใบอนุญาตผลิต น้ำหรือสิ่งยา/ใบจดทะเบียนสถานประกอบการผลิตหรือนำเข้าผลิตภัณฑ์สุขภาพ ที่ยังไม่มีหมดอายุ ในปีที่ยื่นเอกสาร 1 ฉบับ <b>หมายเหตุ</b> 1. ผู้ขอสิทธิใช้งานรับทราบประกาศสำนักงานคณะกรรมการอาหารและยา เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และปฏิบัติตามทุกประการ 2. ผู้ขอสิทธิใช้งานจะใช้งานระบบสารสนเทศศูนย์เฝ้าระวังความปลอดภัยด้านผลิตภัณฑ์สุขภาพในกิจการของทางราชการหรือหน่วยงานเท่านั้น 3. จะไม่เปิดเผยข้อมูลที่เป็นความลับทางการค้า และ/หรือ ความลับของทางราชการ 4. สิทธิเข้าใช้งานระบบสารสนเทศฯ มีอายุ 1 ปีนับตั้งแต่วันที่ระบุในหนังสือมอบอำนาจ 5. กรณีต่ออายุให้ยื่นเอกสารใหม่ทั้งหมด		
<b>ผู้ขอใช้</b>	<b>ผู้ตรวจสอบการยื่นคำขอ</b>	<b>ผู้เห็นชอบการยื่นคำขอ</b>
ลงชื่อ.....	ลงชื่อ.....	ลงชื่อ.....
(.....)	(.....)	(.....)
ตำแหน่ง.....	ตำแหน่ง.....	ตำแหน่ง.....
วันที่...../...../.....	วันที่...../...../.....	วันที่...../...../.....

# 1. แนวทางการดำเนินงาน PDPA ในหน่วยงานของท่านเป็นอย่างไร (ต่อ)

การดำเนินการ เพื่อรักษาความลับของผู้ป่วยที่ถูกบันทึกในรายงาน AE ที่อยู่ในฐานข้อมูล Thai Vigibase มีดังนี้

## 2. การเข้าถึงข้อมูล AE ในฐานข้อมูล Thai Vigibase

2.1 ต้องใช้ username และ password ในการใช้งานระบบ AE Online reporting

2.2 เจ้าหน้าที่จากหน่วยงานหนึ่งๆ สามารถดูข้อมูล AE ได้เฉพาะที่หน่วยงานตนเองส่งมา

2.3 หากผู้ใช้งานระบบ AE Online reporting ไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง ระบบ AE Online reporting จะ logout อัตโนมัติ

## 3. การส่งต่อข้อมูลกรณีที่มีการขอข้อมูลจากหน่วยงานอื่นมาที่ อย.

3.1 กรณีภาครัฐ : อย. ไม่ให้ข้อมูลที่ระบุถึงตัวตนผู้ป่วย ชื่อผู้รายงาน ชื่อผู้วินิจฉัย ผู้ประเมินรายงาน หน่วยงานที่ส่งข้อมูล

3.2 กรณีภาคเอกชน : หน่วยงานเอกชน สามารถขอรายงาน AE ที่เกิดจากการใช้ผลิตภัณฑ์ของบริษัทตนเอง ทั้งนี้รายงาน AE จะยังคงไม่มีข้อมูลที่ระบุถึงตัวตนผู้ป่วย ชื่อผู้รายงาน ชื่อผู้วินิจฉัย ผู้ประเมินรายงาน หน่วยงานที่ส่งข้อมูล

## 4. ผู้รายงานมีสิทธิในการบันทึก ส่ง แก้ไข ลบรายงานในฐานข้อมูล Thai Vigibase เฉพาะรายงานที่หน่วยงานตนเองส่งมาเท่านั้น

## 2. แนวทางการป้องกันการโจมตีข้อมูลของหน่วยงานท่านเป็นอย่างไร

ในการป้องกันการโจมตีฐานข้อมูล Thai Vigibase ซึ่งมีการเก็บรายงาน AE ในระบบคลาวด์กลางภาครัฐ (Government Data Center and Cloud service : GDCC) ออย มีการดำเนินการดังนี้

1. ผู้ใช้งานต้องมีการลงทะเบียนและเจ้าหน้าที่ HPVC, ออย. ต้องตรวจสอบ และกำหนดสิทธิในการเข้าใช้งานฐานข้อมูล
2. ผู้ใช้งาน ต้องมี username และ password ในการเข้าใช้งานระบบ AE Online reporting
3. ออย. มีการทบทวนบัญชีและสิทธิผู้ใช้งานทุกปี
4. มีการบันทึกเหตุการณ์ (Log) การเข้าใช้งาน
5. มี Next Generation Firewall (NGFW) ซึ่งเป็น Firewall ที่มีประสิทธิภาพสูง ในการรับมือภัยคุกคามที่ซับซ้อน
6. computer มี anti-virus
7. มีแนวปฏิบัติและผู้รับผิดชอบในการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ รวมถึงการดำเนินการตอบสนองเมื่อตรวจพบภัยคุกคาม เช่น ไวรัส โทรจัน สปายแวร์
8. มีแนวปฏิบัติเมื่อเกิด phishing ที่ webserver
9. ศูนย์สารสนเทศ ถูก internal audit หรือ external audit อย่างน้อยปีละ 1 ครั้ง