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

Thank You