การจัดประชุมเสนอผลงานวิจัยระดับบัณฑิตศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 5

The 5th STOU Graduate Research Conference

การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส

Privacy Security Framework Design for Electronic Medical Records Using Web Services in Narathiwat Province

จรูญศักดิ์ เวทมาหะ (Jaroonsak Watmaha)[1] ณัฐพร เห็นเจริญเลิศ (Nuttaporn Hencharoenlert)[2]

สุภาวดี อิงศรีสว่าง (Supawadee Ingsrisawang)[3]

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ออกแบบมาตรฐานความปลอดภัยของการแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพส่วนบุคคลของประชาชนในจังหวัดนราธิวาสที่มีการเรียกใช้ข้อมูลผ่านเว็บเซอร์วิส 2) ทำการทดสอบและประเมินผลมาตรฐานความปลอดภัยของเว็บเซอร์วิสที่ออกแบบให้คุ้มครองข้อมูลสารสนเทศสุขภาพส่วนบุคคล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540 การออกแบบมาตรฐานความปลอดภัยของเว็บเซอร์วิสครอบคลุมองค์ประกอบความปลอดภัยของสารสนเทศทั้ง 3 ด้าน คือ 1) ด้านการรักษาความลับใช้วิธีการพิสูจน์ตัวจริงด้วยการ ตรวจสอบเลขบัตรประจำตัวประชาชนจากฐานข้อมูลระบบบริหารงานบุคคลของสำนักงานสาธารณสุขจังหวัดนราธิวาสและตรวจสอบตัวเลขรหัสเฉพาะของผู้ใช้งาน ร่วมกับโพรโทคอลความปลอดภัยที่มีการเข้ารหัส และกำหนดสิทธิ์การเข้าถึงสารสนเทศ 2) ด้านการคงสภาพของข้อมูล มีการกำหนดสถานะของหน่วยบริการสาธารณสุขและสิทธิในการแลกเปลี่ยนข้อมูล การเรียกใช้ข้อมูล ร่วมกับการใช้ภาษาพีเอชพีสลิมเฟรมเวิร์ค 3) ด้านความพร้อมในการใช้งานมีการพิสูจน์ตัวตน และการให้สิทธิ์ในการใช้งาน ผลการวิจัยพบว่าหน่วยบริการสาธารณสุขสามารถแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพระหว่างหน่วยบริการโดยใช้มาตรฐานความปลอดภัยที่ออกแบบไว้ และมีความปลอดภัยตามองค์ประกอบความปลอดภัยของเว็บเซอร์วิสที่ใช้โพรโทคอลเรส ครบทั้งหมด 9 ฟังก์ชัน

คำสำคัญ : เว็บเซอร์วิส มาตรฐานความปลอดภัย ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์

Abstract

The main objective of the paper consist of 1) to design security framework for exchanging the personal health information in Narathiwat province via web services, 2) to evaluate the security framework of web services that designed to protect personal health information based on the National Health ACT, B.E. (2007) and the security in accordance with Official Information ACT, B.E.(1997) Security framework designed using web services included of comprehensive security of information in three methods: (1) the first method introduced the confidentiality by authenticating the identification number that stored in the personal records and verified by the client key using the protocol secure sockets layers status identification and authentication, (2) the second method assigned the integrity of data by setting health information for exchanging and retrieving information using PHP Slim framework and (3) the last method deployed the availability by identification and authorization. From the experimental results, the public health services could exchange information between service units using this proposed security framework design based on REST technology which was tested in 9 functions.

Keywords: Web service ,Security framework , Electronic medical personal record

1 นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช jroonsak@hotmail.com.

2 รองศาสตราจารย์ ประจำสาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช Nuttaporn.Hen@stou.ac.th.

3 นักวิจัยหัวหน้าห้องปฏิบัติการ Information Systems ศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ supawadee@biotec.or.th.

บทนำ

ปัจจุบันกระทรวงสาธารณสุขได้นำเอาเทคโนโลยีสารสนเทศที่มีความก้าวหน้าเป็นอย่างมากมาใช้เป็นเครื่องมือในการให้บริการของสถานบริการสาธารณสุขสังกัดกระทรวงสาธารณสุข ซึ่งครอบคลุมการให้บริการผู้ป่วยนอก การให้บริการสร้างเสริมสุขภาพและป้องกันโรค มีการกำหนดมาตรฐานการจัดเก็บฐานข้อมูลสารสนเทศสุขภาพตามโครงสร้างมาตรฐานข้อมูล 21 แฟ้ม และโครงสร้างฐานข้อมูลด้านการแพทย์และสุขภาพในรูปแบบ 43 แฟ้มมาตรฐาน สำหรับหน่วยบริการ คือ โรงพยาบาลส่งเสริมสุขภาพตำบล (รพ.สต.) ,ศูนย์สุขภาพชุมชน และโรงพยาบาลทั้งภาครัฐและเอกชนของทุกจังหวัดทั่วประเทศ โดยจัดเก็บข้อมูลพื้นฐานและข้อมูลการให้บริการสาธารณสุข การไหลเวียนของข้อมูลสุขภาพจังหวัดนราธิวาสเข้าสู่ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) เป็นระบบสารสนเทศ ที่ทำหน้าที่ในการรับข้อมูลพื้นฐาน และข้อมูลการให้บริการจากโรงพยาบาลที่บันทึกโดยโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาล (HosXP) โรงพยาบาลส่งเสริมสุขภาพตำบลที่บันทึกโดยโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) และศูนย์บริการสาธารณสุขที่บันทึกโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล (HosXp-PCU) หรือ ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) โดยส่งข้อมูลในรูปแบบอิเล็กทรอนิกส์เข้ามาที่สำนักงานสาธารณสุขจังหวัดนราธิวาสแบบอัตโนมัติตลอดเวลา และมีการประมวลผลข้อมูลให้อยู่ในรูปแบบโครงสร้างมาตรฐาน 21 แฟ้ม หน่วยบริการสาธารณสุขในจังหวัดนราธิวาสมีการแลกเปลี่ยนข้อมูลการให้บริการสาธารณสุขผ่านเว็บเซอร์วิสระหว่างโรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลอื่นๆ หรือโรงพยาบาลอื่น ๆ ในจังหวัดนราธิวาส เพื่อนำข้อมูลไปบริหารจัดการได้อย่างมีประสิทธิภาพ การแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสในระบบเดิม (PROVIS web service) ผ่านระบบอินเทอร์เน็ตที่ใช้อยู่ขณะนี้ ยังไม่มีมาตรฐานความปลอดภัยของสารสนเทศ (C.I.A Triangle) ที่สมบูรณ์ครบถ้วน 3 องค์ประกอบ คือ 1) ด้านการรักษาความลับ (Confidentiality) มีการเข้าถึงข้อมูลได้โดยผ่านการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านเดียวกันรายหน่วยบริการและไม่เป็นไปตามมาตรฐานการกำหนดรหัสจำเป็นต้องมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ และการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) ต้องมีการกำหนดรหัสผ่านรายบุคคลร่วมกับฐานข้อมูลระบบบริหารงานบุคคล (PIS) และมีโปรโตคอลที่ปลอดภัย 2) ด้านการคงสภาพของข้อมูล (Integrity) มีการป้องกันแม้ว่าจะไม่เคยเกิดปัญหาแต่ก็มีความเสี่ยงที่ข้อมูลสารสนเทศอาจจะถูกแก้ไขโดยความไม่ตั้งใจของผู้ที่เข้าถึงข้อมูล หรือ SQL Injection จำเป็นต้องมีการการควบคุมการเข้าถึงสารสนเทศ (access control) และการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) และ 3) ด้านความพร้อมในการใช้งาน (Availability) มีความเสี่ยงของข้อมูลสารสนเทศอิเล็กทรอนิกส์ สามารถที่จะถูกลบทำลายได้โดยไวรัสคอมพิวเตอร์ การผิดพลาดถูกลบโดยไม่ตั้งใจ จำเป็นต้องมีการควบคุมการเข้าถึงสารสนเทศและการบริหารจัดการการเข้าถึงของผู้ใช้งาน

หากการเรียกใช้และการแลกเปลี่ยนของข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิส ระหว่างหน่วยบริการสาธารณสุขของสำนักงานสาธารณสุขจังหวัดนราธิวาสไม่ได้มาตรฐานความปลอดภัยของสารสนเทศ (C.I.A Triangle) คือ ด้านการรักษาความลับ หากมีการเปิดเผยข้อมูลที่ผู้รับบริการไม่ต้องการเปิดเผย ทำให้ผู้รับบริการสาธารณสุขเกิดความไม่มั่นใจในบริการสาธารณสุขของรัฐ ด้านการคงสภาพ ข้อมูลประวัติการรับบริการสาธารณสุขใช้ประกอบการให้การบริการสาธารณสุขได้อย่างถูกต้อง อาจเกิดการให้บริการสาธารณสุขที่ผิดพลาดไป เป็นอันตรายกับผู้รับบริการ ด้านความพร้อมใช้งาน ทำให้ไม่สามารถให้บริการได้ หรือเกิดความล่าช้าเพราะไม่สามารถเรียกใช้งานข้อมูลได้ นอกจากนี้ข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 และต้องมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540 มาตรา 23 24 และ 25

ด้วยเหตุผลดังกล่าว ผู้วิจัยต้องการออกแบบมาตรฐานความปลอดภัยในการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาสทดแทนระบบเดิมโดยมีเป้าหมายการรักษาความปลอดภัย สร้างกลไกและเครื่องมือในการรักษาความลับของข้อมูลสุขภาพส่วนบุคคล การคงสภาพข้อมูลสารสนเทศ และการเตรียมความพร้อมในการให้บริการเรียกใช้หรือแลกเปลี่ยนข้อมูลตามการร้องขอใน ลำดับชั้นขนส่ง (Transport Layer) ลำดับชั้นส่วนงาน (Session Layer) ลำดับชั้นนำเสนอ (Presentation Layer) และลำดับชั้นการประยุกต์ (Application Layer) ของแบบจำลองโอเอสไอ (OSI Model) ให้เป็นไปตามข้อกำหนดและนโยบายด้านความปลอดภัย

การออกแบบมาตรฐานความปลอดภัยในการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาสทดแทนระบบเดิมโดยมีเป้าหมายการรักษาความปลอดภัย สร้างกลไกและเครื่องมือในการรักษาความลับของข้อมูลสุขภาพส่วนบุคคล การคงสภาพข้อมูลสารสนเทศ และการเตรียมความพร้อมในการให้บริการเรียกใช้หรือแลกเปลี่ยนข้อมูล มาตรฐานการรักษาความปลอดภัยที่นำมาใช้เป็นมาตรฐานที่เกิดขึ้นจากการใช้งาน (De facto) เป็นมาตรฐานที่เกิดขึ้นจากการใช้งานที่ยอมรับจากคนทั่วไป (สิทธิศักดิ์ สายเงิน : 2556) ซึ่งหน่วยบริการในสำนักงานสาธารณสุขจังหวัดนราธิวาสยอมรับมาตรฐานนี้ทั้งการบริหารจัดการโดยใช้นโยบายด้านความมั่นคง (สิทธิศักดิ์ สายเงิน : 2556) และ ด้านเทคนิค โดยทั้ง 2 ส่วนมีความเกี่ยวเนื่องกัน ให้เป็นไปตามข้อกำหนดและนโยบายด้านความปลอดภัยและพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540

วัตถุประสงค์การวิจัย

1.เพื่อออกแบบมาตรฐานความปลอดภัย (security framework) ของการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคล ของประชาชนในจังหวัดนราธิวาสที่มีการเรียกใช้ข้อมูลผ่านเว็บเซอร์วิส (Web Service) และมีการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค ระหว่างระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน(JHCIS) กับระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial health Information System : PROVIS) ผ่านเครือข่ายอินเทอร์เน็ต

2.เพื่อทดสอบมาตรฐานความปลอดภัยที่ออกแบบไว้ ในการคุ้มครองข้อมูลสารสนเทศสุขภาพส่วนบุคคลจากผู้ที่ไม่เกี่ยวข้องกับข้อมูล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7,8,9 และ 10 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตาม พระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540 มาตรา 23,24 และ 25

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการวิจัยและพัฒนา มีการออกแบบและสร้างมาตรฐานความปลอดภัย (security framework) ตามมาตรฐานความปลอดภัยของสารสนเทศ (C.I.A Triangle) อ้างอิงตามแบบจำลองโอเอสไอ (OSI Model) ทั้งด้านการบริหารจัดการการเรียกใช้และแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพส่วนบุคคลด้วยเว็บเซอร์วิส และด้านเทคนิค มีการพัฒนาระบบแลกเปลี่ยนข้อมูล Healthws System ซึ่งประกอบด้วยเว็บเซอร์วิสเซิร์ฟเวอร์ของสำนักงานสาธารณสุขจังหวัดนราธิวาสทำหน้าที่ให้บริการข้อมูลกับเว็บเซอร์วิสไคลเอนต์ (Healthws Client) ที่โรงพยาบาลส่งเสริมสุขภาพตำบลในจังหวัดนราธิวาสด้วยเทคโนโลยีเว็บเซอร์วิส (Web Service) โดยอ้างอิงแบบจำลองโอเอสไอ (OSI Model) ในลำดับชั้นขนส่ง (Transport Layer) ใช้มาตรฐาน SSL 3.0/TLS 1.0 (Secure Sockets / Layer Transport Layer Security) เป็นระบบรักษาความปลอดภัยของเว็บเซอร์วิสเซิร์ฟเวอร์ เข้ารหัสข้อมูลด้วย WS-Security Tokens / X.509 Certificate ลำดับชั้นส่วนงาน (Session Layer) ใช้การจัดการ Session ลำดับชั้นนำเสนอ (Presentation Layer) มีการแปลงข้อมูลให้อยู่ในรูปแบบ JSON (JavaScript Object Notation) ด้วยเครื่องมือ PHP Slim Framework ในการให้บริการเว็บเซอร์วิสเซิร์ฟเวอร์แบบ REST Web Service และ ลำดับชั้นการประยุกต์ (Application Layer) มีการพัฒนาเว็บเซอร์วิสเซิร์ฟเวอร์ด้วยเครื่องมือ PHP Slim Framework และพัฒนาเว็บเซอร์วิสไคลเอนต์ด้วยเครื่องมือ NetBeans IDE8.0 ใช้ภาษา JAVA Application ตรวจสอบผู้ใช้งานร่วมกับฐานข้อมูลระบบบริหารงานบุคคล (PIS)

การทดสอบมาตรฐานความปลอดภัย (security framework)ในการเรียกใช้และแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพส่วนบุคคลด้วยระบบ Healthws System ตามมาตรฐานความปลอดภัยของสารสนเทศ (C.I.A Triangle) คือ

1) ด้านการรักษาความลับ (Confidentiality) ด้วยการทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์ด้วยเครื่องมือ Google Chrome Advanced Rest Client และทดสอบการใช้งาน Healthws-Client

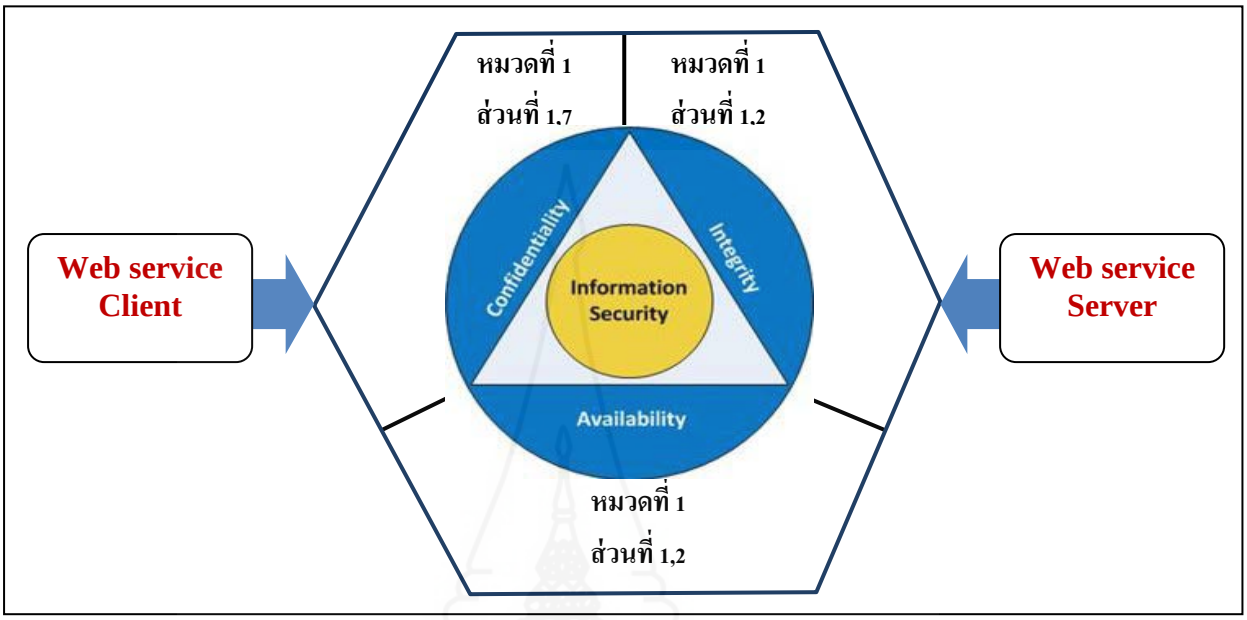
2) ด้านการคงสภาพข้อมูล (Integrity) ทำการทดสอบด้วยวิธีการทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ REST โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี และมีการประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ โดยการประเมินตามข้อกำหนด NIST SP 800-44 Guidelines on Securing Public Web Servers ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST)

3) ด้านความพร้อมใช้งาน (Availability) ทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์ด้วยเครื่องมือ Google Chrome Advanced และทดสอบการใช้งาน Healthws-Client

ผลการวิจัย

การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส ครอบคลุมด้านการบริหารจัดการ และด้านเทคนิค เพื่อให้ข้อมูลสารสนเทศมีมาตรฐานความปลอดภัยอ้างอิงแบบจำลองโอเอสไอ (OSI Model) ในลำดับชั้นการประยุกต์ (Application Layer) รวมทั้งการออกแบบมาตรฐานความปลอดภัยตามมาตรฐานขึ้นมาใช้งานตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) และประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ 7 มกราคม 2556 เพื่อให้เป็นไปตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ที่สมบูรณ์ คือ 1) ด้านการรักษาความลับ (Confidentiality) ใช้วิธีการ Authentication ตรวจสอบค่าเลขบัตรประจำตัวประชาชนจากฐานข้อมูลระบบบริหารงานบุคคลของสำนักงานสาธารณสุขจังหวัดนราธิวาสและตรวจสอบค่า Client Key ของผู้ใช้งาน ร่วมกับมาตรฐาน SSL 3.0 / TLS 1.0 2) ด้านการคงสภาพของข้อมูล (Integrity) มีการกำหนดสถานะของหน่วยบริการสาธารณสุขและสิทธิ(Authorization)ในการแลกเปลี่ยนข้อมูล การเรียกใช้ข้อมูล ร่วมกับการใช้ภาษา PHP Slim Framework และ 3) ด้านความพร้อมในการใช้งาน (Availability) มีการพิสูจน์ตัวตน (Identification) และการให้สิทธิ์ (Authorization)

จากการวิเคราะห์รูปแบบการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส ด้านการบริหารจัดการ ผู้วิจัยได้ออกแบบมาตรฐานความปลอดภัยตามมาตรฐานเรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข ลงวันที่ 7 มกราคม 2556 ตามภาพที่ 1 เพื่อให้ครอบคลุมตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ตามตารางที่ 1

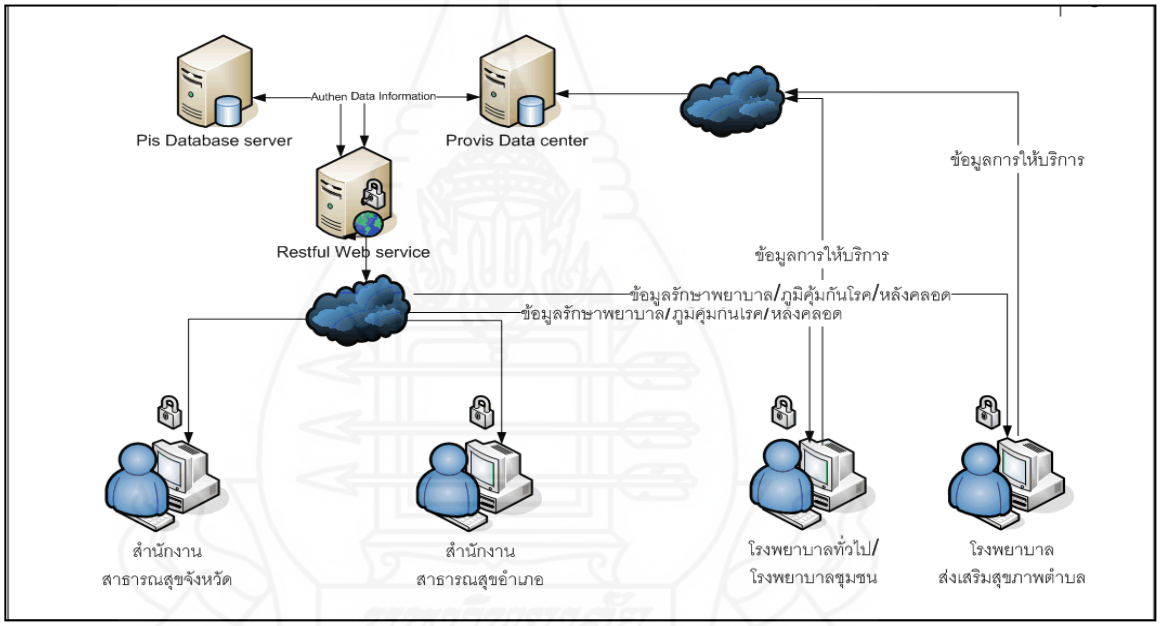


ภาพที่ 1 การออกแบบกรอบงานมาตรฐานความปลอดภัยเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส

ตารางที่ 1 ความสอดคล้องกันระหว่าง **CIA Triangle** กับนโยบายความปลอดภัย

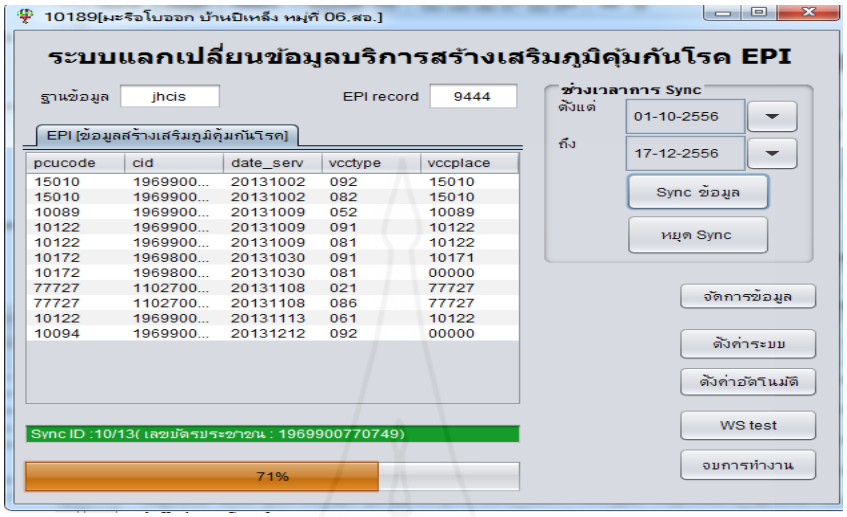
CIA Triangle	**นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข**
การรักษาความลับของสารสนเทศ(Confidentiality)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)
ความสมบูรณ์ของสารสนเทศ (Integrity)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (access control) ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)
ความพร้อมใช้ (Availability)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (access control) ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

การแลกเปลี่ยนข้อมูลระหว่างสถานบริการสาธารณสุขที่เป็นโรงพยาบาลทั่วไป โรงพยาบาลชุมชนและโรงพยาบาลส่งเสริมสุขภาพตำบลนั้นเป็นการสื่อสารแลกเปลี่ยนข้อมูลผ่าน REST web service ในการพัฒนาระบบแลกเปลี่ยนข้อมูล Healthws System ซึ่งประกอบด้วยเว็บเซอร์วิสเซิร์ฟเวอร์ของสำนักงานสาธารณสุขจังหวัดนราธิวาสที่ให้บริการแลกเปลี่ยนข้อมูลกับเว็บเซอร์วิสไคลเอนต์ (Healthws Client) ที่โรงพยาบาลส่งเสริมสุขภาพตำบลในจังหวัดนราธิวาส ข้อมูลที่แลกเปลี่ยนในรูปแบบ JSON (JavaScript Object Notation) เป็นข้อมูลที่มีขนาดเล็ก ทำให้มีความรวดเร็วในการรับส่งข้อมูล ผู้ที่มีสิทธิ์ในการเรียกใช้และแลกเปลี่ยนข้อมูลจะต้องเป็นเจ้าหน้าที่สาธารณสุขที่มีข้อมูลอยู่ในฐานข้อมูลระบบบริหารงานบุคคลของสำนักงานสาธารณสุขจังหวัดนราธิวาสและมีสถานะการปฏิบัติงานอยู่ในปัจจุบันเท่านั้น และมีการออกแบบความปลอดภัยของชุดโปรแกรมคำสั่งของเว็บเซอร์วิสเซิร์ฟเวอร์ ด้วยวิธีการ Security REST web service ตามภาพที่ 2



ภาพที่ 2 การออกแบบรูปแบบแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสแบบ REST

ระบบ Healthws System ประกอบด้วยเว็บเซอร์วิสเซิร์ฟเวอร์แบบ REST web service ทำหน้าที่ให้บริการแลกเปลี่ยนข้อมูล และ เว็บเซอร์วิสไคลเอนต์ (Healthws Client) ที่ติดตั้งไว้ที่โรงพยาบาลส่งเสริมสุขภาพตำบลของจังหวัดนราธิวาสเข้าเรียกใช้บริการจากเว็บเซอร์วิสเซิร์ฟเวอร์ในการแลกเปลี่ยนข้อมูลดังกล่าวตามภาพที่ 3



ภาพที่ 3 หน้าจอ Healthws Client กำลังทำงานดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์

ผู้วิจัยมีการประเมินผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบมาตรฐานความปลอดภัยของสารสนเทศ (C.I.A Triangle) ทั้ง 3 ด้าน ดังนี้

1) ด้านการรักษาความลับ (Confidentiality) ทดสอบการเข้าถึงข้อมูล โดยผู้พัฒนาระบบทำการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีและไม่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ทดสอบการเข้าสู่ระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ในรูปแบบต่างๆ การแลกเปลี่ยนข้อมูลด้วย Client Key ที่ถูกต้องได้ตามตารางที่ 2 และหากมีการปลอมแปลงข้อมูลที่ใช้ในการพิสูจน์ตัวจริงของเว็บเซอร์วิสไคลเอนต์ จะไม่สามารถทำได้เนื่องจาก Client Key ผ่านการเข้ารหัสข้อมูลแบบ WS-Security Tokens / X.509 Certificate ด้วยโปรโตคอล SSL ทำให้เว็บเซอร์วิสเซิร์ฟเวอร์ปฏิเสธการแลกเปลี่ยนข้อมูล ตามตารางที่ 3

2) ด้านการคงสภาพของข้อมูล (Integrity) โดยผู้พัฒนาระบบทำการทดสอบด้วยวิธีการทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ REST โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศิลปหัตถกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี ผู้พัฒนาระบบทำการทดสอบการยืนยันตัวตน การตรวจสอบคีย์ที่ใช้ยืนยันการขอใช้บริการเว็บเซอร์วิส ทดสอบด้วยการดึงข้อมูลทดสอบของผู้รับบริการ โดยจะทดสอบส่วนการร้องขอข้อมูลไปยังเว็บเซอร์วิสเซิร์ฟเวอร์ และส่วนการตอบกลับข้อมูล โดยการเชื่อมต่อด้วยอินเตอร์เน็ต

3) ด้านความพร้อมในการใช้งาน (Availability) โดยผู้พัฒนาระบบทดสอบการเข้าไปเรียกใช้ข้อมูลโดยการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล ทดสอบการเรียกใช้ และ

แลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล ผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System และทำการประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ ตามข้อกำหนดของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ผลการประเมิน(แสดงบางข้อกำหนด)ตามตารางที่ 4

ผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบความปลอดภัยของสารสนเทศโดยเรียกใช้เว็บเซอร์วิสจาก URL ที่ทดสอบ https://healthws.ntwo.moph.go.th/serviceapi/epiinfo.php

ก) หมายเลขกรณีทดสอบ SE01 ตามตารางที่ 2

ตารางที่ 2 กรณีทดสอบ SE01

หมายเลขกรณีทดสอบ	SE01	**ชื่อ**	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชัน getEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับเมื่อมีการเรียกใช้ฟังก์ชันว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย **คำอธิบาย**	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getEPI 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getEPI - Client Key มีค่า ********** - pcucode มีค่า 11111		
เงื่อนไขในการทดสอบ	ระบบต้องแสดงค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน		☐ ไม่ผ่าน
หมายเหตุ			
ผู้ทดสอบ	จรูญศักดิ์ เวทมาหะ		

ข) หมายเลขกรณีทดสอบ SE02 ตามตารางที่ 3

ตารางที่ 3 กรณีทดสอบ SE02

หมายเลขกรณีทดสอบ	SE02	**ชื่อ**	พิสูจน์ตัวจริงของผู้ใช้งานในการเรียกใช้ฟังก์ชัน getEPI
ทดสอบความต้องการ	เพื่อพิสูจน์ตัวจริงของผู้ใช้งานในการเรียกใช้ฟังก์ชัน getEPI เมื่อมีการเรียกใช้ฟังก์ชัน getEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getEPI 3. ระบุค่าข้อมูล Client Key ที่ไม่ถูกต้องและ pcucode ที่ถูกต้อง โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getEPI - Client Key มีค่า **********xxxxxx********** - pcucode มีค่า 10089		
เงื่อนไขในการทดสอบ	ระบบต้องแสดงข้อความให้ผู้ใช้งานทราบว่าข้อมูลผู้ใช้งานที่ระบุไม่ถูกต้อง		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบแสดงข้อความ Invalid Clientkey		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบแสดงข้อความ [{"statusid":"0","status":"Invalid Clientkey","pcucode":"10089"}]		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	จรูญศักดิ์ เวทมาหะ		

การประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ โดยการประเมินตามข้อกำหนดของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทั้ง 3 ส่วน ปรากฏผลดังนี้

ส่วนที่ 1) ข้อกำหนดความปลอดภัยของระบบปฏิบัติการ (Checklist for Securing the Web Server Operating System) จำนวน 20 ข้อกำหนด มีการดำเนินการครบทุกข้อกำหนด แสดงรายละเอียดบางข้อกำหนดตามตารางที่ 4

ส่วนที่ 2) ข้อกำหนดความปลอดภัยของเว็บเซิร์ฟเวอร์ (Checklist for Securing the Web Server) จำนวน 32 ข้อกำหนด มีการดำเนินการ 30 ข้อกำหนด ไม่ได้ดำเนินการ 2 ข้อกำหนด คือ ข้อกำหนดที่ 18 เนื่องจากไม่อนุญาตให้ผู้ใช้งานมีการอัพโหลดไฟล์ (uploads files) ไปยังเว็บเซิร์ฟเวอร์ และข้อกำหนดที่ 31 เนื่องจากไม่มีความจำเป็น

ต้องใช้ robots.txt file แสดงรายละเอียดบางข้อกำหนดตามตารางที่ 4

ส่วนที่ 3) ข้อกำหนดความปลอดภัยของเนื้อหา (Checklist for Securing Web Content) จำนวน 64 ข้อกำหนด มีการดำเนินการ 61 ข้อกำหนด ไม่ได้ดำเนินการ 3 ข้อกำหนด คือ ข้อกำหนดที่ 9 ,10 เนื่องจากไม่ใช่ข้อมูลด้านการสืบสวนและการเงิน ข้อกำหนดที่ 32 เนื่องจากไม่มีความจำเป็นต้องใช้ลายมือชื่ออิเล็กทรอนิกส์ แสดงรายละเอียดบางข้อกำหนดตามตารางที่ 4

ตารางที่ 4 ผลการประเมินตามข้อกำหนดของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (บางส่วน)

Completed	**Action**
ส่วนที่ 1 มาตรฐานความปลอดภัยของระบบปฏิบัติการ	
Y	1.Create, document, and implement a patching process
Y	2.Keep the servers disconnected from networks or on an isolated network that severely restricts communications until all patches have been installed
Y	3.Identify and install all necessary patches and upgrades to the OS
ส่วนที่ 2 มาตรฐานความปลอดภัยของเว็บเซิร์ฟเวอร์	
N/A	18.If uploads are allowed to the Web server, configure it so that a limit is placed on the amount of hard drive space that is dedicated for this purpose; uploads should be placed on a separate partition
Y	21.Ensure that any virtualized guest OSs follow this checklist
N/A	31.Use the robots.txt file, if appropriate
ส่วนที่ 3 มาตรฐานความปลอดภัยของเนื้อหา	
N/A	9.Investigative records
N/A	10.Financial records (beyond those already publicly available)
N/A	32.Use digital signatures on e-mail if appropriate

อภิปรายผลการวิจัย

ผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ทั้ง 3 องค์ประกอบ ปรากฏผลดังนี้

1) ด้านการรักษาความลับ(Confidentiality) ทดสอบการเข้าถึงข้อมูล โดยผู้พัฒนาระบบทดสอบการเข้าสู่ระบบและการเข้าถึงข้อมูล ผลการทดสอบระบบ Healthws-Client ทดสอบการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่ไม่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ผลการทดสอบไม่สามารถเข้าสู่ระบบได้ และทดสอบการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล ผลการทดสอบสามารถเข้าสู่ระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้ ผลการทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์ https://healthws.ntwo.moph.go.th/serviceapi/ epiinfo.php ด้วยเครื่องมือ Google Chrome Advanced Rest Client เมื่อทดสอบการเข้าถึงข้อมูลด้วย Client Key ที่ไม่ถูกต้อง ผลการทดสอบไม่สามารถเข้าถึงข้อมูลได้ และ เมื่อทดสอบการเข้าถึงข้อมูลด้วย Client Key ที่ถูกต้อง ผลการทดสอบสามารถเข้าถึงข้อมูลสุขภาพส่วนบุคคล ได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

2) ด้านการคงสภาพของข้อมูล (Integrity) โดยผู้พัฒนาระบบทำการทดสอบด้วยวิธีการทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ Rest ตรวจสอบความถูกต้องในการเรียกใช้ในแต่ละฟังก์ชัน จำนวน 9 ฟังก์ชัน คือ getEPI ,addEPI ,updateEPI ,deleteEPI ,searchEPI ,getSERVICEINFO ,getDIAGINFO, getDRUGINFO และ getMCHINFO โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี ด้วยเครื่องมือ Google Chrome Advanced Rest Client ผลการทดสอบพบว่า ผ่านทุกฟังก์ชัน

3) ด้านความพร้อมในการใช้งาน (Availability) เมื่อทดสอบการเข้าไปเรียกใช้ข้อมูลโดยการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคลสามารถเรียกใช้และแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล ผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ได้

ผลการทดสอบระบบ Healthws-Client ด้วยผู้ใช้งานตามสถานะสถานบริการที่แตกต่างกัน ผลการทดสอบสามารถเข้าถึงข้อมูลของผู้รับบริการตามสถานะการแลกเปลี่ยนข้อมูลและการเรียกใช้ข้อมูลได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

ผลการทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์ https://healthws.ntwo.moph.go.th/serviceapi/epiinfo.php ทดสอบการเข้าถึงข้อมูลด้วยเครื่องมือ Google Chrome Advanced Rest Client ทดสอบ getEPI operation โดยป้อนค่า Client Key ที่ถูกต้องและสถานะสถานบริการที่แตกต่างกัน ผลการทดสอบสามารถเข้าถึงข้อมูลของผู้รับบริการตามสถานะการแลกเปลี่ยนข้อมูลและการเรียกใช้ข้อมูลได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

การประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ตามข้อกำหนดของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทำการประเมิน 3 ส่วนคือ

1. ข้อกำหนดความปลอดภัยของระบบปฏิบัติการ (Checklist for Securing the Web Server Operating System) จำนวน 20 ข้อกำหนด มีการดำเนินการครบทุกข้อกำหนด

2 ข้อกำหนดความปลอดภัยของเว็บเซิร์ฟเวอร์ (Checklist for Securing the Web Server) จำนวน 32 ข้อกำหนด มีการดำเนินการ 30 ข้อกำหนด ไม่ได้ดำเนินการ 2 ข้อกำหนด คือ ข้อกำหนดที่ 18 เนื่องจากไม่อนุญาตให้ผู้ใช้งานมีการ uploads files ไปยังเว็บเซิร์ฟเวอร์ และข้อกำหนดที่ 31 เนื่องจากไม่มีความจำเป็นต้องใช้ robots.txt file

3. ข้อกำหนดความปลอดภัยของเนื้อหา(Checklist for Securing Web Content) จำนวน 64 ข้อกำหนด มีการดำเนินการ 61 ข้อกำหนด ไม่ได้ดำเนินการ 3 ข้อกำหนด คือ ข้อกำหนดที่ 9 ,10 เนื่องจากไม่ใช่ข้อมูลด้านการสืบสวนและการเงิน ข้อกำหนดที่ 32 เนื่องจากไม่มีความจำเป็นต้องใช้ลายมือชื่ออิเล็กทรอนิกส์

ผลการออกแบบมาตรฐานความปลอดภัย (Security Framework) และทดสอบมาตรฐานความปลอดภัยที่ออกแบบไว้ ทำให้การแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค ระหว่างระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน(JHCIS) กับระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial Health Information System : PROVIS) ผ่านเครือข่ายอินเทอร์เน็ต ได้รับการคุ้มครองข้อมูลสารสนเทศสุขภาพส่วนบุคคลจากผู้ที่ไม่เกี่ยวข้องกับข้อมูล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 ,8 ,9 และ10 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตาม พระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540 มาตรา 23 ,24 และ 25

ข้อเสนอแนะ

1.ในการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส เว็บเซอร์วิสพัฒนาด้วยภาษา PHP ร่วมกับ PHP Slim Framework และเว็บเซอร์วิสไคลเอนต์ พัฒนาด้วยภาษา JAVA มีความสะดวกเป็น opensource ไม่มีลิขสิทธิ์ โดยใช้เครื่องมือ Netbean 8.0 เนื่องจากมี Library สนับสนุนครบถ้วนและสามารถทำงานได้หลาย platform และควรทำการอัพเดตช่องโหว่ในส่วน Openssl ของเซิร์ฟเวอร์ให้เป็นปัจจุบันอย่างสม่ำเสมอเพื่อความปลอดภัยในการแลกเปลี่ยนข้อมูล

2.ในการเตรียมข้อมูลสำหรับการวิจัยครั้งนี้ ระบบจัดการฐานข้อมูล คือ MySQL พบว่าหากมีการร้องขอข้อมูลจากการสร้างความสัมพันธ์จากตารางข้อมูลมากกว่า 2 ตาราง จะทำให้การทำงานของระบบในการค้นหาข้อมูลและปรับปรุงข้อมูลมีความล่าช้าเล็กน้อย เนื่องจากการสร้างความสัมพันธ์ระหว่างตาราง ผู้วิจัยได้ใช้วิธีการ

สร้างฟังก์ชันเฉพาะขึ้นมาทำงานแทนกรณีดังกล่าวโดยเก็บค่าข้อมูลที่มีความสัมพันธ์มาเก็บไว้ในตัวแปรและส่งค่าข้อมูลนั้นคืนกลับเมื่อมีการร้องขอข้อมูลนั้น ปรากฏว่าการค้นหาข้อมูลและปรับปรุงข้อมูลทำได้รวดเร็ว ขึ้นและได้เพิ่มตัวเลือกให้มีการเลือกตั้งค่าการร้องขอข้อมูลได้ตามช่วงเวลาที่ต้องการ โดยค่าเริ่มต้นของระบบจะกำหนดช่วงเวลาในการแลกเปลี่ยนข้อมูล เริ่มตั้งแต่วันแรกของปีงบประมาณ คือ วันที่ 1 ตุลาคม จนถึงวันที่ปัจจุบัน หรือช่วงเวลาอื่นๆ ซึ่งผู้ใช้งานสามารถกำหนดช่วงเวลาได้ตามต้องการ ดังนั้นควรจำกัดช่วงข้อมูลในการแลกเปลี่ยนผ่านเว็บเซอร์วิสไคลเอนต์ไม่เกิน 1 ปี ซึ่งข้อมูลมีความครบถ้วนและเป็นปัจจุบันในการนำมาใช้ในการดำเนินงาน

3. เพื่อให้การให้บริการแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสมีความปลอดภัยเพิ่มขึ้น ต้องมีการรักษาความปลอดภัยของข้อมูลสารสนเทศสุขภาพแบบอื่นๆ เช่น การออกแบบ policy ของ Firewall หรือ การรักษาความปลอดภัยทางกายภาพร่วมด้วย

เอกสารอ้างอิง

กานดา รุณนะพงศา และคณะ (2557) “แนวทางในการทดสอบฟังก์ชันการทำงานของเว็บเซอร์วิสแบบ Rest (ออนไลน์)สืบค้นจาก : http://www.pongsak.hoontrakul.com/papers/060705_REST_Functional_Testing_Guidelines_by_Kanda_n_Pongsak_et_al.pdf [28 มิถุนายน 2557]

กิตติ ภักดีวัฒนะกุล (2553) “การพัฒนาระบบด้วยสถาปัตยกรรมเชิงบริการบนเทคโนโลยีของ web Service” กรุงเทพมหานคร บริษัท เคทีพี คอมพ์ แอนด์ คอนซัลท์

ชาลี ธรรมรัตน์ (2554) “ความมั่นคงปลอดภัยการรับส่งแฟ้มข้อมูลและการจัดการการเข้ารหัสลับภายในองค์กร” สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร

เดชาวัต นิชาญานันท์ (2555) “การจัดทำนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร กรณีศึกษาสำหรับบริษัท สินแพทย์ จำกัด (โรงพยาบาลสินแพทย์)” สารนิพนธ์ ปริญญาวิทยาศาสตรหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร

ใบรับรองอิเล็กทรอนิกส์ (ออนไลน์) (2550) สืบค้นจาก : http://wiki.nectec.or.th/setec/Knowledge/AdvancedPKI [1 กรกฎาคม 2557]

ปัญหาของ OpenSSL และแนวทางแก้ไข (ออนไลน์) (2557) สืบค้นจาก : http://www.tisa.or.th/articles/The Heartbleed-Bug_12042014.pdf [30 มิถุนายน 2557]

สิทธิศักดิ์ สายเงิน (2556) “การรักษาความปลอดภัยในการให้บริการผ่านเว็บ” ใน*เอกสารการสอนชุดวิชา* เทคโนโลยีการให้บริการผ่านเว็บและการประยุกต์ หน่วยที่ 11 หน้า 11-24 นนทบุรี มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

"พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550" (2550, 19 มีนาคม) *ราชกิจจานุเบกษา* เล่มที่ 124 ตอนที่ 16 ก หน้า 3-4

"พระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. 2540" (2540, 10 กันยายน) *ราชกิจจานุเบกษา* เล่มที่ 114 ตอนที่ 46 ก หน้า 8-10

ศราวุฒิ จันทะคัด (2554) "การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา : บริษัท แซนด์ แอนด์ซอยล์อุตสาหกรรม จำกัด" สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร

Khalid Aldrawiesh. (2011). Security Policy Architecture for Web Services Environment . Software Technology Research Laboratory (STRL) Faculty of Technology. England: De Montfort University.

Miles Tracy ,Wayne Jansen ,Karen Scarfone ,Theodore Winograd (2007). Guidelines on Securing Public Web Servers. National Institute of Standards and Technology : NIST

Omar Slomic.(2011). A message-level security approach for RESTful services. Norway: UNIVERSITY OF OSLO Department of informatics.