สรุปเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหลจากฐานข้อมูลกระทรวงสาธารณสุข ระหว่างเดือนมีนาคม พ.ศ.2566 - มีนาคม พ.ศ.2567

นายแพทย์สุรัคเมธ มหาศิริมงคล

ผู้อำนวยการศูนย์เทคโนโลยีและการสื่อสาร สป.สธ.

วันที่ 25 มีนาคม 2567

ตามที่มีข่าวรายงานเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหลจากฐานข้อมูลกระทรวงสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข (ศทส. สป.สธ.) ได้จัดการประชุมร่วมกับคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) สรุปประเด็นสำคัญได้ 3 ส่วน ได้แก่

1. **ระบบคลังข้อมูลขนาดใหญ่กระทรวงสาธารณสุข**
2. **รายงานเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหล**
3. **มาตรการยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข**

1. คลังข้อมูลขนาดใหญ่ของกระทรวงสาธารณสุข

คลังข้อมูลขนาดใหญ่กระทรวงสาธารณสุข ประกอบไปด้วย **5 ฐานข้อมูล และ 1 ระบบ** โดย Health Data Center (HDC) มีการจัดเก็บข้อมูลที่ฐานข้อมูลของศูนย์เทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข ส่วนอีก 4 ฐานข้อมูล ถูกจัดเก็บอยู่ที่ฐานข้อมูลของบริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ซึ่งได้รับการรับรองมาตรฐาน ISO 27001 และ ISO 27799 (ISO Healthcare) ตามบันทึกข้อตกลงความร่วมมือระหว่างบริษัทอินเทอร์เน็ตฯ และกระทรวงสาธารณสุข โดยมีรายละเอียดดังนี้

คลังข้อมูลขนาดใหญ่	รายละเอียด	การจัดเก็บข้อมูล	เกี่ยวข้องกับนโยบายยกระดับ 30 บาทรักษาทุกที่ฯ	เกี่ยวข้องกับเหตุการณ์ข้อมูลรั่วไหล
Health Data Center (HDC)	คลังข้อมูลสุขภาพ	ศูนย์เทคโนโลยีสารสนเทศ สธ.	⊖	✓ (3 เหตุการณ์)
Immunization Data Center (MOPH IC)	ระบบรองรับการฉีดวัคซีนโควิด-19	สำนักสุภาพดิจิทัล สธ.	⊖	✓ (1 เหตุการณ์)
Digital Disease Surveillance (DDS)	ระบบรายงานเฝ้าระวังโรคติดต่อ	กรมควบคุมโรค สธ.	⊖	⊖
Financial Data Hub (FDH)	ศูนย์กลางข้อมูลด้านการเงิน	กองเศรษฐกิจสุขภาพฯ สธ.	✓	⊖
Personal Health Record (MOPH PHR)	ประวัติสุขภาพอิเล็กทรอนิกส์	สำนักสุขภาพดิจิทัล สธ.	✓	⊖
Application และ Line OA หมอพร้อม	ระบบเชื่อมต่อและเข้าถึงข้อมูลสุขภาพของประชาชน	สำนักสุขภาพดิจิทัล สธ.	✓	⊖

2. สรุปรายงานเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหลจากฐานข้อมูลกระทรวงสาธารณสุข ระหว่างเดือนมีนาคม พ.ศ. 2566 – เดือนมีนาคม พ.ศ. ๒๕๖๗

ช่วงเวลาเกิดเหตุการณ์	ข่าวที่ปรากฏ	ฐานข้อมูลกระทรวงสาธารณสุขที่เกี่ยวข้อง	ข้อเท็จจริงจากการสืบสวนจากการตรวจสอบของ สกมช. และสำนักงานตำรวจแห่งชาติ
มีนาคม 2566	 9near ประกาศขายข้อมูลส่วนบุคคลไทย 55 ล้านชุดข้อมูล	MOPH - IC	- ไม่มีพยานหลักฐานว่ามาจากระบบหมอพร้อมหรือ MOPH-IC - สธ. ได้ดำเนินการรักษาความปลอดภัยตามมาตรฐานและแก้ปัญหาได้อย่างเหมาะสม
พฤศจิกายน 2566	FantomeJ3 ประกาศขายข้อมูล Thailand HDC 7 ล้านรายชื่อ (ไม่เป็นข่าว ทราบจากทำงานร่วมกับ สกมช.)	HDC	- ตรวจพบการเข้าถึงข้อมูล HDC - ศูนย์เทคโนโลยีฯ สธ. ดำเนินการปิดระบบและติดตั้ง Network Sensor - ดำเนินการตามกฎหมาย

2. สรุปรายงานเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหลจากฐานข้อมูลกระทรวงสาธารณสุข ระหว่างเดือนมีนาคม พ.ศ. 2566 – เดือนมีนาคม พ.ศ. ๒๕๖๗ (ต่อ)

ช่วงเวลาเกิดเหตุการณ์	ข่าวที่ปรากฏ		ฐานข้อมูลกระทรวงสาธารณสุขที่เกี่ยวข้อง	ข้อเท็จจริงจากการสืบสวนจากการตรวจสอบของ สกมช. และสำนักงานตำรวจแห่งชาติ
มีนาคม 2567		Infamous ประกาศขายข้อมูล 2.2 ล้านรายชื่อ	HDC	- ไม่พบข้อมูลที่เกี่ยวข้องกับด้านการแพทย์และสาธารณสุข - ไม่ตรงกับรูปแบบการเก็บข้อมูลของ HDC สธ. - ดำเนินการตามกฎหมาย
มีนาคม 2567		Infamous ประกาศขายข้อมูล รอบที่ 2	HDC	- พบข้อมูลรั่วไหล 39 รายการ ลักษณะเดียวกันกับที่สอบสวนเมื่อเดือนพฤศจิกายน พ.ศ. 2566 - ไม่ตรงกับรูปแบบการเก็บข้อมูลของHDC สธ. และหมอพร้อม (MOPH-IC) - ดำเนินการตามกฎหมาย

3. มาตรการดำเนินงานยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข

เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ตามนโยบายยกระดับ 30 บาทรักษาทุกที่ฯ กระทรวงสาธารณสุข โดยปลัดกระทรวงสาธารณสุข ได้ประชุมสั่งการผู้ตรวจราชการ โดยได้ออกมาตรการสำคัญดังต่อไปนี้

1. ตั้งคณะกรรมการสอบสวนข้อเท็จจริง โดยมีองค์ประกอบได้แก่ ศทส.สป.สธ, สกมช. และสำนักงานตำรวจแห่งชาติ เพื่อลงเก็บข้อมูลเพิ่มเติม จากทั้ง 2 กรณี

2. ยกระดับระบบความปลอดภัยของ Health Data Center และปรับสิทธิในการเข้าถึงข้อมูลโดยใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Multi-factor Authentication) ในหน่วยงานระดับจังหวัดทุกแห่งทั่วประเทศ

3. ห้ามทุกหน่วยงานสำเนาข้อมูล (Duplicate) จากฐานข้อมูลกลาง โดยไม่ได้รับอนุญาต และต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

4. สั่งการให้ทุกหน่วยงานวางมาตรการ กำกับติดตาม ดูแลความปลอดภัยไซเบอร์ ให้เป็นไปตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

3. มาตรการดำเนินงานยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข (ต่อ)

5 ให้ทุกหน่วยงานปรับระบบการทำงานที่ผ่าน Website ภายใน 31 พฤษภาคม พ.ศ. 2567 ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และการรักษาความมั่นคงปลอดภัยไซเบอร์

6 สั่งการให้ทุกหน่วยงานระงับการเชื่อมต่อข้อมูล (Health Information Exchange) กับหน่วยงานภายนอกที่ไม่ผ่านกระบวนการธรรมาภิบาลของกระทรวงสาธารณสุขทันที

7 ดำเนินคดีตามกฎหมายกับผู้ที่กระทำความผิดต่อไป

Healthcare Accreditation Information Technology : HAIT+

แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับโรงพยาบาลของรัฐ พ.ศ. 2567

แนวทางการดำเนินงาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับโรงพยาบาลของรัฐ

พ.ศ. 2567

นพ.วรรษา เปาอินทร์
นายกสมาคม เวชสารสนเทศไทย

พลอากาศตรี จเด็ด คูหะก้องกิจ
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ภาพ: Facebook "School of Hospital Management"
,สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ(สกมช.)

Healthcare Accreditation Information Technology : HAIT+

การนำ HAIT +มาใช้ร่วมกับการรับรอง HAIT

1. เริ่มใช้ ปีงบประมาณ 2567
2. ทำ HAIT ระดับ 1 หรือ 2 หรือ 3 เหมือนเดิม
3. เสริมด้วยกิจกรรม ใน ฉบับ HAIT +
4. ได้การรับรองคุณภาพเป็นระดับ 1+ หรือ 2+ หรือ 3+

สิ่งที่ไม่มีใน HAIT เดิม แต่มีในฉบับ HAIT +

1. การทดสอบการเจาะระบบ (Penetration Test)
2. การเฝ้าระวังภัยไซเบอร์ การกำหนดมาตรการเผชิญเหตุ ซ้อมแผนรับมือ และแก้ไขเมื่อเกิด ภัยไซเบอร์
3. การจัดทำรายงาน และส่งรายงานให้กับศูนย์ THAI Cert ทั้งกรณีปกติ และ กรณีเกิดภัยไซเบอร์

การพัฒนาคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล ที่สำคัญ : HAIT

Information Security Management

Datacenter

- ระบบล็อคประตูและการควบคุมติดตามการเข้า
- ระบบปรับอากาศที่ทำให้อุณหภูมิคงที่
- เซ็นเซอร์ตรวจวัดอุณหภูมิ และระบบแจ้งเตือน
- ระบบตรวจจับควัน และระบบแจ้งเตือนอัคคีภัย
- เครื่องดับเพลิงที่ใช้ดับเพลิงจากระบบคอมพิวเตอร์โดยเฉพาะ
- การจัดระเบียบของอุปกรณ์และสายสัญญาณ
- ระบบ Monitor (Availability & Capacity) ถูกลิขสิทธิ์
- ระบบสำรองข้อมูลแบบ online และ offline ของ server **
- ระบบ firewall & ระบบ Log **
- การ Update Patch OS & Software Server ถูกลิขสิทธิ์
- ระบบสำรองไฟห้อง Datacenter

Shall จำเป็น

Capacity Management and Change Management

- OS & Software ที่ถูกลิขสิทธิ์ **
- Antivirus ที่ถูกลิขสิทธิ์ **

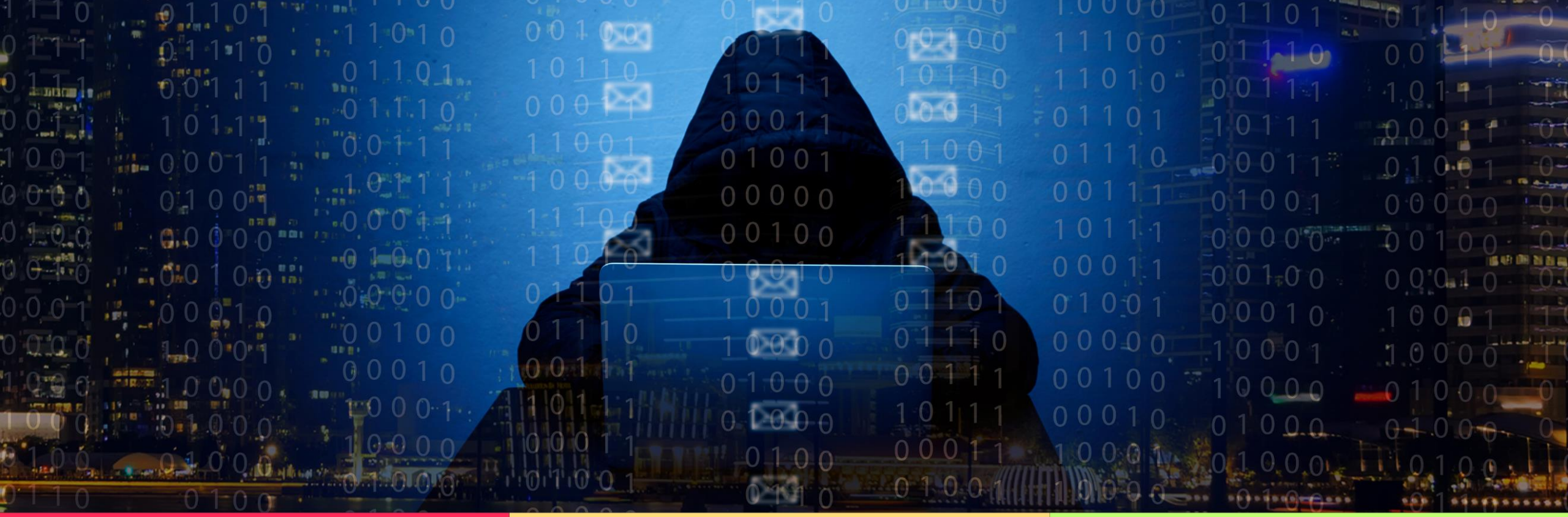
Should แนะนำ
เสนอวางแผน

** หนังสือสั่งการจาก สธ

ผลการสำรวจ

Cyber Security

ระดับความเสี่ยง	รายละเอียด
สูง	**Backup** : มีการสำรองข้อมูลอย่างน้อย 1 วันย้อนหลังได้ 7 วันเป็นอย่างน้อย
	Antivirus : มีการติดตั้ง Antivirus Software และ Signature ทุกวัน
	Access Control : มีอุปกรณ์ Security Physical หรือ Virtual ในการควบคุม Policy การเข้าถึงระบบทั้งทาง Public และ Private โดยไม่มีการเปลี่ยน Password ที่มีความเสี่ยงผ่านทาง Public
	Privileged Access : 1. มีการ Disable Administrator / Root / Admin บนระบบเพื่อป้องกันการโจมตีในรูปแบบ Brute Force
	Privileged Access : 2. มี Policy การเปลี่ยน Password อย่างน้อยทุก 3 เดือน
	Privileged Access : 3. มีการกำหนดสิทธิ์ในการเข้าระบบในระดับAdmin และ User
	Privileged Access : 4. มีการตั้ง Password ให้ Complex ตามมาตรฐาน
ปานกลาง	**Business Continuity Plan (BCP)** : มีการซ้อมแผนเพื่อช่วยเตรียมการรับมือเมื่อเกิดเหตุการณ์ที่ไม่ปกติที่อาจจะเกิดขึ้นกับระบบ
	Disaster Recovery site (DR) : มีระบบ Disaster Recovery site (DR)
	OS patching : มีการ Update Security Patching ในระดับ Operating System ทั้ง Windows / Linux ทุกๆ 3 เดือนหรือทันทีหากมี critical security patching
	Multi-Factor Authentication (2FA) : มีการใช้งานระบบ Multi-Factor Authentication (2FA)
	Web Application Firewall (WAF) : มีระบบ Web Application Firewall (WAF) กรณีที่ระบบเป็น Web Application
	Log Management : มีระบบการจัดเก็บ Log อินเตอร์เน็ตและคอมพิวเตอร์ ตาม พ.ร.บ.ฯ อย่างน้อย 90 วัน
	Security Information & Event Management (SIEM) : มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการ
	Vulnerability Assessment (VA Scan) : มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบช่องโหว่ในระดับ OS และ Service ที่ติดตั้ง
ต่ำ	**Software Update** : มีการ Update ให้เป็น Version ล่าสุดเพื่อเป็นการปิดช่องโหว่ที่เกิดขึ้นใน Version ก่อนหน้า
	Penetration Testing : มีการ Pentest อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบช่องโหว่ในระดับ Code ของโปรแกรมที่ใช้งาน



เสี่ยงสูง	เสี่ยงปานกลาง	เสี่ยงต่ำ
ภายใน 2 wks	ภายใน 4 wks	ภายใน 8 wks
46 แห่ง 71.88%	18 แห่ง 28.12%	

จังหวัด	ระดับความเสี่ยง	แห่ง	โรงพยาบาล
อุบลราชธานี	สูง	19	รพ.ทุ่งศรีอุดม,รพ.พิบูลมังสาหาร,รพ.เขมราฐ,รพ.นาเยีย,รพ.ตระการพืชผล,รพศ.สรรพสิทธิประสงค์,รพ.กุดข้าวปุ้น,รพ.น้ำยืน,รพ.โขงเจียม,รพ.ตาลสุม,รพ.สิรินธร,รพ.ม่วงสามสิบ,รพท.วารินชำราบ,รพ.เขื่องใน,รพ.เหล่าเสือโก้ก,รพ.บุณฑริก,รพ.นาตาล,รพ.น้ำขุ่น,รพ.ดอนมดแดง
	กลาง	8	รพ.สว่างวีระวงศ์,รพ.สำโรง,รพ.ศรีเมืองใหม่,รพท.เดชอุดม,รพท. 50 พรรษา มหาวชิราลงกรณ,รพ.โพธิ์ไทร,รพ.นาจะหลวย
	ต่ำ		
มุกดาหาร	สูง	6	รพ.ดงหลวง,รพ.ดงหลวง,รพ.ดอนตาล,รพ.นำคมคำสร้อย,รพ.คำชะอี,รพ.หว้านใหญ่
	กลาง	1	รพท.มุกดาหาร
	ต่ำ		
อำนาจเจริญ	สูง		
	กลาง	7	รพท.อำนาจเจริญ,รพ.ชานุมาน,รพ.ปทุมราชวงศา,รพ.พนา,รพ.เสนางคนิคม,รพ.หัวตะพาน,รพ.ลืออำนาจ
	ต่ำ		
ยโสธร	สูง	6	รพ.ทรายมูล,รพ.มหาชนะชัย,รพ.ค้อวัง,รพ.ไทยเจริญ,รพ.ป่าติ้ว,รพร.เลิงนกทา
	กลาง	3	รพท.ยโสธร,รพ.คำเขื่อนแก้ว,รพ.กุดชุม
	ต่ำ		
ศรีสะเกษ	สูง	15	รพ.บึงบูรพ์,รพ.วังหิน,รพ.ยางชุมน้อย,รพ.ขุนหาญ,รพ.ไพรบึง,รพ.โพธิ์ศรีสุวรรณ,รพ.เมืองจันทร์,รพท.กันทรลักษ์,รพ.โนนคูณ,รพศ.ศรีสะเกษ,รพ.ปรางค์กู่,รพ.ราษีไศล,รพ.ห้วยทับทัน,รพ.ศรีรัตนะ,รพ.กันทรารมย์
	กลาง	6	รพ.ศิลาลาด,รพ.ขุขันธ์,รพ.พยุห์,รพ.น้ำเกลี้ยง,รพ.ภูสิงห์,รพ.เบญจลักษณ์ เฉลิมพระเกียรติฯ
	ต่ำ		
			* รพ.อุทุมพรพิสัย ประเมินไม่พบความเสี่ยง

Cyber Security Concept

เก็บ

- มาตรฐาน Data Center
- Back Up 3-2-1-1-0 Principle (3 Copies,2 Differnce type , 1 Copy Off line , 1 copies at an offsite location , 0 verified backup without errors)

กัน

- Web Server แยกจากฐานข้อมูล
- Software ลิขสิทธิ์ / Update / MA
- Penetration Test ปรับจุดที่เป็นปัญหาตามข้อแนะนำ
- ประเมินความเสี่ยงตาม Standard Check List
- HAIT

กู้

- Restore
- Recovery
- ขอความช่วยเหลือจากผู้เชี่ยวชาญ

ที่ อบ ๐๐๓๓.๐๐๒/ว ๓๖๕๔

สำนักงานสาธารณสุขจังหวัดอุบลราชธานี
ถนนพรหมเทพ อบ ๓๔๐๐๐

๒๗ มีนาคม ๒๕๖๗

เรื่อง ข้อสั่งการมาตรการยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข

เรียน ผู้อำนวยการโรงพยาบาลศูนย์, ผู้อำนวยการโรงพยาบาลทั่วไป, ผู้อำนวยการโรงพยาบาลชุมชน ทุกแห่ง และสาธารณสุขอำเภอทุกอำเภอ

ตามที่มีข่าวรายงานเหตุสงสัยข้อมูลส่วนบุคคลรั่วไหลจากฐานข้อมูลกระทรวงสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ได้จัดประชุมยกระดับความมั่นคงปลอดภัยไซเบอร์ร่วมกับคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กสมช.) เพื่อให้เป็นตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้มีการกำหนดมาตรการยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข นั้น

ในการนี้ สำนักงานสาธารณสุขจังหวัดอุบลราชธานี เห็นควรให้หน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดอุบลราชธานีทุกแห่ง ดำเนินการตามมาตรการยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข ดังนี้

๑. ยกระดับระบบความปลอดภัยของ Health Data Center และปรับสิทธิในการเข้าถึงข้อมูลโดยใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Multifactor Authentications) ในหน่วยงานระดับจังหวัด

๒. ห้ามทุกหน่วยงานสำเนาข้อมูล (Duplicate) จากฐานข้อมูลกลาง โดยไม่ได้รับอนุญาตและต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยความคุ้มครองข้อมูลส่วนบุคคล (PDPA)

๓. ให้ทุกหน่วยงานวางมาตรการ กำกับติดตาม ดูแลระบบความปลอดภัยไซเบอร์ให้เป็นไปตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ให้ทุกหน่วยงานปรับระบบการทำงานผ่าน Website ของทุกหน่วยบริการภายในวันที่ ๓๑ พฤษภาคม ๒๕๖๗ ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และการรักษาความมั่นคงปลอดภัยไซเบอร์

๕. ให้ทุกหน่วยงานระงับการเชื่อมต่อข้อมูล (Health Information Exchange) กับหน่วยงานภายนอกที่ไม่ผ่านกระบวนการธรรมาภิบาลข้อมูลของกระทรวงสาธารณสุข

จึงเรียนมาเพื่อทราบ และดำเนินการตามมาตรการอย่างเคร่งครัดต่อไป

ขอแสดงความนับถือ

(นายภิรักษ์ รุ่งพัฒนาชัยกุล)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)
ปฏิบัติราชการแทนนายแพทย์สาธารณสุขจังหวัดอุบลราชธานี

กลุ่มพัฒนายุทธศาสตร์สาธารณสุข
โทร.๐ ๔๕-๒๔๓๓๐๑ ต่อ ๑๑๑
ผู้ประสานงาน นางหรรษา ชื่นชูผล โทรศัพท์ ๐๘๙-๘๔๕-๒๒๕๕
นายธนสิทธิ์ สนั่นเมือง โทรศัพท์ ๐๙๖-๓๙๕-๓๕๙๙

๑. ยกระดับระบบความปลอดภัยของ Health Data Center และปรับสิทธิในการเข้าถึงข้อมูลโดยใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Multifactor Authentications) ในหน่วยงานระดับจังหวัด

๒. ห้ามทุกหน่วยงานสำเนาข้อมูล (Duplicate) จากฐานข้อมูลกลาง โดยไม่ได้รับอนุญาตและต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยความคุ้มครองข้อมูลส่วนบุคคล (PDPA)

๓. ให้ทุกหน่วยงานวางมาตรการ กำกับติดตาม ดูแลระบบความปลอดภัยไซเบอร์ให้เป็นไปตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ให้ทุกหน่วยงานปรับระบบการทำงานผ่าน Website ของทุกหน่วยบริการภายในวันที่ ๓๑ พฤษภาคม ๒๕๖๗ ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และการรักษาความมั่นคงปลอดภัยไซเบอร์

๕. ให้ทุกหน่วยงานระงับการเชื่อมต่อข้อมูล (Health Information Exchange) กับหน่วยงานภายนอกที่ไม่ผ่านกระบวนการธรรมาภิบาลข้อมูลของกระทรวงสาธารณสุข

CYBER SAFETY