A survey of literature and case studies to summarize factors in selecting a cloud service provider for healthcare organizations in Thailand

Songsak Rongviriyapanich

Computer science department, Thammasat university

Abstract

Cloud has gained interest in being used in building information systems for healthcare agencies around the world, including Thailand. However, the transition to the cloud requires consideration of many factors including security and organizational readiness. In order to make the information system of public health agencies in the cloud secure and safe in accordance with the laws of Thailand. This paper explores the literature related to cloud safety standards and cloud use for public health agencies in order to summarize recommendations for cloud adoption approaches for public health agencies in Thailand.

Keywords: Cloud for healthcare, Selection criteria for cloud provider, Cloud standards

Revised: 10 May 2022, Revise: 25 July 2022, Accepted: 30 September 2022

Correspondence: Songsak Rongviriyapanich, Computer science department, Thammasat university, 99 Moo 18 Khlong Nueng, Khlong Luang District, Pathum Thani 12120, E-mail: songsak_r@sci.tu.ac.th

การสกัดข้อมูลผู้ป่วยด้วยเทคนิคตัวช่วยแปลงไฟล์เอกสาร

ทรงศักดิ์ รองวิริยะพานิช
สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

บทคัดย่อ
คลาวด์ได้รับความสนใจในการนำมาใช้ในการสร้างระบบสารสนเทศสำหรับหน่วยงานด้านสาธารณสุขทั่วโลกรวมทั้งประเทศไทย หากแต่การปรับเปลี่ยนไปใช้คลาวด์จำเป็นต้องพิจารณาปัจจัยหลายด้านทั้งด้านความปลอดภัยและความพร้อมของหน่วยงาน เพื่อให้ระบบสารสนเทศของหน่วยงานสาธารณสุขบนคลาวด์มีความมั่นคงปลอดภัยเป็นไปตามกฎหมายของประเทศไทย บทความนี้เป็นการสำรวจศึกษาวรรณกรรมที่เกี่ยวข้องกับการใช้คลาวด์สำหรับหน่วยงานด้านสาธารณสุขเพื่อนำสรุปแนะนำแนวทางการปรับเปลี่ยนไปใช้คลาวด์ให้เหมาะสมกับหน่วยงานสาธารณสุขในประเทศไทย

คำสำคัญ: *คลาวด์สำหรับงานสาธารณสุข ปัจจัยการเลือกผู้ให้บริการคลาวด์ มาตรฐานคลาวด์*

วันที่รับต้นฉบับ: 10 พฤษภาคม 2565, วันที่แก้ไข: 25 กรกฎาคม 2565, วันที่ตอบรับ: 30 กันยายน 2565

บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

คลาวด์คือทรัพยากรคอมพิวเตอร์ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ ระบบเครือข่าย แพลตฟอร์มสำหรับการประมวลผล หรือแอพพลิเคชั่นที่ผู้ใช้งานสามารถเข้าถึงบริการได้ผ่านอินเทอร์เน็ต โดยผู้ให้บริการคลาวด์จะจัดหาทรัพยากรไว้และสามารถจัดสรรให้ผู้รับบริการได้ตามความต้องการโดยคิดค่าใช้บริการตามการใช้งานจริง ผู้ใช้บริการคลาวด์สามารถขยายปริมาณทรัพยากรที่จะใช้ได้อย่าง สะดวก รวดเร็ว ง่ายดายทำได้ด้วยตนเอง ทรัพยากรจะมีการแบ่งปันกันใช้ระหว่างผู้ใช้บริกา ประเภทบริการคลาวด์ครอบคลุมตั้งแต่การเช่าใช้โครงสร้างพื้นฐาน Infrastructure as a Service (IaaS), การเช่าใช้แพลตฟอร์ม Platform as a Service (PaaS), การเช่าใช้ซอฟต์แวร์Software as a Service (SaaS), การเช่าบริการสำรองและกู้คืนข้อมูล Backup and Disaster Recovery-as-a-service (DRaaS) ซึ่งเป็นบริการสำรองข้อมูลไว้ในสถานที่ปลอดภัยเพื่อสามารถกู้คืนข้อมูลได้หากเกิดภัยธรรมชาติหรือเหตุโจรกรรมข้อมูล นอกจากนั้นคลาวด์ยังแบ่งออกเป็น 3 ประเภทตามระดับการแบ่งปันทรัพยากรระหว่างผู้ใช้บริการ คือ 1. Public cloud คือ บริการคลาวด์ที่มีการใช้ร่วมกันระหว่างผู้ใช้บริการ โดยผู้ให้บริการคลาวด์เป็นผู้จัดสรรและดูแลจัดการทรัพยากร 2. Private Cloud คือ บริการที่จัดสรรให้เฉพาะผู้ให้บริการรายเดียวใช้งานไม่ใช้ร่วมกับผู้อื่น ผู้ให้บริการคลาวด์เป็นผู้จัดสรรดูแลจัดการทรัพยากร 3. Hybrid cloud คือการใช้บริการคลาวด์แบบผสม มีบางบริการที่ใช้แบบ Public cloud บางบริการเป็นแบบ Private Cloud และบางบริการเป็นบริการที่ใช้ทรัพยากรที่ผู้ใช้บริการจัดสรรเอง (On premise data center)

จากคุณสมบัติของบริการคลาวด์ดังที่กล่าวข้างต้น ทำให้องค์กรด้านสาธารณสุขมีความสนใจที่จะเปลี่ยนมาใช้คลาวด์ จากผลการสำรวจการเปลี่ยนมาใช้คลาวด์ขององค์กรผู้ให้บริการด้านสุขภาพปี 2014 (CCA survey 2014 in healthcare provider establishments) [1] รายงานปริมาณการใช้งานคลาวด์สูงถึง 83% ของผู้ตอบ และเป็นการใช้ในรูปแบบ SaaS 66.9% มากสุดใน 3 ประเภทการให้บริการคลาวด์ ซึ่งแสดงให้เห็นถึงการยอมรับการใช้งานคลาวด์ในงานด้านสาธารณสุข นอกจากนั้นจากผลการสำรวจของ HIMSS Media [2] ในปี 2017 มีบุคลากรด้านสาธารณสุข 45% ได้เปลี่ยนไปใช้คลาวด์แล้ว โดยบริการคลาวด์ 3 อันดับแรกที่องค์การด้านสาธารณสุขเปลี่ยนไปใช้คือ 1. อีเมล์ 2. การใช้ซอฟต์แวร์เวชระเบียนอิเล็กทรอนิกส์ หรือ EMR (Electronic Medical Record) และการใช้ซอฟต์แวร์จัดการบันทึกสุขภาพอิเล็กทรอนิกส์ หรือ HER (Electronic Health Record) บน Hybrid cloud 3. บริการ

ผู้ประสานงาน: ทรงศักดิ์ รองวิริยะพานิช, สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ 99 หมู่ 18 อ.คลองหลวง จ.ปทุมธานี 12120
E-mail: songsak_r@sci.tu.ac.th

แฟกซ์ นอกจากข้อดีของคลาวด์ในเรื่อง 1. ความสามารถในการขยายศักยภาพในการให้บริการ เมื่อปริมาณข้อมูล หรือ จำนวนผู้ใช้งานมากขึ้น (Scalability) 2. การประหยัดงบประมาณในการจัดหา Infrastructure ที่จำเป็นสำหรับการทำงานของหน่วยงานด้านสาธารณสุขจากการใช้ Public cloud เทียบกับการจัดหาทรัพยากรคอมพิวเตอร์และบุคลากรผู้ดูแลระบบสำหรับศูนย์คอมพิวเตอร์ (On Premise Data Center) 3. ความสามารถในการเพิ่มประสิทธิภาพการให้บริการที่ดีขึ้นจากการใช้ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (AI & machine learning) กับข้อมูลด้านสุขภาพ

อย่างไรก็ดี มีองค์กรด้านสาธารณสุขจำนวนไม่น้อยที่ลังเลที่จะเปลี่ยนไปใช้คลาวด์ บทความ [3] ได้อ้างผลการสำรวจของ Bitglass ในปี 2015 ระบุว่า องค์กรด้านสาธารณสุขในสหรัฐอเมริกายังมีความกังวลไม่กล้าที่จะใช้บริการคลาวด์ เนื่องจากสาเหตุที่ 1 เกรงว่าผู้ให้บริการคลาวด์ยังไม่เข้าใจมาตรฐานด้านความปลอดภัยสำหรับข้อมูลสุขภาพที่ประเทศอเมริกามีการกำหนดขึ้นเป็นกฎหมาย HIPAA (The US Health Insurance Portability and Accountability Act of 1996) หรือไม่แน่ใจว่าคลาวด์ของผู้ให้บริการอาจจะยังไม่สามารถให้บริการให้สอดคล้องตามกฎหมาย HIPAA สาเหตุที่ 2 การขาดความสามารถในการควบคุมทรัพยากรคลาวด์ที่ใช้ (Controllability) ที่ผู้ใช้บริการ SaaS มีไม่เต็มที่ เช่น การจัดเก็บข้อมูลโดย SaaS ไม่ได้อยู่ในการควบคุมของผู้ใช้บริการ SaaS ซึ่งอาจนำไปสู่การไม่สามารถการันตีคุณสมบัติการรักษาความลับความส่วนตัวของข้อมูลสุขภาพของผู้ป่วยได้ การให้บริการประเภท SaaS บน Public cloud ผู้ให้บริการคลาวด์จะทำการจัดสรรซอฟต์แวร์ และฐานข้อมูล 1 ชุด ให้ผู้ใช้บริการหลายคนใช้งานร่วมกัน แต่ผู้ใช้บริการแต่ละรายจะไม่สามารถเห็นข้อมูลของผู้ใช้บริการรายอื่น (Multi-tenant cloud architecture) ขณะที่การให้บริการบนคลาวด์แบบ Private cloud ผู้ใช้บริการแต่ละรายจะมีซอฟต์แวร์และฐานข้อมูลแยกกัน ไม่ใช้ร่วมกัน (Single-tenant cloud architecture) โดยหลักการนี้ทำให้ Private cloud มีความปลอดภัยมากกว่า เหมาะสำหรับสาขางานที่ต้องการรักษาความปลอดภัยและความลับความเป็นส่วนตัวของข้อมูล เช่น สาขาการเงินสาขาสาธารณสุข แต่ต้องใช้งบประมาณสูงขึ้น สาเหตุที่ 3 แม้ว่าผู้ใช้บริการคลาวหด์ประเภท PaaS และ IaaS ผู้ใช้บริการจะสามารถควบคุมทรัพยากรได้ด้วยตนเอง แต่หน่วยงานของผู้ใช้บริการ PaaS และ IaaS จำเป็นต้องมีบุคลากรที่มีความเชี่ยวชาญด้าน Cloud เพื่อควบคุมการตั้งค่าระบบให้ป้องกันความปลอดภัยและการเข้าถึงข้อมูลส่วนตัว ซึ่งผู้ใช้บริการคลาวด์จำนวนมากขาดบุคลากรดังกล่าว

คำถามของการสำรวจศึกษาในบทความนี้ คือ

- ปัจจัยใดที่ต้องนำมาพิจารณาสำหรับองค์กรด้านสาธารณสุขก่อนตัดสินใจเปลี่ยนไปใช้คลาวด์

- รูปแบบการใช้คลาวด์แบบใดเป็นการใช้ประโยชน์จากคลาวด์ที่เหมาะสมกับบริบทในประเทศไทยสำหรับองค์กรด้านสาธารณสุข ซึ่งแตกต่างจากต่างประเทศ เช่น กฎหมายที่เกี่ยวข้องกับข้อมูลด้านสุขภาพ ความพร้อมด้านงบประมาณการลงทุน และข้อจำกัดด้านบุคลากรไอทีในหน่วยงานสาธารณสุข

วัตถุประสงค์การสำรวจ

- ศึกษาและสำรวจบทความจากวรรณกรรมทั้งที่เป็นวารสารวิชาการและสื่อออนไลน์ จากนักวิจัยและจากผู้เชี่ยวชาญในองค์กรบริษัทในประเทศไทยและต่างประเทศ โดยศึกษาจากบทเรียนที่ได้กรณีตัวอย่าง จากประสบการณ์การเปลี่ยนไปใช้คลาวด์ขององค์กรด้านสาธารณสุขในต่างประเทศเพื่อสรุปปัจจัยที่ต้องนำมาพิจารณาในการตัดสินใจก่อนการเปลี่ยนไปใช้คลาวด์

- แนะนำรูปแบบการใช้คลาวด์ที่เหมาะสมกับบริบทในประเทศไทยที่มีการกำหนดกฎหมายการคุ้มครองข้อมูลด้านสุขภาพ และมีข้อจำกัดด้านงบประมาณและบุคลากรสายไอทีในองค์กรด้านสาธารณสุขในประเทศไทย

2. การสำรวจวรรณกรรมและกรณีตัวอย่างที่เกี่ยวข้องกับการย้ายไปใช้บริการคลาวด์สำหรับหน่วยงานสาธารณสุข

วรรณกรรมที่นำมาศึกษา สามารถแบ่งได้เป็น 3 กลุ่มคือ

1. กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลด้านสาธารณสุข ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับสาขาสาธารณสุข ซึ่งเป็นหนึ่งในปัจจัยที่องค์กรด้านสาธารณสุขที่จะเปลี่ยนไปใช้คลาวด์ต้องเข้าใจข้อกำหนดต่างๆ เหล่านี้ก่อน เพื่อใช้ประกอบการเลือกผู้ให้บริการคลาวด์ที่มีความพร้อมที่สามารถให้บริการคลาวด์ให้สอดคล้องตามข้อกำหนด

2. บทความจากหน่วยงานด้านมาตรฐานคลาวด์ระดับสากลและจากหน่วยงานด้านไอทีในประเทศไทย ซึ่งจะทำให้เข้าใจมาตรฐานด้านคลาวด์ที่สำคัญ แนวปฏิบัติที่เกี่ยวกับการใช้คลาวด์ ประสบการณ์ บทเรียนที่เรียนรู้จากโครงการเหล่านั้น

3. บทความจากผู้เชี่ยวชาญด้านคลาวด์ในบริษัทเอกชนที่ให้บริการคลาวด์ และบทความวิจัยจากนักวิจัยที่เสนอแนะปัจจัยที่ต้องนำมาพิจารณาในการเปลี่ยนไปใช้คลาวด์ ซึ่งจะนำไปสู่การสรุปหาแนวปฏิบัติที่เหมาะสมสำหรับการใช้คลาวด์สำหรับหน่วยงานด้านสาธารณสุข

2.1 ข้อกำหนดที่เกี่ยวข้องกับระบบสารสนเทศและข้อมูลด้านสุขภาพและสาธารณสุข (Healthcare regulation)

หน่วยงานด้านสาธารณสุขถือเป็นหน่วยงานที่ถือครองข้อมูลที่มีความสำคัญที่ต้องรับการคุ้มครองด้านความปลอดภัย ความเป็นส่วนตัว ซึ่งในประเทศต่างๆมีการประกาศเป็นกฎหมายเพื่อบังคับให้หน่วยงานที่ถือครองข้อมูลสุขภาพต้องปฏิบัติ

รวมถึงการคุ้มครองสิทธิของเจ้าของข้อมูลสุขภาพ เช่น การเปลี่ยนแปลง การยกเลิกการให้ความยินยอม ดังนั้นหากหน่วยงานสาธารณสุขที่ถือครองข้อมูลสุขภาพจะปรับไปใช้คลาวด์ หน่วยงานยังจำเป็นต้องปฏิบัติได้ตามกฎหมายที่แต่ละประเทศกำหนด

ข้อกำหนดกฎหมายที่สำคัญเกี่ยวกับข้อมูลสุขภาพและหน่วยงานสาธารณสุขในต่างประเทศได้แก่ กฎหมาย GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรป และกฎหมาย HIPAA (The US Health Insurance Portability and Accountability Act of 1996) ที่กำหนดข้อบังคับความปลอดภัยข้อมูลและความเป็นส่วนบุคคลของข้อมูลสุขภาพ (data security and privacy requirement) รวมทั้งการกำหนดหน่วยงาน ผู้เกี่ยวข้องที่มีหน้าที่ต้องดำเนินการจัดการ ควบคุมทั้งในด้านกายภาพ นำเทคนิคที่จำเป็นมาใช้ปกป้องคุ้มครองให้ข้อมูลสุขภาพปลอดภัย

สำหรับประเทศไทย กฎหมายที่เกี่ยวข้องกับข้อกำหนดข้อมูลสุขภาพและระบบสารสนเทศหน่วยงานด้านสาธารณสุขมี 4 ฉบับคือ 1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act : PDPA) เป็นกฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลให้การประมวลผลข้อมูลส่วนบุคคลขององค์กรใดใดที่มีการดำเนินการกับข้อมูลส่วนบุคคลของผู้บริโภคต้องชอบด้วยกฎหมาย เพื่อปกป้องบุคคลจากผลร้ายที่อาจเกิดขึ้นจากการจัดการและการประมวลผลข้อมูลส่วนบุคคล [4] เป็นกฎหมายที่เทียบเท่ากับกฎหมาย GDPR 2. พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 เป็นกฎหมายกำหนดข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ไม่สามารถเปิดเผยในประการที่จะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้น 3. พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ ฉบับ พ.ศ. 2544 และฉบับแก้ไข พ.ศ. 2551 4. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ เป็นกฎหมายที่กำหนดว่าธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานสาธารณสุขต้องใช้วิธีการแบบปลอดภัยอย่างเคร่งครัด และกำหนดหน้าที่ให้หน่วยงานต้องคุ้มครองข้อมูลส่วนบุคคล หากหน่วยงานภาครัฐมีการทำธุรกรรมอิเล็กทรอนิกส์

2.2 บทความจากหน่วยงานด้านมาตรฐานคลาวด์ระดับสากล

จากการสำรวจเว็บไซต์ผู้ให้บริการคลาวด์ระดับโลก เช่น IBM [5] และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) [6] ที่เป็นหน่วยงานหลักด้านคลาวด์ของภาครัฐในประเทศไทย พบว่ามาตรฐานด้านคลาวด์สำหรับองค์กรด้านสาธารณสุขที่สำคัญที่ผู้ให้บริการคลาวด์ทุกเจ้าต้องผ่านมาตรฐาน มี 2 มาตรฐาน คือ มาตรฐาน ISO/IEC 27001:2013และ มาตรฐาน CSA-STAR (Cloud Security Alliance-Security Trust Assurance and Risk) มาตรฐาน CSA-STAR เป็นมาตรฐานความปลอดภัยบนระบบคลาวด์เพิ่มเติมมาจากมาตรฐานความปลอดภัยของ ISO 27001 โดยมาตรฐาน CSA-STAR มุ่งเน้นที่ความปลอดภัยของการให้บริการคลาวด์เป็นหลักแต่ครอบคลุมการประเมินการดำเนินการตามข้อกำหนด GDPR ด้วย (GDPR CoC Certification ย่อมาจาก CSA Code of Conduct for GDPR Compliance) [7] ส่วนมาตรฐาน ISO 27001:2013 เป็นการรับรองมาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system) ของผู้ให้บริการคลาวด์ว่าองค์กรผู้ให้บริการคลาวด์มีการบริหารจัดการการทำงานเพื่อทำให้ระบบคลาวด์มีความมั่นคงปลอดภัยด้านสารสนเทศอย่างแท้จริง ครอบคลุมถึงการจัดการให้ระบบสามารถใช้งานได้อย่างต่อเนื่องด้วย (Business Continuity)

มาตรฐานทั้ง 2 มาตรฐานเป็นการส่งเสริม ไม่ซ้ำซ้อน มาตรฐาน CSA STAR มี 3 ระดับ คือ Level 1 อนุญาตให้ผู้ให้บริการคลาว์ประเมินตนเอง (Self-Assessment) Level 2 เป็นการให้องค์กรภายนอกเป็นผู้ประเมิน(Third-Party Certification) Level 3 (Continuous Monitoring) ซึ่งเป็นระดับที่เพิ่มเติมใน Levels 1 และ 2 เพื่อแยกระดับผู้ให้บริการคลาวด์ที่ทำการประเมินอย่างต่อเนื่อง ออกจากผู้ให้บริการคลาวด์ที่ผ่านการประเมินคุณภาพแบบไม่ต่อเนื่อง ผู้ให้บริการที่ผ่านระดับ Level 1 หรือ Level 2 จะถือว่าผ่านข้อกำหนด GDPR ด้วย การผ่าน Level 2 จะมีความน่าเชื่อถือมากกว่า

ความปลอดภัยของข้อมูลถือเป็นเรื่องสำคัญสำหรับองค์กรด้านสาธารณสุขที่จัดเก็บข้อมูลสุขภาพ ผู้ให้บริการคลาวด์ประเภท SaaS สำหรับสาขาสุขภาพจำเป็นต้องดำเนินการให้คลาวด์มีมาตรฐานความปลอดภัยของข้อมูลโดยเฉพาะการเข้าถึงข้อมูล มาตรฐานที่สำคัญ มี 2 มาตรฐานคือ มาตรฐานที่ 1 FHIR (Fast Healthcare Interoperability Resources) [8] ซึ่งเป็นมาตรฐานในการแลกเปลี่ยนข้อมูลสารสนเทศด้านสุขภาพที่กำหนดโดยองค์กร Health Level Seven (HL7) International ที่ใช้กันอย่างแพร่หลายโดยองค์กร HL7 ได้เสนอโมเดลโครงสร้างข้อมูลด้านสุขภาพที่เป็นมาตรฐานสากลสำหรับใช้ในการแลกเปลี่ยนระหว่างระบบสารสนเทศ (Healthcare data exchange and information modeling standards) FHIR เป็นเนื้อหากำหนดเรื่องมาตรฐานด้านความปลอดภัยและด้านการรักษาข้อมูลความลับ (Security and Privacy) กำหนดโครงสร้างข้อมูล แนะนำแนวทางและหลักการสำหรับการอินพลีเม้นท์กลไกการรักษาความปลอดภัย (Implementation Guidance and Principles) เช่น Security Principles, Security Labels, Signatures ซอฟต์แวร์ SaaS ที่ยึดถือ FHIR เป็นมาตรฐานในการพัฒนา จะทำให้สามารถแลกเปลี่ยนข้อมูลสุขภาพระหว่างระบบสารสนเทศได้และมีความปลอดภัยและความเป็นส่วนตัว มาตรฐานที่ 2. มาตรฐาน SOC 2 (Service Organization Control 2) ที่กำหนดโดยสถาบัน AICPA (American Institute of Certified Public Accountants) [9] เป็นมาตรฐานด้านแนว

ปฏิบัติพื้นฐานด้านความปลอดภัยข้อมูลเหมาะสำหรับผู้ให้บริการคลาวด์ประเภท SaaS ที่มีการจัดเก็บ ประมวลผล และแลกเปลี่ยนข้อมูลที่จำเป็นต้องมีคุณสมบัติต่อไปนี้ ได้รับการปกป้องความเป็นส่วนตัว (privacy) เก็บเป็นความลับ (confidentiality) การป้องกันการเข้าถึงข้อมูล มีความปลอดภัยของข้อมูล (security) พร้อมใช้งานของข้อมูล (availability) มีความถูกต้องสมบูรณ์ของการประมวลผลข้อมูล (processing integrity)

จากการสำรวจวรรณกรรม พบว่าซอฟต์แวร์รูปแบบ SaaS บางโปรแกรมจะเน้นการโฆษณาคุณสมบัติผ่านข้อกำหนด HIPAA หรือ HIPAA Compliant เช่น โปรแกรม IQ Web PACS [10] ซึ่งเป็นโปรแกรมสำหรับอ่านภาพถ่ายรังสีให้บริการในรูปแบบ SaaS ที่ได้คุณสมบัติ HIPAA compliant ซึ่ง HIPAA ไม่ใช่ชื่อมาตรฐานด้านคลาวด์ แต่เป็นชื่อกฎหมายของประเทศสหรัฐอเมริกาที่กำหนดข้อบังคับให้หน่วยงานที่จัดเก็บข้อมูลสุขภาพ ดังนั้นการได้คุณสมบัติ HIPAA compliant เป็นการรับประกันว่าซอฟต์แวร์ได้ดำเนินการตามข้อบังคับในกฎหมาย HIPAA เท่านั้น แตกต่างจากมาตรฐาน SOC 2 แม้ว่า SOC 2 จะสามารถเปรียบเทียบหัวข้อกับข้อกำหนด HIPAA ได้ในส่วนมาตรฐานด้านความปลอดภัยข้อมูล แต่ HIPAA มีข้อกำหนดที่มากกว่า และ HIPAA เป็นข้อกำหนดสำหรับหน่วยงานด้านสาธารณสุขของสหรัฐอเมริการต้องปฏิบัติ

ในปัจจุบันเกิดแนวทางการใช้คลาวด์รูปแบบใหม่ที่เรียกว่า Multi-cloud ซึ่งเป็นการใช้บริการจากผู้ให้บริการคลาวด์ประเภทเดียวเช่น public cloud แต่ไม่จำกัดการเช่าใช้จากผู้ให้บริการคลาวด์เพียงเจ้าเดียว แต่ใช้บริการจากผู้ให้บริการหลายเจ้า จากข้อแนะนำของบริษัท Gartner ได้คาดการณ์ว่ารูปแบบการใช้คลาวด์แบบ multi-cloud จะเป็นสัดส่วนถึง 70% ของการใช้งานคลาวด์ทั้งหมด [11] โดยข้อดีของ multi-cloud คือการป้องกันการผูกติดกับผู้ให้บริการรายใดเป็นพิเศษ (Vendor lock-in)

กรณีตัวอย่างของการอินพลีเม้นท์คลาวด์ในงานด้านสาธารณสุข

ในบทความนี้ได้สำรวจโครงการ 3 โครงการ คือ โครงการที่ 1 Health Link ของกระทรวงดิจิทัล [12] ซึ่งเป็นแพลตฟอร์มเชื่อมโยงข้อมูลสุขภาพระหว่างโรงพยาบาลภาคี ทำให้สามารถแลกเปลี่ยนข้อมูลด้านสุขภาพของผู้ป่วยได้ โดยระบบข้อมูลของโรงพยาบาลที่เข้าร่วมโครงการจะมีการจัดเก็บข้อมูลตามมาตรฐาน FHIR ข้อมูลของผู้ป่วยมีการจัดเก็บแยกเป็น 2 ก้อน (De-identified data storage:) ส่วนแรกจะเป็นข้อมูลที่ใช้ระบุตัวตนของผู้ป่วย ส่วนที่ 2 จะเป็นข้อมูลสุขภาพ ระบบจะนำข้อมูลทั้งสองส่วนมาประกอบกันที่ปลายทางเมื่อแพทย์ขอดูข้อมูลได้ผ่านขั้นตอนการตรวจสอบสิทธิ์การเข้า ระบบ Health Link จะถูกติดตั้งบนคลาวด์ของบริษัท กสท โทรคมนาคม จำกัด (มหาชน)ที่ได้มาตรฐาน ISO/IEC 27001 และ ISO/IEC 20000-1 ซึ่งเป็นมาตรฐานว่าด้วยการบริหารงานบริการด้านเทคโนโลยีสารสนเทศ นอกจากนั้นระบบ Health Link จะมีการควบคุมความปลอดภัยของข้อมูลและการรักษาความลับข้อมูลส่วนตัวตามมาตรฐาน FHIR มีการให้ความยินยอมในการเข้าถึงข้อมูลของผู้ป่วยผ่านแอพพลิเคชันเป๋าตังและระบบยืนยันตัวตนของธนาคารกรุงไทย ผลการวิเคราะห์กรณีตัวอย่างนี้พบว่าหลักการ แนวคิดในการพัฒนาคลาวด์แพลตฟอร์มอิงหลักการและมาตรฐานสากลอย่างดีเยี่ยม แต่จากบทความที่นำเสนอโครงการไม่กล่าวถึงมาตรฐานด้านความปลอดภัยของคลาวด์ระดับ IaaS อย่างเช่น CSA-STAR ซึ่งจริงจริงแล้วผู้พัฒนาแพลตฟอร์มควรต้องรับประกันว่ามีความปลอดภัยเทียบเท่ากับระดับสากลสำหรับองค์กรด้านสาธารณสุขที่ใช้คลาวด์

• โครงการที่ 2 G-Cloud ซึ่งเป็นระบบคลาวด์กลางภาครัฐของประเทศไทย (Government Data Center and Cloud service: GDCC) [6] จัดทำโดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) และเป็นผู้ให้บริการ G-Cloud โดยในปี พ.ศ. 2559 G-Cloud ได้ผ่านการรับรองมาตรฐาน CSA STAR ในระดับที่ 2 CSA STAR Certification จากผู้ตรวจสอบภายนอกเป็นที่เรียบร้อย นอกจากนั้นยังได้ผ่านการรับรองมาตรฐาน ISO/IEC 27001:2013 อีกด้วย ผลการวิเคราะห์กรณีนี้ พบว่า G-Cloud ได้รับการพัฒนาให้ผ่านทั้งสองมาตรฐานที่เป็นมาตรฐานสากลด้านคลาวด์ ทำให้หากหน่วยงานด้านสาธารณสุขเลือกใช้บริการ G-Cloud จะสามารถมั่นใจว่า มีแนวทางการปฏิบัติ การให้บริการ การจัดการข้อมูลสำคัญ ที่ได้ประสิทธิภาพและมีความปลอดภัยสูงตามมาตรฐานสากล ทั้งนี้ขึ้นกับการใช้งาน G-Cloud ของหน่วยงานด้านสาธารณสุขว่าใช้งานลักษณะใด หากมีการนำซอฟต์แวร์มาใช้งานบน G-Cloud ความปลอดภัยข้อมูลสุขภาพจะขึ้นกับมาตรฐานของซอฟต์แวร์นั้น

• โครงการที่ 3 โครงการจัดหาระบบจัดเก็บและรับส่งข้อมูลภาพทางการแพทย์ผ่านระบบคลาวด์ (Cloud-Based PACS System) สำนักงานเขตสุขภาพที่ 8 [13] ใช้แนวทางการใช้ SaaS จากผู้ให้บริการคลาวด์ที่การันตีว่าซอฟต์แวร์ผ่านข้อกำหนด HIPAA อย่างเช่น แนวทางการจัดหาโปรแกรม IQ Web PACS ที่เป็นโปรแกรมสำหรับอ่านภาพถ่ายรังสีที่ผ่านข้อกำหนด HIPAA [8] ผลการวิเคราะห์กรณีนี้ นับเป็นแนวทางการใช้คลาวด์ที่เหมาะสม เนื่องจากการใช้บริการคลาวด์แบบ SaaS จะทำให้หน่วยงานได้รับบริการครอบคลุมไปถึง IaaS และ PaaS อัตโนมัติ และการใช้ซอฟต์แวร์ SaaS ที่ได้มาตรฐาน เช่น ผ่านข้อกำหนด HIPAA จะมีความเสี่ยงน้อยกว่าการย้ายซอฟต์แวร์ระบบที่มีอยู่ไปใช้งานบนคลาวด์ แต่จากรายละเอียดโครงการอาจจะขาดการพิจารณาป้องกันปัญหาการผูกติดกับผู้ให้บริการคลาวด์ตลอดไป (Vendor lock-in) อาจทำให้หน่วยงานไม่สามารถเปลี่ยนผู้ให้บริการคลาวด์ได้

2.3 บทความวิจัยที่ศึกษาปัจจัยในการตัดสินใจเปลี่ยนไปใช้บริการคลาวด์

งานวิจัย [14] สำรวจความเห็นของบุคลการทางแพทย์และสายไอทีในประเทศอียิปต์ซึ่งเป็นประเทศกำลังพัฒนาเหมือนไทย ถามเกี่ยวกับปัจจัยที่ใช้พิจารณาในการเปลี่ยนไปใช้คลาวด์ พบ 2 ประเด็นหลักที่ทำให้เกิดความกังวล 1. ความเสี่ยงด้านความปลอดภัย (Security risk) ในระหว่างการรับส่งข้อมูลที่ต้องควบคุมความปลอดภัยระหว่างเครื่องคลาวด์และผู้เข้าใช้ข้อมูล และความกังวลเรื่องการเชื่อมต่อข้อมูลระหว่างระบบต่างๆ ให้มีความปลอดภัยทั้งในระดับ Logical และ Physical กล่าวคือ การควบคุมความปลอดภัยการเข้าถึงข้อมูลเชิงกายภาพคือควบคุมเครื่องที่สามารถเข้าถึงข้อมูลได้ และการควบคุมสิทธิบุคลากรที่สามารถเข้าถึงข้อมูลได้ 2. ความพร้อมด้านงบประมาณและบุคลากรในการย้ายไปใช้คลาวด์สำหรับประทศกำลังพัฒนาที่มีข้อจำกัด (Integration and transition) นอกจากนั้นในบทความได้สรุปว่ารูปแบบการให้บริการคลาวด์แบบ Hybrid และ Private Cloud เหมาะสมสำหรับงานด้านสาธารณสุขมากกว่า เนื่องจากมีความปลอดภัยและการเก็บรักษาข้อมูลส่วนบุคคลที่ดีกว่า

3. สรุปแนวทางการใช้คลาวด์สำหรับหน่วยงานสาธารณสุขในประเทศไทย

จากการศึกษาวรรณกรรม สามารถสรุปปัจจัยสำหรับเลือกผู้ให้บริการคลาวด์สำหรับหน่วยงานสาธารณสุขในประเทศไทยได้ 2 ปัจจัยดังนี้ 1.ปัจจัยด้านความสามารถของผู้ให้บริการคลาวด์ในการให้บริการได้ตามข้อกำหนดทางกฎหมายของประเทศไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลสุขภาพและการจัดการระบบสารสนเทศของหน่วยงานด้านสาธารณสุข ซึ่งวิธีที่ใช้คือการพิจารณาจากมาตรฐานคลาวด์ที่ผู้ให้บริการผ่าน 2.พิจารณาเลือกผู้ให้บริการให้สอดคล้องกับงบประมาณและความพร้อมด้านบุคลากรที่จะดูแลระบบบนคลาวด์ หลังการปรับเปลี่ยนไปใช้คลาวด์ จากปัจจัยทั้งสองด้าน สรุปเป็นแนวทางในการเปลี่ยนไปใช้คลาวด์ดังนี้

แนวทางการเปลี่ยนไปใช้บริการคลาวด์ประเภท IaaS สำหรับองค์กรด้านสาธารณสุข แยกเป็นกรณีดังนี้

- สำหรับองค์กรที่ไม่มีข้อจำกัดด้านงบประมาณ แต่ขาดบุคลากรด้านไอทีที่มีความเชี่ยวชาญด้านความปลอดภัย ควรเลือกใช้คลาวด์ประเภท Private cloud เพื่อความปลอดภัยของระบบ เนื่องจากไม่มีการแบ่งปันทรัพยากรกับผู้ใช้บริการคลาวด์รายอื่น
- หากมีข้อจำกัดด้านงบประมาณ แต่มีบุคลากรด้านไอทีที่มีทักษะในการดูแลระบบ สามารถใช้บริการคลาวด์แบบ Hybrid cloud หรือ Public cloud โดยควรพิจารณาใช้หลักการ multi-cloud ที่เป็นการใช้บริการคลาวด์ IaaS จากผู้ให้บริการหลายรายเพื่อป้องกันปัญหา Vendor lock-in
- เลือกผู้ให้บริการคลาวด์ที่ผ่านทั้งมาตรฐาน ISO/IEC 27001:2013 และมาตรฐาน CSA-STAR ระดับ Level 2 ถ้าเป็นไปได้ หรือ Level 1 เป็นอย่างน้อยซึ่งรวมการผ่านข้อกำหนด GDPR ด้วย เพื่อเป็นการรับประกันว่าผู้ให้บริการคลาวด์มีการบริหารจัดการการทำงานเพื่อทำให้เกิดระบบคลาวด์มีความมั่นคงปลอดภัยด้านสารสนเทศอย่างแท้จริงและให้บริการได้อย่างต่อเนื่อง และรับประกันมาตรฐานความปลอดภัยของคลาวด์ระดับโครงสร้างพื้นฐาน
- เลือกใช้ผู้ให้บริการคลาวด์ภายในประเทศไทยที่ได้รับมาตรฐานตามที่แนะนำ เพื่อความสะดวกในการติดต่อสื่อสารของบุคลากรด้านไอทีที่ดูแลระบบสามารถสอบถาม ขอความช่วยเหลือและการแก้ปัญหาจากทีมงานของผู้ให้บริการคลาวด์เป็นภาษาไทยได้

แนวทางการเปลี่ยนไปใช้บริการคลาวด์ประเภท SaaS สำหรับองค์กรด้านสาธารณสุข แยกเป็นกรณีดังนี้

- เลือกใช้ซอฟต์แวร์จากผู้ให้บริการที่ได้รับการรับรองมาตรฐาน SOC 2 เป็นอย่างน้อย หรือ เป็นซอฟต์แวร์ที่พัฒนาส่วนการแลกเปลี่ยนข้อมูลตามข้อแนะนำ FHIR ตามมาตรฐาน HL7 หรือที่ได้รับการยืนยันว่าเป็นไปตามข้อกำหนดตามกฎหมาย HIPAA

4. บทสรุป

คลาวด์เป็นแนวทางจัดหาทรัพยากรคอมพิวเตอร์ทั้งระดับโครงสร้างพื้นฐาน แพลตฟอร์มและซอฟต์แวร์ ที่มีข้อดีทำให้หน่วยงานด้านสาธารณสุขมีความสนใจที่จะปรับไปใช้คลาวด์ แต่มีข้อกังวลหลายด้านโดยเฉพาะด้านความปลอดภัย การป้องกันความเป็นส่วนตัวของข้อมูลสุขภาพของผู้ป่วย จากผลการศึกษาสำรวจ มาตรฐานคลาวด์ในระดับสากลและจากกรณีตัวอย่างการอิมพลีเม้นต์คลาวด์ในประเทศไทยทำให้สามารถสรุปมาตรฐานคลาวด์สำหรับบริการ IaaS และSaaS ที่ผู้ให้บริการคลาวด์ต้องมีเพื่อให้หน่วยงานสาธารณสุขของประเทศไทยผ่านข้อกำหนดด้านกฎหมายของประเทศไทยหากปรับไปใช้คลาวด์ นอกจากนั้นบทความได้สรุปแนะนำแนวทางการเปลี่ยนไปใช้คลาวด์ประเภท IaaS และการใช้ SaaS สำหรับหน่วยงานสาธารณสุขของประเทศไทยโดยพิจารณาปัจจัยด้านความพร้อมด้านงบประมาณและบุคลากรด้านไอทีของหน่วยงาน

เอกสารอ้างอิง

[1] HIMSS Analytics, Forbes, 83% Of Healthcare Organizations Are Using Cloud-Based Apps Today. [Online] Available from: https://www.forbes.com/sites/louiscolumbus/2014/07/17/83-of-healthcare-organizations-are-using-cloud-based-apps-today/ [accessed 30 September 2021]

[2] Cloud Computing Survey, HIMSS Media, November 2017

[3] Understanding HIPAA-Compliant Cloud Options for Health IT. [Online] Available from: https://hitinfrastructure.com/features/understanding-hipaa-compliant-cloud-options-for-health-it [accessed 30 September 2021].

[4] ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจารูญลาภ, ชวิน อุ่นภทัร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, “Thailand Data Protection Guidelines 2.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล”, ISBN 978-616-407-458-3, พิมพ์ครั้งที่ 1 ตุลาคม 2562.

[5] Cloud solutions for healthcare and life sciences. [Online] Available from: https://www.ibm.com/cloud/healthcare [accessed 30 September 2021]

[6] Government Cloud ได้รับรางวัล CSA STAR Certification จาก Cloud Security Alliance. [Online] Available from: https://www.dga.or.th/document-sharing/article/35977/ [accessed 30 September 2021]

[7] Cloud Security Alliance Code of Conduct for GDPR Compliance (Updated - September 2020). [Online] Available from: https://cloudsecurityalliance.org/artifacts/cloud-security-alliance-code-of-conduct-for-gdpr-compliance/ [accessed 30 September 2021]

[8] HL7FHIR. Release 4. [Online] Available from: https://www.hl7.org/fhir/overview.html [accessed 30 September 2021]

[9] Soc 2 (Service Organization Control 2). [Online] Available from: https://searchcloudsecurity.techtarget.com/definition/Soc-2-Service-Organization-Control-2 [accessed 30 September 2021]

[10] [Online] Available from: https://image-systems.biz/fileadmin/user_upload/iQ-WEB_6.7.3_Brochure_150dpi_PUB_INT_EN_-_001TR.pdf [accessed 30 September 2021]

[11] Gartner. “The Future of the Data Center in the Cloud Era.” June 2015, refreshed September 2016.

[12] Health Link: แพลตฟอร์มเชื่อมโยงข้อมูลสุขภาพของไทย. [Online] Available from: https://bigdata.go.th/showroom/health-link/ [accessed 30 September 2021]

[13] โครงการจัดหาระบบจัดเก็บและรับส่งข้อมูลภาพทางการแพทย์ผ่านระบบคลาวด์ (Cloud -Based PACS System สำนักงานเขตสุขภาพที่ 8 [Online] Available from: https://r8way.moph.go.th/r8wayadmin/page/uploads_file/20200319125608_%E0%B8%A7%E0%B8%B2%E0%B8%A3%E0%B8%B0%E0%B8%97%E0%B8%B5%E0%B9%88%203.2%20Cloud-Based%20PACS%20R8%20-19%20Mar%202020%20-edit.pdf [accessed 30 September 2021]

[14] Nermeen Mekawiea, Kesmat Yehia, "Challenges of Deploying Cloud Computing in eHealth", Procedia Computer Science 181 (2021), pp. 1049–1057