การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส

นายจรูญศักดิ์ เวทมาหะ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2557

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

Mr. Jaroonsak Watmaha

A Thesis Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Science in Information and Communication Technology

School of Science and Technology

Sukhothai Thammathirat Open University

2014

หัวข้อวิทยานิพนธ์ การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส

ชื่อและนามสกุล นายจรูญศักดิ์ เวทมาหะ

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา 1. รองศาสตราจารย์ณัฐพร เห็นเจริญเลิศ

2. อาจารย์ ดร.สุภาวดี อิงศรีสว่าง

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 28 สิงหาคม 2557

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(นาวาอากาศเอก อาจารย์ ดร.สิทธิศักดิ์ สายเงิน)

..... กรรมการ
(รองศาสตราจารย์ณัฐพร เห็นเจริญเลิศ)

..... กรรมการ
(อาจารย์ ดร.สุภาวดี อิงศรีสว่าง)

..... ประธานกรรมการบัณฑิตศึกษา
(ศาสตราจารย์ ดร.สิริวรรณ ศรีพหล)

ชื่อวิทยานิพนธ์ การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส

ผู้วิจัย นายจรูญศักดิ์ เวทมาหะ **รหัสนักศึกษา** 2549600084

ปริญญา วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

อาจารย์ที่ปรึกษา (1) รองศาสตราจารย์ณัฐพร เห็นเจริญเลิศ (2) อาจารย์ ดร. สุภาวดี อิงศรีสว่าง

ปีการศึกษา 2557

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ออกแบบมาตรฐานความปลอดภัยของการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลของประชาชนในจังหวัดนราธิวาสที่มีการเรียกใช้ข้อมูลผ่านเว็บเซอร์วิส 2) ทำการทดสอบและประเมินผลมาตรฐานความปลอดภัยของเว็บเซอร์วิสที่ออกแบบให้คุ้มครองข้อมูลสารสนเทศสุขภาพส่วนบุคคล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตาม พระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540

การออกแบบมาตรฐานความปลอดภัยของการเรียกใช้ข้อมูลสารสนเทศสุขภาพครอบคลุมองค์ประกอบความปลอดภัยของสารสนเทศทั้ง 3 ด้าน คือ 1) ด้านการรักษาความลับใช้วิธีการพิสูจน์ตัวจริงด้วยการ ตรวจสอบเลขบัตรประจำตัวประชาชนจากฐานข้อมูลระบบบริหารงานบุคคลของสำนักงานสาธารณสุขจังหวัดนราธิวาสและตรวจสอบตัวเลขรหัสเฉพาะของผู้ใช้งาน ร่วมกับโพรโทคอลความปลอดภัยที่มีการเข้ารหัส และกำหนดสิทธิ์การเข้าถึงสารสนเทศ 2) ด้านการคงสภาพของข้อมูล มีการกำหนดสถานะของหน่วยบริการสาธารณสุขและสิทธิในการเรียกใช้ข้อมูล ร่วมกับการใช้ภาษาพีเอชพีสลิมเฟรมเวิร์ค 3) ด้านความพร้อมในการใช้งานมีการพิสูจน์ตัวตน และการให้สิทธิ์ในการใช้งาน

ผลการวิจัยพบว่าหน่วยบริการสาธารณสุขสามารถแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพระหว่างหน่วยบริการโดยใช้มาตรฐานความปลอดภัยที่ออกแบบไว้ และมีความปลอดภัยตามองค์ประกอบความปลอดภัยของสารสนเทศครบทั้ง 3 ด้าน

คำสำคัญ เว็บเซอร์วิส มาตรฐานความปลอดภัย ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์

Thesis title: Privacy Security Framework Design for Electronic Medical Records using Web Services in Narathiwat Province
Researcher: Mr. Jaroonsak Watmaha ; **ID:** 2549600084;
Degree: Master of Science (Information and Communication Technology);
Thesis advisors: (1) Nuttaporn Hencharoenlert, Associate Professer;
(2) Dr. Supawadee Ingsrisawang; **Academic year:** 2014

Abstract

The main objectives of this study are 1) to design security framework for retrieving the personal health information in Narathiwat province via web services, 2) to evaluate the designed framework for the protection of personal health information based on the National Health ACT, B.E. (2007) and the security in accordance with the Official Information ACT, B.E.(1997).

The security framework has been designed and implemented using web-services to assure the information security with the following activities: (1) the identification and authentication at the secure socket layer to create the confidentiality by using encrypted protocol and identifying information accessibility, (2) the data validation with PHP slim framework for maintaining the integrity, and (3) the availability of information at a required level of performance.

The findings of this study showed that the designed security framework can be used to ensure the security of public health information sharing among health service-units.

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

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยได้รับความร่วมอนุเคราะห์จากท่านผู้ทรงคุณวุฒิหลายท่านโดยเฉพาะ อาจารย์ รองศาสตราจารย์ณัฐพร เห็นเจริญเลิศ อาจารย์ที่ปรึกษาหลัก และอาจารย์ ดร.สุภาวดี อิงศรีสว่าง อาจารย์ที่ปรึกษาร่วมของวิทยานิพนธ์ฉบับนี้ ซึ่งได้สละเวลาในการให้คำปรึกษาแนวทางตลอดจนแนะนำเกี่ยวกับข้อมูลและเนื้อหาที่จะนำมาปรับปรุงแก้ไข้ข้อบกพร่องต่างๆ เพื่อให้เป็นวิทยานิพนธ์ที่สมบรูณ์ฉบับหนึ่ง ผู้วิจัยกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ นายแพทย์สรรพงษ์ ฤทธิรักษา นายแพทย์สาธารณสุขจังหวัดนราธิวาส ที่ให้ความอนุเคราะห์ข้อมูลและสถานที่เพื่อนำระบบเข้ามาทำการทดสอบการใช้งาน และขอขอบคุณเจ้าหน้าที่สาธารณสุขโรงพยาบาลส่งเสริมสุขภาพตำบล ที่อำนายความสะดวกในเรื่องข้อมูล รวมทั้งให้ความช่วยเหลือแนะนำในส่วนต่างๆ ของระบบได้เป็นอย่างดี และขอขอบคุณผู้ที่มีส่วนร่วมทุกท่านที่มิได้เอ่ยนามไว้ ณ ที่นี้

นอกจากนี้ ขอขอบคุณคณาจารย์สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช เพื่อนนักศึกษาและผู้ที่มีส่วนเกี่ยวข้องในการทำวิทยานิพนธ์ครั้งนี้ ทุกท่านที่ได้กรุณาให้การสนับสนุน ช่วยเหลือ และให้กำลังใจตลอดมาจนกระทั่งการทำวิจัยวิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์ด้วยดี

จรูญศักดิ์ เวทมาหะ

สิงหาคม 2557

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1. ประเด็นปัญหาการวิจัย

ปัจจุบันกระทรวงสาธารณสุขได้นำเอาเทคโนโลยีสารสนเทศที่มีความก้าวหน้าเป็นอย่างมากมาใช้เป็นเครื่องมือในการให้บริการของสถานบริการสาธารณสุขสังกัดกระทรวงสาธารณสุข ซึ่งครอบคลุมการให้บริการผู้ป่วยนอก การให้บริการสร้างเสริมสุขภาพและป้องกันโรค มีการกำหนดมาตรฐานการจัดเก็บฐานข้อมูลสารสนเทศสุขภาพตามโครงสร้างมาตรฐานข้อมูล 21 แฟ้ม (ปัจจุบันใช้ เวอร์ชั่น 5.0 วันที่ 1 ตุลาคม 2555) และโครงสร้างฐานข้อมูลด้านการแพทย์และสุขภาพ ในรูปแบบ 43 แฟ้มมาตรฐาน (ปัจจุบันใช้เวอร์ชั่น 1.0 วันที่ 16 มีนาคม 2555) สำหรับหน่วยบริการประจำ คือ โรงพยาบาลส่งเสริมสุขภาพตำบล (รพ.สต.) ศูนย์สุขภาพชุมชน และโรงพยาบาลทั้งภาครัฐและเอกชนของทุกจังหวัดทั่วประเทศ โดยจัดเก็บข้อมูลพื้นฐานและข้อมูลการให้บริการสาธารณสุข หรือ “ข้อมูลการให้บริการผู้ป่วยนอกและการสร้างเสริมสุขภาพและป้องกันโรครายบุคคล (OP/PP Individual Data)” ส่งไปยังสำนักงานหลักประกันสุขภาพแห่งชาติและสำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข เป็นประจำทุกเดือนผ่านสำนักงานสาธารณสุขจังหวัดมาตั้งแต่ ปี พ.ศ. 2546 ปัจจุบันแต่ละจังหวัดจะมีระบบคลังข้อมูลด้านการแพทย์และสุขภาพ (Data Center) ระดับจังหวัด จัดเก็บข้อมูลตามโครงสร้างฐานข้อมูลด้านการแพทย์และสุขภาพ ในรูปแบบ 43 แฟ้มมาตรฐาน และระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) จัดเก็บฐานข้อมูลสารสนเทศสุขภาพตามโครงสร้างมาตรฐานข้อมูล 21 แฟ้ม ซึ่งพัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ติดตั้งให้กับสำนักงานสาธารณสุขจังหวัดต่างๆ ทั่วประเทศ

การไหลเวียนของข้อมูลสุขภาพจังหวัดนราธิวาสเข้าสู่ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) เป็นระบบสารสนเทศ ที่ทำหน้าที่ในการรับข้อมูลพื้นฐานและข้อมูลการให้บริการจากโรงพยาบาลที่บันทึกโดยโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาล (HosXP) โรงพยาบาลส่งเสริมสุขภาพตำบลที่บันทึกโดยโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) และศูนย์บริการสาธารณสุขที่บันทึกโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล (HosXp-PCU) หรือ ระบบงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) โดยส่งข้อมูลในรูปแบบอิเล็กทรอนิกส์เข้ามาที่สำนักงานสาธารณสุขจังหวัดนราธิวาสแบบอัตโนมัติตลอดเวลา และมีการประมวลผลข้อมูลให้อยู่ในรูปแบบโครงสร้างมาตรฐาน 21 แฟ้ม

หน่วยบริการสาธารณสุขในจังหวัดนราธิวาสมีการแลกเปลี่ยนข้อมูลการให้บริการสาธารณสุขผ่านเว็บเซอร์วิสระหว่างโรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลอื่นๆ หรือโรงพยาบาลอื่นๆ ในจังหวัดนราธิวาส เพื่อนำข้อมูลไปบริหารจัดการในการดำเนินงานส่งเสริมป้องกันโรคได้อย่างรวดเร็ว และมีประสิทธิภาพมากขึ้น การแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพผ่านระบบเครือข่ายคอมพิวเตอร์ของสถานบริการสาธารณสุขเกิดขึ้นโดยโรงพยาบาลส่งเสริมสุขภาพตำบล และศูนย์บริการสาธารณสุขที่ใช้โปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) ทุกแห่ง มีการสืบค้นข้อมูลของกับเจ้าหน้าที่สาธารณสุขในหน่วยงานสาธารณสุขจังหวัดนราธิวาสต่างๆ เช่น เจ้าพนักงานสาธารณสุข นักวิชาการสาธารณสุข พยาบาล แพทย์ ฯลฯ ที่มีความจำเป็นต้องสืบค้นข้อมูล ในกรณี เช่น โรงพยาบาลส่งเสริมสุขภาพตำบลต้องการทราบประวัติการได้รับภูมิคุ้มกันโรคของเด็กอายุต่ำกว่า 1 ปี ว่ามีการได้รับบริการจากโรงพยาบาลส่งเสริมสุขภาพตำบลอื่น หรือโรงพยาบาลอื่นๆ ครบตามเกณฑ์อายุหรือไม่ หรือแพทย์ในโรงพยาบาลต้องการสืบค้นประวัติการใช้ยาของผู้ป่วยจากโรงพยาบาลอื่นเพื่อให้การรักษาพยาบาลได้อย่างต่อเนื่อง หรือนักวิชาการสาธารณสุขประจำฝ่ายควบคุมโรคติดต่อ สำนักงานสาธารณสุขจังหวัดต้องการข้อมูลประวัติการป่วยของผู้ป่วยที่ป่วยด้วยโรคที่จำเป็นต้องมีการรายงานการสอบสวนโรคและเฝ้าระวังทางระบาดวิทยา

1.1 สถาปัตยกรรมของระบบงานเดิม

โดยเว็บเซอร์วิสในระบบเดิม (PROVIS Web Service) ที่ใช้งานพิจารณาตามแบบจำลองโอเอสไอ (OSI Model) มีรายละเอียดการทำงานและมีการรักษาความปลอดภัยดังนี้

1.1.1 ลำดับชั้นกายภาพ (Physical Layer) มีการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ลูกข่าย (client) และเครื่องคอมพิวเตอร์แม่ข่ายเว็บเซอร์วิส ผ่านเส้นใยแก้วนำแสง (fiber optic) มีการรักษาความปลอดภัยด้วยการรักษาความปลอดภัยทางกายภาพ

1.1.2 ลำดับชั้นเชื่อมโยงข้อมูล (Data link Layer) การรักษาความปลอดภัยใช้สถาปัตยกรรม WAN โปรโตคอล ในการเชื่อมต่อข้อมูล WAN แบบ Connection-oriented รวมกันกับเฟรม และ Secure Sockets Layer (SSL) โปรโตคอล

1.1.3 ลำดับชั้นเครือข่าย (Network Layer) มีการรักษาความปลอดภัยโดยมี Cisco Router ทำการ config ความปลอดภัย

1.1.4 ลำดับชั้นขนส่ง (Transport Layer) มีการรับข้อมูลจากลำดับชั้นเครือข่าย ตรวจสอบ และแก้ไขปัญหาข้อผิดพลาดที่เกิดขึ้นระหว่างการส่ง เพื่อส่งต่อให้กับชั้นส่วนงาน มีการรักษาความปลอดภัยด้วย Secure Sockets Layer (SSL) โปรโตคอล

1.1.5 ลำดับชั้นส่วนงาน (Session Layer) มีการจัดการกับเซสชั่นของโปรแกรม ควบคุมการเชื่อมต่อระหว่างคอมพิวเตอร์หลายตัว บริหารจัดการการเชื่อมต่อการใช้งานระหว่างภายในกับระยะไกล ทำงานแบบ duplex จัดทำวิธีการตรวจสอบ การเสร็จสิ้น การยกเลิกดำเนินการ และการเริ่มต้นใหม่ มีการรักษาความปลอดภัยด้วย NFS Network File System

1.1.6 ลำดับชั้นนำเสนอ (Presentation Layer) มีการเข้ารหัสข้อมูล และกระบวนการแปลแสดงผลให้กับเครื่องคอมพิวเตอร์ลูกข่าย (client) ที่ใช้งานระบบเว็บเซอร์วิส มีการรักษาความปลอดภัยด้วยการแปลงข้อมูลให้อยู่ในรูปแบบ XML

1.1.7 ลำดับชั้นการประยุกต์ (Application Layer) มีการรับคำสั่งต่างๆจากผู้ใช้งาน และดึงข้อมูลมาจากแสดงผลบนหน้าจอโปรแกรมระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล (JHCIS) มีการรักษาความปลอดภัย แต่ชื่อผู้ใช้งานระบบเว็บเซอร์วิสหน่วยบริการเดียวกันมีการใช้งานร่วมกันของเจ้าหน้าที่

การแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสในระบบเดิม (PROVIS Web Service) ผ่านระบบอินเทอร์เน็ตที่ใช้อยู่ขณะนี้ ยังไม่มีมาตรฐานตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ทั้ง 3 ด้าน ที่สมบูรณ์ คือ

1) ด้านการรักษาความลับ (Confidentiality)

มีการเข้าถึงข้อมูลได้โดยผ่านการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านเดียวกันรายหน่วยบริการ และไม่เป็นไปตามมาตรฐานการกำหนดรหัส จำเป็นต้องมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศและการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) ต้องมีการกำหนดรหัสผ่านรายบุคคลร่วมกับฐานข้อมูลระบบบริหารงานบุคคล (PIS) และมีโปรโตคอลที่ปลอดภัย

2) ด้านการคงสภาพของข้อมูล (Integrity)

ต้องมีการป้องกันแม้ว่าจะไม่เคยเกิดปัญหาแต่ก็มีความเสี่ยงที่ข้อมูลสารสนเทศอาจจะถูกแก้ไขโดยความไม่ตั้งใจของผู้ที่เข้าถึงข้อมูล หรือ SQL Injection จำเป็นต้องมีการการควบคุมการเข้าถึงสารสนเทศ (access control) และการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

3) ด้านความพร้อมในการใช้งาน (Availability)

มีความเสี่ยงของข้อมูลสารสนเทศอิเล็กทรอนิกส์ สามารถที่จะถูกลบทำลายได้โดยไวรัสคอมพิวเตอร์ ความผิดพลาดจากการถูกลบโดยไม่ตั้งใจ หรือถูกโจมตีจากภัยคุกคามต่างๆ ทำให้เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการไม่พร้อมใช้งาน จำเป็นต้องมีการควบคุมการเข้าถึงสารสนเทศ และการบริหารจัดการการเข้าถึงของผู้ใช้งาน

การเรียกใช้ข้อมูลหรือแลกเปลี่ยนของข้อมูลหน่วยงานและหน่วยบริการสาธารณสุขต้องมีมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส และข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 และต้องมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540 มาตรา 23 24 และ 25

ด้วยเหตุผลดังกล่าว ผู้วิจัยต้องการออกแบบมาตรฐานความปลอดภัยในการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาสทดแทนระบบเดิมโดยมีเป้าหมายการรักษาความปลอดภัย สร้างกลไกและเครื่องมือในการรักษาความลับของข้อมูลสุขภาพส่วนบุคคล การคงสภาพข้อมูลสารสนเทศ และการเตรียมความพร้อมในการให้บริการเรียกใช้หรือแลกเปลี่ยนข้อมูลตามการร้องขอใน ลำดับชั้นการประยุกต์ (Application Layer) ของแบบจำลองโอเอสไอ (OSI Model) ให้เป็นไปตามข้อกำหนดและนโยบายด้านความปลอดภัย

2. วัตถุประสงค์ของการศึกษา

2.1 เพื่อออกแบบมาตรฐานความปลอดภัย (Security Framework) ของการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคล ของประชาชนในจังหวัดนราธิวาสที่มีการเรียกใช้ข้อมูลผ่านเว็บเซอร์วิส (Web Service) และมีการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคระหว่างระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน(JHCIS) กับระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial Health Information System : PROVIS) ผ่านเครือข่ายอินเทอร์เน็ต

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

3. ขอบเขตของการวิจัย

ในการวิจัยนี้ได้ศึกษาตัวอย่างข้อมูลสารสนเทศสุขภาพจากสำนักงานสาธารณสุขจังหวัดนราธิวาส ที่ให้บริการเรียกใช้ข้อมูลประวัติการรับบริการสาธารณสุข และแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค ด้วยระบบแลกเปลี่ยนข้อมูล (Restful Health Web Service) ผ่านเว็บเซอร์วิสที่ https://healthws.ntwo.moph.go.th/ การศึกษาครั้งนี้มีขอบเขตการศึกษาดังนี้

3.1 ข้อมูลส่วนบุคคลให้บริการเรียกใช้ผ่านเว็บเซอร์วิส จากฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) ได้แก่ ข้อมูลประวัติการรับบริการรักษาพยาบาล ข้อมูลรับบริการการสร้างเสริมภูมิคุ้มกันโรค และการรับบริการดูแลหลังคลอด จากฐานข้อมูลของผู้ป่วยนอกจากระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) ข้อมูลหลัก คือ หมายเลขบัตรประชาชน , คำนำหน้าชื่อ , ชื่อ สกุล ,วันที่รับบริการ และสถานบริการที่ให้บริการ ข้อมูลรายละเอียด ได้แก่

3.1.1 การรับบริการผู้ป่วยนอก**

การวินิจฉัยโรค

ยาและเวชภัณฑ์ที่ใช้

3.1.2 การรับบริการสร้างเสริมภูมิคุ้มกันโรค

ภูมิคุ้มกันโรค ที่ได้รับ

3.1.3 การรับบริการดูแลหลังคลอด

ครรภ์ที่

อายุครรภ์

สถานะครรภ์

3.2 ขอบเขตด้านฮาร์ดแวร์ แบ่งเป็น 2 ส่วน

3.2.1 เครื่องแม่ข่าย (Server) รองรับการให้บริการเว็บเซอร์วิส

3.2.2 เครื่องลูกข่าย (Client) ติดตั้ง Java Development Kit (JDK) 1.7.0 ขึ้นไป และติดตั้ง chrome Internet browser และโปรแกรมคอมพิวเตอร์ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) เวอร์ชัน 2.2.20130809.81 ขึ้นไป

3.3 ขอบเขตด้านซอฟต์แวร์ แบ่งเป็น 2 ส่วน

3.3.1 ระบบปฏิบัติการไม่ต่ำกว่า Windows XP Professional หรือ ไม่ต่ำกว่า Linux CentOS 6.2

3.3.2 เว็บเบราเซอร์ chrome Internet browser

3.3.3 ระบบจัดการฐานข้อมูล MySQL 5.0.51 ขึ้นไป

3.3.4 ภาษาคอมพิวเตอร์ที่ใช้ในการพัฒนา คือ ภาษา PHP, JAVA โดยใช้เครื่องมือ Edit Plus 3.2 และ NetBeans IDE 8.0

3.4 ขอบเขตด้านการแลกเปลี่ยนข้อมูล ระหว่างระบบสารสนเทศ 2 ระบบ

3.4.1 ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS)

3.4.2 ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial health Information System : PROVIS) แฟ้มข้อมูลสร้างเสริมภูมิคุ้มกันโรค

3.5 ขอบเขตเครือข่ายคอมพิวเตอร์ที่ใช้ในการแลกเปลี่ยนข้อมูล คือ เครือข่ายอินเตอร์เน็ตที่ใช้ในการเชื่อมโยงข้อมูลสุขภาพของหน่วยงานและหน่วยบริการของสำนักงานสาธารณสุขจังหวัดนราธิวาส

4. ข้อจำกัดในการวิจัย

การออกแบบและพัฒนาระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws ข้อมูลที่มีการแลกเปลี่ยนกันเต็มรูปแบบ สามารถเพิ่ม ปรับปรุง แก้ไข ลบข้อมูลสุขภาพส่วนบุคคลที่มีการบันทึกรหัสข้อมูลผิดพลาดให้ถูกต้องได้ งานวิจัยนี้มีข้อจำกัดของการเรียกใช้และแลกเปลี่ยนข้อมูลดังนี้

4.1 การเรียกใช้ข้อมูล สามารถเรียกใช้ข้อมูลได้ดังนี้

4.1.1 ประวัติการรับบริการรักษาพยาบาล

4.1.2 ข้อมูลรับบริการการสร้างเสริมภูมิคุ้มกันโรค

4.1.3 ข้อมูลการรับบริการดูแลหลังคลอด

4.2 การแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค 2 กรณี คือ

4.2.1 โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลอื่นๆ ในจังหวัดนราธิวาส

4.2.2 โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลอื่นๆในจังหวัดนราธิวาส

เนื่องจากเป็นข้อมูลที่สามารถบันทึกในลักษณะที่เป็นความครอบคลุมได้ และมีโครงสร้างข้อมูลที่ไม่ซับซ้อนมาก สามารถแลกเปลี่ยนกันได้ทันที ส่วนข้อมูลการรับบริการดูแลหลังคลอดข้อมูลมีความซับซ้อนมาก ยังไม่สามารถแลกเปลี่ยนกันได้เต็มรูปแบบในการปรับปรุงแก้ไขข้อมูล

5. นิยามศัพท์เฉพาะ

5.1 หน่วยบริการสาธารณสุข หมายถึง สถานบริการสาธารณสุขที่ให้บริการสาธารณสุขแก่ประชาชน ได้แก่ ศูนย์สุขภาพชุมชน สถานีอนามัย หรือโรงพยาบาลส่งเสริมสุขภาพตำบล (รพ.สต.) ในปัจจุบัน และโรงพยาบาลทั้งภาครัฐและเอกชนในจังหวัดนราธิวาส

5.2 ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial Health Information System : PROVIS) หมายถึง ระบบฐานข้อมูลสาธารณสุขที่เก็บรวบรวมข้อมูลการให้บริการของหน่วยบริการสาธารณสุขของจังหวัดต่างๆ ในรูปแบบข้อมูลมาตรฐาน 21 แฟ้ม พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

5.1 ระบบข้อมูลผู้ป่วยนอกและส่งเสริมป้องกันโรครายบุคคล (OP/PP Individual Data) หมายถึง ระบบการจัดเก็บข้อมูลการให้บริการของหน่วยบริการสาธารณสุขโดยสำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.) กำหนดให้หน่วยบริการสาธารณสุขทั่วประเทศต้องส่งข้อมูลการให้บริการไปยังสำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.) หลังจากการให้บริการในแต่ละเดือน และจะจ่ายค่าตอบแทนในการจัดส่งข้อมูลให้กับหน่วยบริการสาธารณสุขตามคุณภาพของข้อมูลที่ผ่านการตรวจสอบความถูกต้องแล้ว

5.3 ระบบฐานข้อมูลการบริหารงานบุคคล (Personal Information System : PIS) พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข เป็นระบบการจัดเก็บฐานข้อมูลเจ้าหน้าที่ และบุคลากรสาธารณสุขที่ปฏิบัติงานในหน่วยบริการสาธารณสุขทุกระดับ คือ สำนักงานสาธารณสุขจังหวัด โรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบล โดยกลุ่มงานทรัพยากรบุคคลของสำนักงานสาธารณสุขจังหวัดจะเป็นผู้บันทึกข้อมูลทั้งหมดเข้าไปในระบบ PIS

5.4 Google Chrome Advanced Rest Client คือ เครื่องมือที่ใช้ในการทดสอบเว็บเซอร์วิสแบบ REST พัฒนาโดย GOOGLE สามารถทำการทดสอบออนไลน์บนเครือข่ายอินเตอร์เน็ตและแสดงผลการทดสอบได้แบบเรียลไทม์

5.5 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ลงนามโดยปลัดกระทรวงสาธารณสุข เมื่อวันที่ 7 มกราคม 2556 สามารถดาวน์โหลดได้ที่ http://ops.moph.go.th/download/complete/2556-01-29.pdf

5.6 มาตรฐานการรักษาความปลอดภัย หมายถึง การรักษาความปลอดภัยของสารสนเทศให้มีความปลอดภัยตามหลักการ C.I.A Triangle 3 ด้าน คือ การรักษาความลับ (Confidentiality) การคงสภาพ (Integrity) และสภาพพร้อมสำหรับการใช้งาน (Availability)

6. ขั้นตอนและวิธีดำเนินการวิจัย

6.1 ศึกษาเกี่ยวกับเทคโนโลยีเว็บเซอร์วิส (Web Service) และข้อกำหนดซอฟต์แวร์และมาตรฐานอื่นที่เชื่อมโยงกัน ความปลอดภัยของสารสนเทศ ได้แก่

6.1.1 PHP Slim framework

6.1.2 REST Web Service (Representational State Transfer)

6.1.3 SSL/TLS (Secure Sockets Layer/Transport Layer Security)

6.1.4 WS-Security Tokens / X.509 Certificate

6.1.5 JSON (JavaScript Object Notation)

6.1.6 JAVA Application

6.1.7 C.I.A Triangle

6.2 ออกแบบและสร้างมาตรฐานความปลอดภัย (security framework) ทั้งด้านการบริหารจัดการและด้านเทคนิคของการเรียกใช้และแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพส่วนบุคคลด้วยเว็บเซอร์วิส (Web Service)

6.3 ทดสอบความปลอดภัย (security framework) ของการเรียกใช้และแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพส่วนบุคคลด้วยเว็บเซอร์วิส (Web Service)

6.4 จัดทำสรุปและข้อเสนอแนะสำหรับการดำเนินงานวิจัย

6.5 จัดทำวิทยานิพนธ์

7. ประโยชน์ที่ได้จากการศึกษา

ประโยชน์ที่คาดว่าจะได้รับจากการศึกษามีดังต่อไปนี้

7.1 มีการออกแบบมาตรฐานความปลอดภัย (Security Framework) ของการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคล (ข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค) ของประชาชนในจังหวัดนราธิวาสที่มีการเรียกใช้ข้อมูลสารสนเทศส่วนบุคคลผ่านเว็บเซอร์วิส (Web Service) ของจังหวัดนราธิวาส

7.2 มีการทดสอบมาตรฐานความปลอดภัยที่ออกแบบไว้ เพื่อการคุ้มครองข้อมูลสารสนเทศสุขภาพส่วนบุคคลจากผู้ที่ไม่เกี่ยวข้องกับข้อมูล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 ,8 ,9 และ10 และพระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540 มาตรา 23 ,24 และ 25

8. ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์นี้แบ่งเนื้อหาออกเป็น 5 บทดังต่อไปนี้ บทที่ 1 เป็นบทนำซึ่งกล่าวถึงความเป็นมาและความสำคัญของปัญหา รวมถึงวัตถุประสงค์ของการวิจัย บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้องในงานวิจัยนี้ บทที่ 3 กล่าวถึงการออกแบบมาตรฐานความปลอดภัย (security framework) ของเว็บเซอร์วิส (Web Service) บทที่ 4 กล่าวถึงการพัฒนามาตรฐานความปลอดภัย (security framework) ของเว็บเซอร์วิส (Web Service) และ บทที่ 5 กล่าวถึงสรุปการวิจัยและข้อเสนอแนะ

บทที่ 2
วรรณกรรมที่เกี่ยวข้อง

การศึกษาวิจัยเรื่อง การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาสนี้ ได้อาศัยหลักการความมั่นคงปลอดภัยของสารสนเทศ ซึ่งผู้วิจัยได้ศึกษาค้นคว้าแนวคิดทฤษฎี จากเอกสารและงานวิจัยที่เกี่ยวข้อง ซึ่งจำแนกรายละเอียดของเนื้อหารายละเอียดดังนี้

1. ระบบสารสนเทศของสำนักงานสาธารณสุขจังหวัดนราธิวาส
2. การเรียกใช้ข้อมูลของสถานบริการสาธารณสุขในจังหวัดนราธิวาส
3. ความมั่นคงปลอดภัยของสารสนเทศสุขภาพ
4. มาตรฐานการรักษาความปลอดภัยของการเรียกใช้ข้อมูลสารสนเทศที่นำมาใช้ในการออกแบบ
5. การทดสอบความปลอดภัยและความถูกต้องฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST
6. แนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา
7. กฎหมายที่เกี่ยวข้อง
8. งานวิจัยที่เกี่ยวข้อง

1. ระบบสารสนเทศของสถานบริการสาธารณสุขในจังหวัดนราธิวาส

1.1 ระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบล

ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล และศูนย์สุขภาพชุมชน (Java Health Center Information System: JHCIS) เป็นโปรแกรมคอมพิวเตอร์ Open Source สำหรับบันทึกข้อมูลการให้บริการของโรงพยาบาลส่งเสริมสุขภาพตำบล และศูนย์สุขภาพชุมชน พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข JHCIS เป็นโปรแกรมระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน ที่ใช้งานได้ครอบคลุมข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบลได้อย่างเป็นระบบสะดวกรวดเร็วและมีประสิทธิภาพและ

ตอบสนองต่อรายงานต่างๆ ทั้งที่ส่วนกลางและส่วนภูมิภาคต้องการ สามารถใช้งานได้บนระบบปฏิบัติการทั้ง Windows, Ubuntu, Linux ฯลฯ โดยใช้เทคโนโลยี Open Source Technology ทั้งหมด ปัจจุบันมีโรงพยาบาลส่งเสริมสุขภาพตำบล ทั้งหมด 111 แห่ง และ ศูนย์บริการสาธารณสุขของจังหวัดนราธิวาส จำนวน 1 แห่ง ใช้ระบบงานนี้

1.2 ระบบสารสนเทศของโรงพยาบาลและศูนย์สุขภาพชุมชน

ระบบสารสนเทศโรงพยาบาล (Hospital Experience: HOSxP) ฮอสเอกซ์พีเป็นซอฟต์แวร์แอปพลิเคชัน สำหรับโรงพยาบาล พัฒนาโดยบุคลากรที่อาสาสมัครมาจากหลายโรงพยาบาล ริเริ่มโดย เภสัชกรชัยพร สุรเตมีย์กุล โดยเป็นโครงการทดลองพัฒนาระบบสารสนเทศใช้เองภายในโรงพยาบาลเขาสวนกวาง จังหวัดขอนแก่น เพื่อเพิ่มประสิทธิภาพในการให้บริการผู้ป่วย และช่วยลดภาระในการทำรายงานประจำเดือนของฝ่ายต่างๆ โครงการเริ่มพัฒนาเมื่อกลางปี พ.ศ. 2542 โดยเริ่มต้นพัฒนา ระบบเวชระเบียน เป็นระบบแรก ตามด้วยระบบผู้ป่วยใน และระบบห้องจ่ายยา ปัจจุบันได้มีอาสาสมัครจากหลายโรงพยาบาล มาช่วยทดสอบและพัฒนา และมีผู้นำโครงการคือ เภสัชกรชัยพร สุรเตมีย์กุล - ปัจจุบันทำงานใน บริษัทบางกอกเมดิคัลซอฟต์แวร์ จำกัด (ซึ่งทำหน้าที่เป็นผู้จัดการโครงการ และผู้พัฒนาหลัก) โรงพยาบาลในจังหวัดนราธิวาส ทั้งหมด 13 แห่ง และศูนย์สุขภาพชุมชนของโรงพยาบาล จำนวน 5 แห่งใช้ระบบงานนี้ ที่มาของข้อมูลการรับบริการสาธารณสุขของโรงพยาบาลและศูนย์สุขภาพชุมชนเหมือนกับโรงพยาบาลส่งเสริมสุขภาพตำบล

1.3 ระบบบริหารงานบุคคล (PIS)

โปรแกรมระบบบริหารงานบุคคลส่วนภูมิภาค (Personal Information System : PIS) พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตั้งแต่ปีงบประมาณ 2538 ทำงานบนระบบปฏิบัติการ Windows ซึ่งสามารถทำงานได้ทั้งบนเครื่องเดี่ยว (Stand alone) และแบบ client/server ระบบจัดการฐานข้อมูลที่ใช้มีลิขสิทธิ์มาเป็นตัวจัดการฐานข้อมูล และแจกจ่ายโปรแกรมที่ได้พัฒนาในรูปแบบของโปรแกรมสำเร็จรูปให้แก่หน่วยงานในส่วนภูมิภาค ได้แก่ สำนักงานสาธารณสุขจังหวัด โรงพยาบาลศูนย์ โรงพยาบาลทั่วไป เป็นต้น ปัจจุบันได้ติดตั้งใช้งานในการจัดเก็บข้อมูลบุคลากรที่ปฏิบัติงานในสังกัดสำนักงานสาธารณสุขจังหวัดนราธิวาส ได้แก่ สำนักงานสาธารณสุขจังหวัด สำนักงานสาธารณสุขอำเภอ โรงพยาบาล โรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน โครงสร้างฐานข้อมูลระบบจัดการฐานข้อมูล PostgesSQL มีฟังก์ชั่นการทำงานเพื่อรองรับกับโปรแกรมอื่นๆ ที่เกี่ยวข้องและครอบคลุมในการใช้งาน เช่น ข้อมูลเกี่ยวกับแพทย์เฉพาะทาง/การลาศึกษาต่อ การประชุม/อบรม/สัมมนา

1.4 ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS)

ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (Provincial Health Information System: PROVIS) เป็น ระบบฐานข้อมูลสาธารณสุขที่เก็บรวบรวมข้อมูลการให้บริการของหน่วยบริการสาธารณสุขของจังหวัดนราธิวาสในรูปแบบข้อมูลมาตรฐาน 21 แฟ้ม (รายละเอียดในบทที่ 3) พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ซึ่งสำนักงานสาธารณสุขจังหวัดนราธิวาสจะต้องทำการส่งต่อข้อมูลรูปแบบข้อมูลมาตรฐาน 21 แฟ้ม ไปยังหน่วยงานส่วนกลาง ภายใน 30 วัน เป็นประจำทุกเดือน จำนวน 2 หน่วยงาน คือ 1) สำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข และ 2) สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.)

2. การเรียกใช้ข้อมูลของสถานบริการสาธารณสุขในจังหวัดนราธิวาส

ระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล และศูนย์สุขภาพชุมชนจะทำการเรียกใช้และแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพ กับระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข ผ่านเว็บเซอร์วิส เฉพาะข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค ของประชาชนที่ขึ้นทะเบียนการรับบริการในเขตรับผิดชอบของโรงพยาบาลส่งเสริมสุขภาพตำบล โดยข้อมูลดังกล่าวต้องอยู่ในรูปแบบโครงสร้างรูปแบบ 21 แฟ้มมาตรฐาน เวอร์ชั่น 5.0 วันที่ 1 ตุลาคม 2555 ตามประกาศของสำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข ตัวอย่างที่มาของข้อมูลการรับบริการสาธารณสุขมีที่มาดังนี้

ข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค เจ้าหน้าที่สาธารณสุขผู้ให้บริการจะทำการบันทึกข้อมูลรับบริการสร้างเสริมภูมิคุ้มกันโรค หลังจากมีการให้บริการผู้มารับบริการเรียบร้อยแล้ว ข้อมูลที่ต้องบันทึกเข้าไปในระบบ มี 2 กรณี ดังนี้

1) ผู้รับบริการมารับบริการที่โรงพยาบาลส่งเสริมสุขภาพตำบล ณ เวลานั้น ข้อมูลที่บันทึกประกอบด้วยชนิดของภูมิคุ้มกันโรคที่ได้รับบริการ วันที่มารับบริการ วันที่นัดมารับบริการสร้างเสริมภูมิคุ้มกันโรคครั้งต่อไป (ถ้ามี)

2) ผู้รับบริการมารับบริการที่โรงพยาบาลส่งเสริมสุขภาพตำบล ณ เวลานั้น แต่จากการตรวจดูสมุดประจำตัวผู้รับบริการสร้างเสริมภูมิคุ้มกันโรค พบว่าได้รับบริการสร้างเสริมภูมิคุ้มกันโรค จากหน่วยบริการอื่นมาแล้วก่อนหน้า จะต้องบันทึกข้อมูลชนิดของภูมิคุ้มกันโรคที่ได้รับบริการ วันที่มารับบริการ และหน่วยบริการที่ได้รับบริการสร้างเสริมภูมิคุ้มกันโรค กรณีที่ได้รับบริการสร้างเสริมภูมิคุ้มกันโรค มาจากหน่วยบริการอื่นแล้ว

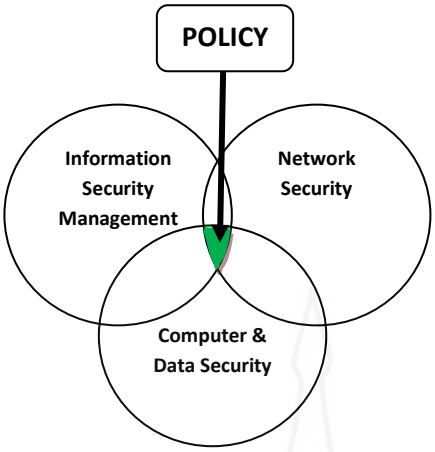
การเรียกใช้และแลกเปลี่ยนข้อมูลของสถานบริการสาธารณสุขในจังหวัดนราธิวาส สามารถทำได้โดยสถานบริการทุกแห่งที่มีการเชื่อมต่อระบบอินเตอร์เน็ต ตามที่ได้กล่าวในหน่วยที่ 1 การเรียกใช้ข้อมูลหรือแลกเปลี่ยนของข้อมูลหน่วยงานและหน่วยบริการสาธารณสุขต้องมีมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส และข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 และต้องมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540 มาตรา 23 24 และ 25 ทำให้ข้อมูลข้อมูลสุขภาพไม่มีความมั่นคงปลอดภัยตามหลัก C.I.A Triangle

3. ความมั่นคงปลอดภัยของสารสนเทศสุขภาพ

ข้อมูลสารสนเทศเป็นทรัพยากรที่มีค่าขององค์กร (บุญฤทธิ์ คิดหงัน: 2554) การรักษาความปลอดภัยให้กับข้อมูลสารสนเทศ หมายถึง สถานะที่ทำให้ข้อมูลสารสนเทศมีความปลอดภัยอยู่ในสถานะที่ไม่มีอันตราย และได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ การรักษาปลอดภัย (security) ของข้อมูลสารสนเทศ เป็นการรักษาคุณค่าพื้นฐานโดยหลัก 3 ประการ (CIA) คือ การรักษาความลับ (Confidentiality) การคงสภาพ (Integrity) และสภาพพร้อมสำหรับการใช้งาน (Availability) ข้อมูลสารสนเทศต้องได้รับการปกป้องจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้นและมีความประสงค์ร้ายต่อข้อมูลสารสนเทศ เช่น การปลอมแปลง เปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศ หรือการลักลอบทำสำเนาข้อมูล

ความมั่นคงปลอดภัยของสารสนเทศ (Information Security) คือ การป้องกันสารสนเทศและองค์ประกอบอื่นๆ ที่เกี่ยวข้อง ซึ่งรวมถึงระบบฮาร์ดแวร์ที่ใช้ในการจัดเก็บและโอนสารสนเทศนั้นด้วย

จากนิยามความมั่นคงปลอดภัยของสารสนเทศข้างต้น สามารถอธิบายได้ด้วยภาพที่ 2.1

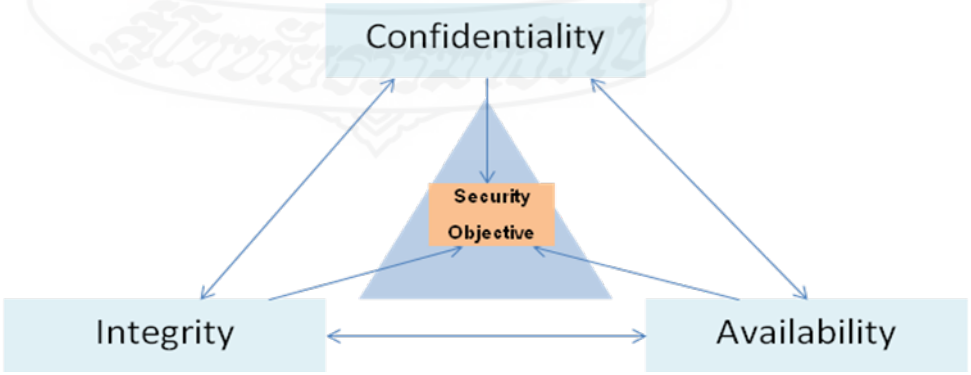


ภาพที่ 2.1 นิยามความมั่นคงปลอดภัยของสารสนเทศ

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

แนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ C.I.A Triangle ถูกกำหนดขึ้นโดยกลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้มีการกำหนดขึ้น ประกอบด้วยการรักษาความลับ (Confidentiality) การคงสภาพ (Integrity) และสภาพพร้อมสำหรับการใช้งาน (Availability)

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย : 2555) ได้นิยามความหมายของการรักษาความปลอดภัยทางข้อมูล Information Security ไว้ว่า การรักษาความปลอดภัยทางข้อมูลคือผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/ หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุมและป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต



ภาพที่ 2.2 C.I.A Triangle

จากภาพที่ 2.2 C.I.A Triangle มีองค์ประกอบที่สำคัญ 3 องค์ประกอบ คือ

3.1 การรักษาความลับของสารสนเทศ (Confidentiality)

ผู้ที่มีสิทธิ์ใช้สารสนเทศจะต้องได้รับสิทธิในการใช้เท่านั้น (มหาวิทยาลัยกรุงเทพ: 2554) การเปิดเผยข้อมูลที่จะต้องได้รับอนุญาตและจะทำโดยผู้มีสิทธิ์เท่านั้น การดำเนินการด้าน Confidentiality จะใช้วิธี Identification คือการระบุตัวตน การระบุตัวเป็นเป็นการยืนยันว่าผู้ใช้มีตัวตนจริงๆ เช่น การใช้หมายเลขบัตรประจำตัวประชาชน หรือ การใช้ Username การรักษาความลับของสารสนเทศเป็นการรับประกันว่า ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ สารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต จะถือเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับด้วยวิธีการต่างๆ เช่น

- การจัดประเภทของสารสนเทศ
- การรักษาความปลอดภัยให้กับแหล่งข้อมูล
- การกำหนดนโยบายความมั่นคงปลอดภัยและนำไปใช้งาน
- การให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและนำไปใช้

การรักษาความลับจะต้องไม่เปิดเผยข้อมูลของผู้ป่วยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ข้อมูลการเจ็บป่วยด้วยโรคบางโรค เช่น โรคภาวะภูมิคุ้มกันบกพร่องหรือเอดส์ หากมีการเปิดเผยให้กับผู้ร่วมงาน อาจส่งผลกระทบให้ต้องถูกออกจากงาน หรือถูกบีบให้ออกจากงาน หรือส่งผลกระทบต่อบุคคลในครอบครัว ข้อมูลอื่นๆ เช่น ประวัติการใช้ยาหรือสารเสพติด ประวัติการรักษาทางจิตเวช ประวัติโรคประจำตัว หรือโรคเรื้อรัง ประวัติโรคทางพันธุกรรม มีผลกระทบในทางร้ายแรงต่อเจ้าของข้อมูลที่ถูกเปิดเผยทั้งสิ้น และสามารถที่จะส่งผลกระทบถึงแก่ชีวิตได้ ผู้ที่ดูแลรับผิดชอบข้อมูลจะต้องมีการออกแบบการเข้าถึงข้อมูลในส่วนที่เกี่ยวกับการดำเนินการรักษาพยาบาลและเป็นประโยชน์ต่อผู้ป่วยเท่านั้น

3.2 ความคงสภาพของสารสนเทศ (Integrity)

ผู้ที่มีสิทธิ์เปลี่ยนแปลงข้อมูลจะใช้สิทธิ์ของตัวเองเท่าที่ได้รับจากผู้ดูแลระบบ จะมีสิทธิ์มากกว่านั้นไม่ได้ สารสนเทศต้องอยู่ในสภาพที่ถูกต้องคงสภาพเดิมตามความต้องการของผู้ใช้ หากระบบมีความขัดข้อง จะต้องกู้คืนข้อมูลขึ้นมาให้บริการในสภาพเป็นสารสนเทศที่คงสภาพเดิม วิธีดำเนินการด้านคงสภาพของสารสนเทศ หมายถึง ความคงสภาพของสารสนเทศและปราศจากสิ่งแปลกปลอมที่ปนมาในสารสนเทศนั้น (บุญฤทธิ์ คิดหงัน: 2554) ดังนั้น สารสนเทศที่มีความคงสภาพเท่านั้น ที่จะสามารถนำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน เช่น ไม่ถูกทำให้เสียหาย มีการเปลี่ยนแปลงแก้ไขสารสนเทศ เนื่องจาก virus, worm หรือ Hacker ทำการปลอมปน สร้าง

ความเสียหายให้กับข้อมูลขององค์กรได้ การแก้ไขยอดเงินในบัญชีธนาคาร หรือ แก้ไขราคาในการสั่งซื้อ จะทำให้สารสนเทศนั้นขาดความคงสภาพ การนำสารสนเทศนั้นไปเปลี่ยนแปลง แก้ไข ปลอมปนด้วยสารสนเทศอื่น เกิดความเสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่นๆ ผิดไปจากสารสนเทศเดิม

ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุหลักมาจากความเจริญก้าวหน้าทางเทคโนโลยี ประกอบกับพฤติกรรมความต้องการความสะดวกสบาย และความรวดเร็วในการสั่งซื้อสินค้าของตัวลูกค้าเอง ทำให้มีความจำเป็นต้องยอมมอบสารสนเทศส่วนบุคคลให้กับเว็บไซต์ เพื่อให้ผู้ขายสินค้ามีสิทธิ์ในการทำธุรกรรมต่างๆ แทนลูกค้า โดยไม่คำนึงว่าเว็บไซต์นั้นจะนำข้อมูลของลูกค้าไปใช้ทำธุรกรรมอื่นที่ลูกค้าไม่ยินยอม ภัยคุกคามที่เกี่ยวกับความคงสภาพของข้อมูลสุขภาพ ต้องมีการป้องกันการแก้ไข เปลี่ยนแปลงข้อมูลที่เกี่ยวกับผู้ป่วยให้มีความถูกต้องและคงสภาพเป็นข้อมูลเดิม เพื่อเป็นข้อมูลประกอบในการให้บริการรักษาพยาบาลผู้ป่วยให้ทุเลาอาการหรือหายจากการเจ็บป่วยโดยเร็ว

3.3 ความพร้อมใช้งานของสารสนเทศ (Availability)

ความพร้อมใช้ของสารสนเทศ หมายถึง สารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น ไม่ติดขัด โดยผู้ใช้ระบบเฉพาะที่ได้รับอนุญาตเท่านั้น (บุญฤทธิ์ คิดหงัน: 2554) หากเป็นผู้ใช้ระบบที่ต้องการเข้าใช้งานระบบด้วยวิธีการที่ไม่ถูกต้องหรือช่องทางที่ไม่ได้รับอนุญาต การเข้าถึงระบบก็จะล้มเหลวและถูกขัดขวาง เช่น การป้องกันข้อมูลสุขภาพส่วนบุคคล ข้อมูลสารสนเทศจะพร้อมใช้ต่อผู้ใช้ที่เฉพาะได้รับอนุญาต คือ เจ้าของข้อมูลหรือเจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องเท่านั้น ดังนั้น จึงต้องมีการระบุตัวตน (Identification) ว่าเป็นเจ้าของข้อมูลหรือเจ้าหน้าที่ และพิสูจน์ได้ว่าได้รับอนุญาตจริง (Authorization) การทำสำรองข้อมูลจากฐานข้อมูล โดยอาจจะแบ่ง Database Server แบบกระจาย ถ้าหากว่ามีระบบใดระบบหนึ่งล่ม ข้อมูลจากอีกระบบก็สามารถใช้งานได้ ศูนย์ข้อมูลสารสนเทศสุขภาพหรือศูนย์สารสนเทศสามารถนำแนวคิด C.I.A. มาตรวจสอบความมั่นคงปลอดภัยทางสารสนเทศภายในองค์กรเพื่อหาจุดบกพร่องต่างๆที่อาจจะเกิดขึ้นมาได้

ความพร้อมใช้ของข้อมูลสุขภาพจะต้องให้บริการข้อมูลได้ทุกครั้งที่มีการเรียกใช้ มีการอนุญาตให้เข้าถึงข้อมูลได้ตามสิทธิ (Authorization) ต้องมีการป้องกันการสูญหายของข้อมูลจากผู้ที่ไม่เกี่ยวข้องหรือไวรัสคอมพิวเตอร์เข้าไปทำลายข้อมูลนั้น รวมทั้งการบำรุงรักษาหรือออกแบบความปลอดภัยให้กับระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ตลอดเวลา

4. มาตรฐานการรักษาความปลอดภัยของการเรียกใช้ข้อมูลสารสนเทศที่นำมาใช้ในการออกแบบ

มาตรฐานการรักษาความปลอดภัยที่นำมาใช้เป็นมาตรฐานที่เกิดขึ้นจากการใช้งาน (De facto) เป็นมาตรฐานที่เกิดขึ้นจากการใช้งานที่ยอมรับจากคนทั่วไป (สิทธิศักดิ์ สายเงิน: 2556) ซึ่งหน่วยบริการในสำนักงานสาธารณสุขจังหวัดนราธิวาสยอมรับมาตรฐานนี้ ทั้งการบริหารจัดการโดยใช้นโยบายด้านความมั่นคง (สิทธิศักดิ์ สายเงิน: 2556) และ ด้านเทคนิค โดยทั้ง 2 ส่วนมีความเกี่ยวเนื่องกัน

4.1 การออกแบบมาตรฐานความปลอดภัยโดยการบริหารจัดการการใช้ข้อมูล

การรักษาความปลอดภัยให้กับสารสนเทศที่มีการให้บริการแบบออนไลน์ที่สำคัญมาก คือการพิสูจน์ว่าผู้ใช้ที่กำลังใช้งานอยู่คือใคร มีสิทธิ์และขอบเขตในการเข้าใช้ระบบเพียงใด โดยผ่านการพิสูจน์ตัวตน การระบุตัวตนเพื่อเข้าสู่ระบบและการให้สิทธิ์ใช้งานระบบ

การพิสูจน์ตัวตน (Authentication) คือ กระบวนการในการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่ต้องการเข้าไปใช้งานระบบ มีขั้นตอนสำคัญ 2 ขั้นตอน คือ ขั้นตอนการระบุตัวตน (Identification) เป็นขั้นตอนที่ผู้ใช้งานแสดงหลักฐานว่าตัวผู้ใช้งานเป็นใคร โดยใช้ข้อมูลสำคัญที่มีอยู่ของบุคคล เช่น ชื่อผู้ใช้งาน (username) และขั้นตอนการตรวจสอบหลักฐานเพื่อพิสูจน์ว่าเป็นตัวบุคคลที่จะเข้าใช้งาน (Authentication) ที่ต้องการเข้าใช้งานจริง ต้องผ่านการบตรวจสอบผู้ที่เข้ามาใช้งานระบบทั่วไป โดยระบบจะทำการตรวจสอบจากผู้ใช้งาน และ รหัสผ่านว่าถูกต้องตรงกับข้อมูลที่ให้ไว้กับระบบหรือไม่ วัตถุประสงค์หลักเพื่อพิสูจน์ตัวบุคคล ว่าผู้ใช้งานที่เข้าใช้งานระบบเป็นใคร หากผ่านขั้นตอนการพิสูจน์ตัวตน ก็จะเข้าสู่ขั้นตอนการตรวจสอบสิทธิ์ว่าบุคคลนั้นมีขอบเขต และสิทธิ์ใช้งานระบบได้แค่ไหน

การพิสูจน์ตัวตน เป็นวิธีการที่ผู้รับข้อมูลสามารถระบุตัวตนหรือที่มาของข้อมูลได้ว่าผู้ใดเป็นผู้ส่งข้อมูล ซึ่งทำให้ตัดสินใจได้ว่าข้อมูลที่ได้รับมามีความปลอดภัยและน่าเชื่อถือมากน้อยเพียงใด ซึ่งวิธีการที่นิยมใช้ระบุตัวตน คือการให้ผู้ใช้กรอกชื่อผู้ใช้งาน และรหัสผ่านก่อนเข้าสู่ระบบ

ขั้นตอนของการพิสูจน์ตัวตน (Authentication) ในการเข้าใช้งานระบบ มี 2 ขั้นตอน คือ การระบุตัวตน (Identification) และการพิสูจน์ตัวตน (Authentication)

– การระบุตัวตน (Identification) เป็นขั้นตอนที่ผู้ใช้งานจะต้องแสดงหลักฐานว่าผู้ใช้งานเป็นใคร โดยทั่วไปจะใช้ ชื่อผู้ใช้ (username) ในทางกายภาพการระบุตัวตน อาจใช้สิ่งของหรือข้อมูลเฉพาะบุคคลเพื่อ ให้สามารถแยกความแตกต่าง หรือระบุได้ว่าบุคคลนั้นเป็นใคร

หลักฐานที่ใช้ เช่น บัตรประจำตัวประชาชน ชื่อและนามสกุล รูปลักษณ์ของแต่ละบุคคล แผลเป็น หลักฐานทางร่างกายจากการให้บริการทันตกรรม

– การพิสูจน์ตัวตน (Authentication) เป็นขั้นตอนเพื่อตรวจสอบหลักฐานเพื่อยืนยันว่าเป็นบุคคลที่ผ่านการระบุตัวตนตามที่อ้างจริง (ชฎาวัลย์ สิงห์อินทร์: 2550) องค์ประกอบในการพิสูจน์ตัวตน (Authentication mechanisms) มีคุณลักษณะ ที่สำคัญ 3 คุณลักษณะคือ

1) สิ่งที่ตัวตนต้องมี (Possession factor) จำเป็นต้องมี ชื่อผู้ใช้

2) สิ่งที่ตัวตนต้องรู้ (Knowledge factor) จำเป็นต้องรู้ รหัสผ่าน

3) สิ่งที่ตัวตนเป็นอยู่ (Biometric factor) เป็นลักษณะทางกายภาพ เช่น รูปแบบของลายนิ้วมือ รูปแบบของม่านตา (retinal patterns) หรือใช้รูปแบบของเสียง (voice patterns) เป็นต้น

เพื่อให้กระบวนการพิสูจน์ตัวตนมีความแม่นยำมากที่สุด จำเป็นจะต้องนำ 3 ลักษณะมาตรวจสอบร่วมกันเพื่อการยืนยันหลักฐานที่แสดงก่อนการเข้าใช้งานระบบ หากใช้ลักษณะอย่างหนึ่งอย่างใด (Single-factor authentication) เพียงอย่างเดียว ในการใช้งานจริงจะมีข้อจำกัดในการใช้ เช่น สิ่งที่ตัวตนมี (Possession factor) นั้นอาจผู้ใช้งานอาจลืมชื่อผู้ใช้งาน หรือชื่อผู้ใช้งานถูกผู้ไม่หวังดีขโมยไป เช่นเดียวกับสิ่งที่ตัวตนรู้ (Knowledge factor) อาจจะถูกขโมยข้อมูล หรือแอบนำไปใช้ สิ่งที่ตัวตนเป็นอยู่ (Biometric factor) ของบุคคล มีความปลอดภัยมากที่สุด แต่เทคโนโลยีที่จะนำมาใช้งานในขณะนี้มีมูลค่าสูงมากในปัจจุบัน

การให้สิทธิ์ (Authorization) หมายถึง การกำหนดสิทธิ์ให้กับผู้ใช้ที่ผ่านการพิสูจน์ตัวตนว่าสามารถเข้าถึงทรัพยากรที่อยู่ในระบบสารสนเทศได้ เช่น ผู้ใช้สามารถเข้าถึงข้อมูลอะไรได้บ้าง สามารถลบ หรือแก้ไขข้อมูลได้หรือไม่ เป็นต้น นอกจากนี้ยังอาจมีการจัดกลุ่มของผู้ใช้เพื่อแบ่งว่าผู้ใช้แต่ละกลุ่มได้รับสิทธิ์อะไรบ้าง โดยผู้ใช้ที่เป็นผู้ดูแลระบบ (Administrator) จะมีสิทธิ์เข้าถึงส่วนต่างๆ ของระบบได้สูงสุด

ในการรักษาความปลอดภัยให้กับสารสนเทศหากมีการนำเอาการพิสูจน์ตัวตน (Authentication) และการให้สิทธิ์ (Authorization) เข้ามาใช้งานร่วมกันก็จะทำให้สารสนเทศมีความมั่นคงปลอดภัยตามหลักการ C.I.A Triangle คือ การรักษาความลับ (Confidentiality) การคงสภาพ (Integrity) และสภาพพร้อมสำหรับการใช้งาน (Availability) มากยิ่งขึ้น

4.2 มาตรฐานการรักษาความปลอดภัยของเว็บเซอร์วิสที่นำมาในการเรียกใช้ข้อมูลด้านเทคนิค

มาตรฐานการรักษาความปลอดภัยด้านเทคนิคนี้เป็นผลสืบเนื่องจากมาตรฐานจากการบริหารจัดการการใช้ข้อมูลโดยใช้นโยบายด้านความมั่นคงของข้อมูลสารสนเทศ

4.2.1 PHP Slim Framework

PHP Slim Framework เป็น PHP Framework ที่มีกลไกการทำงานที่ง่าย ไม่ซับซ้อน แต่ประสิทธิภาพสูง บางครั้งเรียกว่า Micro Framework เหมาะสำหรับการนำมาใช้พัฒนา Web Application ที่เป็น RESTful APIs. ได้ ส่วนประกอบที่สำคัญประกอบด้วย

slim/slim เป็น Core หลัก

slim/views เป็น Custom View Class สำหรับเรียกใช้กับ Templates ภายนอก

twig/twig เป็น Templates

illuminate/database เป็นส่วนที่ทำงานกับข้อมูล (Database)

ในการรักษาความปลอดภัยของการแลกเปลี่ยนข้อมูล สามารถสร้างคีย์ API ลับ และมอบให้กับผู้เรียกใช้ จากนั้นผู้ใช้จะต้องใช้คีย์ลับในการสร้างและต่อท้ายลายเซ็นสำหรับการร้องขอข้อมูลจาก web service ซึ่งจะต้องมีการตรวจสอบทุกครั้งก่อนเข้าใช้ข้อมูล โดยคีย์ลับนี้สามารถเปลี่ยนแปลงได้ตลอดเวลา

4.2.2 SSL/TLS : มาตรฐานการรักษาความปลอดภัยของเว็บเซอร์วิส

เอสเอสแอล หรือ SSL เป็นคำย่อมาจาก ซีเคียวซอคเก็ตเลเยอร์ หรือ Secure Sockets Layer และทีแอลเอส หรือ TLS ซึ่งเป็นคำย่อมาจากทรานสพอร์ตเลเยอร์ซีเคียวริตี้ หรือ Transport Layer Security ทั้ง SSL และ TSL เป็นมาตรฐานการรักษาความปลอดภัยแบบ de facto ซึ่งถูกพัฒนาโดยเนสเคป หรือ Netscape เมื่อปี 1996 และเป็นพื้นฐานสำหรับมาตรฐาน (สิทธิศักดิ์ สายเงิน: 2556) มาตรฐานถัดมาคือ TLS ซึ่งถ้าเปรียบเทียบกับระดับชั้นการทำงานของโปรโตคอลที่รู้จักกันแพร่หลายแล้วนั้น SSL/TLS จะทำงานอยู่ระหว่างชั้นทีซีพีกับเอชทีทีพี ดังภาพที่ 2.3

ภาพที่ 2.3 เอสเอสแอลและทีแอลเอส บนอินเตอร์เน็ตแสต็ค

ที่มา: สิทธิศักดิ์ สายเงิน (2556)

SSL/TLS ทำให้การสื่อสารของเซสชันแบบจุดต่อจุดมีความปลอดภัยโดยให้มีการพิสูจน์ตัวตนของผู้ให้บริการว่ามีตัวตนจริง การรับรองเอกสาร/ข้อความ การป้องกันความลับข้อมูล และการคงสภาพข้อมูล ในส่วนของ TLS นั้น ได้ให้ทางเลือกในการทำแคชของเซสชัน (session caching) เพื่อลดจำนวนการเชื่อมต่อให้น้อยลง การปรับปรุงประสิทธิภาพของการเชื่อมต่อนี้ มีวัตถุประสงค์ที่จะลดเวลาในการประมวลผลสำหรับการเข้ารหัสโดยเฉพาะ ในส่วนที่เข้ารหัสด้วยกุญแจสาธารณะ (Public keys)

วิธีการทำงาน SSL เป็นโปรโตคอลที่อยู่ระหว่าง Application layer และ Transport layer SSL สามารถรองรับการทำงานกับ application โปรโตคอลต่างๆ เช่น HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), Telnet, POP3, SMTP หรือแม้แต่ VPN ได้ SSL ทำงานโดยอาศัยหลักการของการเข้ารหัสข้อมูล (encryption), Message Digests และลายเซ็นอิเล็กทรอนิกส์ (digital signature) โดยแบ่งหน้าที่ออกเป็น 3 ส่วน

1. การตรวจสอบ server ว่าเป็นตัวจริง ตัวโปรแกรม client ที่มีขีดความสามารถในการสื่อสารแบบ SSL จะสามารถตรวจสอบเครื่อง server ที่ตนกำลังจะไปเชื่อมต่อได้ว่า server นั้นเป็น server ตัวจริงหรือไม่ โดยใช้เทคนิคการเข้ารหัสแบบ public key ในการตรวจสอบใบรับรอง (Certificate) และ Public ID ของ server นั้น (โดยที่มีองค์กรที่ Client เชื่อถือเป็นผู้ออกใบรับรองและ public ID ให้แก่ server นั้น) หน้าที่นี้ของ SSL เป็นหน้าที่ที่สำคัญ โดยเฉพาะอย่างยิ่งในกรณีที่ client ต้องการที่จะส่งข้อมูลที่เป็นความลับ (เช่น หมายเลข Credit card) ให้กับ server ซึ่ง Client จะต้องตรวจสอบก่อนว่า Server เป็นตัวจริงหรือไม่

2. การตรวจสอบว่า client เป็นตัวจริงหรือไม่ โดยจะตรวจสอบใบรับรองและ Public ID (ที่มีองค์กรที่ Server เชื่อถือเป็นผู้ออกให้) ของ Client หรือผู้ใช้นั้นServer ที่สามารถสื่อสารแบบ SSL ได้นั้นจะตรวจสอบว่าหน้าที่นี้ของ SSL จะมีประโยชน์ในกรณีเช่น ธนาคารต้องการที่จะส่งข้อมูลลับทางการเงินให้แก่ลูกค้าของตนผ่านทางเครือข่าย Internet (Server ก็จะต้องตรวจสอบ Client ก่อนว่าเป็น Client นั้นจริง)

3. การเข้ารหัสลับการเชื่อมต่อ โดยข้อมูลทั้งหมดที่ถูกส่งระหว่าง Client และ Server จะถูกเข้ารหัสลับ โดยโปรแกรมที่ส่งข้อมูล เป็นผู้เข้ารหัสและโปรแกรมที่รับข้อมูลเป็นผู้ถอดรหัส (โดยใช้วิธี Public key) นอกจากการเข้ารหัสลับในลักษณะนี้แล้ว SSL ยังสามารถปกป้องความถูกต้องสมบูรณ์ของข้อมูลได้อีกด้วย อีกทั้ง ตัวโปรแกรมรับข้อมูลจะทราบได้หากข้อมูลถูกเปลี่ยนแปลงไปในขณะกำลังเดินทางจากผู้ส่งไปยังผู้รับ

ในภาพรวมแล้ว SSL/TLS ให้ความปลอดภัยดังนี้

1) การรักษาความลับโดยใช้การเข้ารหัสข้อมูลแบบสมมาตร (Symmetric Cryptography) เช่น DES ,RC4

2) การคงสภาพข้อความโดยใช้ Message Authentication Code (MAC) เป็นการบล็อกข้อมูลขนาดเล็กที่แนบไปกับเอกสารที่จะส่ง การสร้าง MAC นี้จะใช้การเข้ารหัสแบบแฮชที่เรียกว่า MD5 โดยวิธีการแฮชเป็นวิธีที่นำเอาตัวเลขหรือข้อความมาผ่านกรรมวิธีทางคณิตศาสตร์แล้วได้ผลลัพธ์ออกมาเป็นตัวเลขชุดหนึ่ง ตัวอย่าง เช่น x = HASH(“Hello World”) ได้ค่าเป็น 3452

ภาพที่ 2.4 การเข้ารหัสเฉพาะชั้นขนส่งเท่านั้น

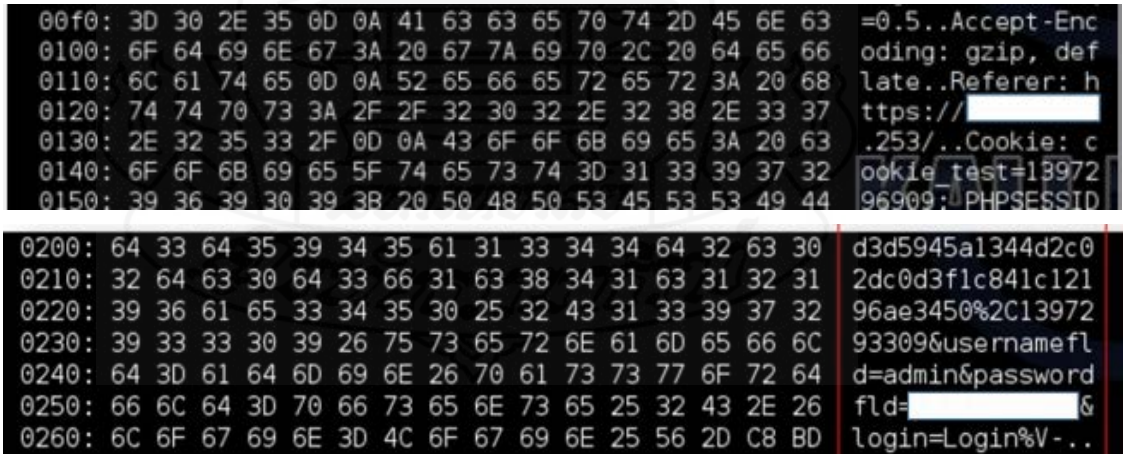
ที่มา: สิทธิศักดิ์ สายเงิน (2556)

3) การพิสูจน์ตัวตนโดยใช้ใบรับรอง (certificate) และกุญแจสาธารณะ

จะเห็นได้ว่า SSL/TLS ค่อนข้างปลอดภัยสำหรับการติดต่อสื่อสารแบบจุดต่อจุด อย่างไรก็ตาม SSL/TLS เพียงลำพังไม่สามารถที่จะรับรองความปลอดภัยสำหรับการสื่อสารจากต้นทางไปปลายทางในบริบทของการบริการผ่านเว็บได้ ซึ่งในรูปแบบนี้ข้อความจะถูกส่งโดยไคลเอ็นต์ เช่นเบราว์เซอร์หรือไม่ก็โปรแกรมประยุกต์ โดยข้อความจะถูกส่งผ่านบริการหรือโปรแกรมต่างๆ ที่อยู่ระหว่างการขนส่งก่อนที่จะถึงจุดหมายปลายทาง SSL/TLS ป้องกันข้อมูลเฉพาะการส่งระหว่างคู่ส่งและรับเท่านั้น ข้อความหลังจากที่ประมวลผลด้วย SSL/TLS ที่ฝั่งรับจะถูกส่งต่อเป็นข้อความที่ถอดรหัสแล้วไปยังระดับชั้นแอปพลิเคชัน ดังภาพที่ 2-4 จะเห็นได้ว่า ผู้ส่งและโหนดตรงกลางที่เป็นคู่ส่งและรับเช่นเดียวกับโหนดตรงกลางและผู้รับปลายทาง ดังนั้นแอปพลิเคชันที่อยู่ระหว่างกลางของผู้ส่งและผู้รับปลายทาง ก็จะสามารถที่จะตรวจสอบหรือแม้กระทั่งเปลี่ยนข้อมูลก่อนที่จะส่งต่อไปยังผู้รับ นอกจากนี้ SSL/TLS ยังมีข้อจำกัดในเรื่องการเข้ารหัสที่ไม่สามารถทำเฉพาะบางส่วนของข้อมูลที่ส่งได้

4.2.3 ปัญหา Heartbleed Bug ของ OpenSSL

สมาคมผู้ดูแลเว็บไทย, สมาคม eCommerce, TISA, และ ACIS Cyber Lab. (2556) ได้นำเสนอบทความแสดงให้เห็นว่า Heartbleed Bug เป็นชองโหว่ความเสี่ยงสูงที่มีอยู่ใน OpenSSL Library ซึ่งเว็บไซต์จำนวนมากทั่วโลกมีการใช้งาน Library นี้อยู่ โดยที่ OpenSSL Library จะถูกเรียกใช้งานโดย Application ที่ต้องการเข้ารหัสการรับส่งข้อมูลโดยใช้ SSL/TLS (เชน HTTPS, VPN, EMAIL) ผลกระทบที่เกิดจาก Heartbleed Bug คือการที่ผู้โจมตีสามารถเข้าถึงข้อมูลที่อยู่ในหน่วยความจำหลัก (RAM) ได้จากระยะไกล ในขณะที่ข้อมูลในระหว่างการรับ-ส่ง นั้นจะถูกเข้ารหัสโดย SSL/TLS แต่เมื่อข้อมูลถูกส่งมาถึงผู้รับ และเข้าไปอยู่ใน RAM นั้น จะเป็น plaintext ไม่ได้ถูกเข้ารหัส เป็นเหตุให้ข้อมูลความลับโดยเฉพาะ key ที่ใช้ถอดรหัสข้อมูล รวมถึงข้อมูลอื่นๆ เช่น username/password ถูกเข้าถึงได้โดย Hacker การที่ช่องโหว่นี้ได้ชื่อว่า Heartbleed เนื่องจากตัว Extension ตัวหนึ่งใน OpenSSL Library ชื่อว่า “Heartbeat” เป็นตัวการให้เกิดการรั่วไหลของข้อมูล Heartbleed Bug จะได้ข้อมูลเฉพาะของ Application ที่ใช้งาน OpenSSL Library นั้นๆ เช่น เครื่อง server 1 เครื่อง ให้บริการ HTTPS Web, VPN, Email แล้วทั้ง 3 บริการนี้มีช่องโหว่ Heartbleed Bug เหมือนกันหมด การโจมตีไปที่ VPN จะไม่ได้ข้อมูลใน RAM ของ Web และ Email ได้เฉพาะ VPN เองเท่านั้น เนื่องจากการทำงานปกติของระบบคอมพิวเตอร์ โปรแกรมต่างๆ ที่ทำงานอยู่ใน RAM จะรู้สึกเหมือนกับว่าตัวมันเองใช้งาน RAM อยู่เพียงผู้เดียว ทั้งๆ ที่จริงแล้วมีโปรแกรมอื่นหลายโปรแกรมทำงานอยู่



ภาพที่ 2.5 ตัวอย่างข้อมูลสำคัญที่ได้จากช่องโหว่ Heartbleed

ที่มา http://www.tisa.or.th/articles/The-Heartbleed-Bug_12042014.pdf ค้นคืนเมื่อวันที่ 15 กรกฎาคม 2557

สำหรับ OpenSSL ที่มีช่องโหว่ดังกล่าว คือเวอร์ชั่น 1.0.1 ที่ออกมาในปี 2012 โดย OpenSSL เวอร์ชั่นนี้ได้ถูกติดตั้งไว้เป็นมาตรฐานบนระบบปฏิบัติการ Linux เช่น

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
- CentOS 6.5, OpenSSL 1.0.1e-15
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
- FreeBSD 10.0 – OpenSSL 1.0.1e 11 Feb 2013
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

ปัจจุบัน ได้มีการออก OpenSSL 1.0.1g (รุ่นล่าสุด) ซึ่งแก้ปัญหาความปลอดภัยนี้ไปเรียบร้อยแล้ว

4.2.4 ใบรับรองดิจิตอล (Digital Certificate : X.509 Certificate)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (2556) ได้กล่าวถึง กระบวนการเข้ารหัส และ ลายมือชื่อดิจิตอล ในการทำธุรกรรม สามารถรักษาความ ลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคล โดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิตอล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) จะถูกนำมาใช้สำหรับยืนยันในการทำ ธุรกรรมว่า เป็นบุคคลนั้นๆ จริงตามที่ได้อ้างไว้ ใบรับรองดิจิตอลที่ออกตามมาตรฐาน X.509 Version 3 ซึ่งเป็นมาตรฐานที่ได้รับความนิยมอย่างแพร่หลายที่สุด ใบรับรองหรือใบรับรองดิจิตอลนั้นทำหน้าที่คล้ายกับบัตรประจำตัวประชาชน คือ ยืนยันตัวตนของผู้ที่เป็นเจ้าของ ซึ่งใบรับรองอิเล็กทรอนิกส์ดังกล่าว เป็นไปตามมาตรฐาน X.509 และบนใบรับรองอิเล็กทรอนิกส์แต่ละใบนั้นจะประกอบไปด้วย

1. หมายเลขของใบรับรองฯ (serial number)
2. วิธีการที่ใช้ในการเข้ารหัสข้อมูล (algorithm)
3. ชื่อขององค์กรออกใบรับรองฯ (issuer)
4. เวลาเริ่มใช้ใบรับรองฯ (starting time) และเวลาที่ใบรับรองหมดอายุ (expiring time)

5. ชื่อผู้ถือใบรับรองฯ (subject) และข้อมูลทั่วไป เช่นหน่วยงานที่สังกัด, e-mail Address เป็นต้น

6. กุญแจสาธารณะของผู้ถือใบรับรองฯ (subject ' s public key)

7. ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรองฯ (Certification Authority Signature)

CA หรือ Certificate Authority คือผู้ประกอบกิจการ ออกใบรับรองอิเล็กทรอนิกส์และเป็นที่เชื่อถือ ซึ่งเปรียบเสมือนบัตรประจำตัวที่ใช้ในการระบุตัวบุคคล ในยุคของการสื่อสารไร้พรมแดน ซึ่งใบรับรองอิเล็กทรอนิกส์ดังกล่าวนั้น จะถูกนำมาใช้ในการยืนยันตัวบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อสร้างให้เกิดความมั่นใจ และเพิ่มความปลอดภัยของข้อมูล

ชนิดของใบรับรองดิจิตอล

Client certificate เป็นใบรับรองดิจิตอลออกให้กับบุคคล เพื่อใช้ในการเข้าสู่ระบบ Intranet/Extranet Secure mail ขององค์กร ข้อมูลที่มีในใบรับรองดิจิตอล จะต้องประกอบไปด้วยชื่อ สกุลและอีเมล์ อย่างน้อย

VPN certificate ใบรับรองดิจิตอลที่มีการระบุข้อมูลของอุปกรณ์ลงในใบรับรองดิจิตอล การขอใบรับรองกระทำโดยผู้ดูแลอุปกรณ์นั้น

Device manufacturing certificate ใบรับรองดิจิตอลที่ติดอยู่กับอุปกรณ์ในหน่วยความจำถาวร ใบรับรองมีอายุการใช้งานเท่ากับอายุการใช้งานของอุปกรณ์นั้น

SSL certificate เป็นใบรับรองดิจิตอลที่สร้างขึ้นโดย web server ใช้ในการทำ SSL Tunnel กับ browser เพื่อพิสูจน์ว่า URL เป็นของ host นั้น

Code signing certificate เป็นใบรับรองใช้ในการพิสูจน์ความถูกต้องครบถ้วนและที่มาของ software เพื่อสร้างความมั่นใจว่ามาจากเจ้าของจริงๆ และไม่ถูกเปลี่ยนแปลงแก้ไขระหว่างทาง

Wireless device certificate เป็นใบรับรองที่ออกแบบมาให้ใช้งาน SSL ร่วมกับอุปกรณ์ที่มีความสามารถในการประมวลผลไม่สูง เช่น WTLS Certificate

Custom organization certificate เป็นใบรับรองที่พัฒนาขึ้นเพื่อใช้งานกับระบบเฉพาะ

4.2.5 มาตรฐานอื่นๆ ที่เกี่ยวข้อง

PKIX เป็นกลุ่มทำงานทำหน้าที่กำหนดมาตรฐานสำหรับใบรับรอง เพื่อให้เกิดความเข้ากันได้ในการใช้งาน

ASN.1 เป็นภาษาที่กำหนดขึ้นเพื่อให้ application ต่างๆ สามารถติดต่อกันได้

PKCS เป็นมาตรฐานรูปแบบข้อมูล algorithm และ API ที่จำเป็น เช่นPKCS#7 รูปแบบการจัดเก็บข้อมูลที่มีการใช้ cryptography

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้อธิบายขั้นตอนและวิธีการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ไว้ดังนี้

ขั้นตอนการขอรับใบรับรอง

1. ผู้ขอแจ้งความจำนงขอใช้ใบรับรอง

2. ผู้ออกใบรับรอง (Registration Authority: RA) ตรวจสอบและยืนยันความถูกต้องของข้อมูล

3. ผู้ออกใบรับรอง (Registration Authority: RA) ส่งคำขอใบรับรองให้ผู้ประกอบกิจการ (Certificate Authority: CA)

4. ผู้ขอสร้างกุญแจคู่และ CSR (Certificate Signing Request) CSR ใช้ในการขอใบรับรองตามมาตรฐาน PKCS#10 ประกอบด้วย ข้อมูลส่วนบุคคล ในรูปแบบของ Distinguished Name ตามมาตรฐาน X.500 กุญแจสาธารณะของผู้ใช้ ลายมือชื่อดิจิตอลของผู้ใช้ ซึ่งเกิดจากกุญแจส่วนตัวของผู้ใช้

5. ผู้ประกอบกิจการ (Certificate Authority: CA) ออกใบรับรอง

6. ผู้ประกอบกิจการ (Certificate Authority: CA) เผยแพร่ใบรับรอง

การเพิกถอนใบรับรอง

การเพิกถอนใบรับรองกระทำเมื่อเกิดเหตุการณ์ดังนี้ เมื่อผู้อื่นล่วงรู้หรือสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ใช้บริการไปใช้งาน เมื่อผู้อื่นล่วงรู้รหัสผ่านในการเรียกใช้กุญแจส่วนตัวของผู้ใช้บริการ อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหายหรือไม่สามารถใช้งานได้ ผู้ใช้บริการออกจากองค์กร ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลในใบรับรอง ผู้ใช้บริการไม่ปฏิบัติตามนโยบายของผู้ประกอบกิจการ (Certificate Authority: CA)

ขั้นตอนการเพิกถอนใบรับรองดังนี้

1. ผู้ขอใช้บริการแจ้งความจำนงขอเพิกถอนใบรับรอง

2. ผู้ออกใบรับรอง (Registration Authority: RA) ตรวจสอบและยืนยันความถูกต้องของข้อมูล

3. ผู้ออกใบรับรอง (Registration Authority: RA) ส่งคำขอเพิกถอนใบรับรองให้ผู้ประกอบกิจการ (Certificate Authority: CA)

4. ผู้ประกอบกิจการ (Certificate Authority: CA) เพิกถอนใบรับรอง

5. ผู้ประกอบกิจการ (Certificate Authority: CA) เผยแพร่รายการเพิกถอนใบรับรอง

6. ผู้ประกอบกิจการ (Certificate Authority: CA) แจ้งผู้ใช้บริการเพื่อทำการ update CRL

7. ผู้ใช้บริการทุกรายทำการ update ใบรับรองดิจิตอลเซิร์ฟเวอร์ (CRL)

การตรวจสอบใบรับรอง

ผู้ใช้ใบรับรองจำเป็นต้องตรวจสอบใบรับรองที่ได้รับว่าสามารถใช้งานได้หรือไม่ ประกอบด้วย

- Certificate chain
- Self-sign certificate ใบรับรองของ Root CA
- Intermediate CA certificate ใบรับรองของผู้ให้บริการภายใต้ Root CA
- End entity certificate ใบรับรองของผู้ใช้งานทั่วไป

หลักการตรวจสอบใบรับรอง

ตรวจสอบ Signature ของใบรับรองของผู้ส่ง

ตรวจสอบวันที่เริ่มต้นสิ้นสุดในการใช้งาน

ตรวจสอบความเหมาะสมในการใช้งานรวมทั้งนโยบายที่ระบุในใบรับรอง

ตรวจสอบว่าใบรับรองยังไม่ถูกเพิกถอน จากใบรับรองดิจิตอลเซิร์ฟเวอร์ (CRL), CDP และ OCSP

CDP (CRL Distribution Point) เป็น URL ที่ใช้ในการเข้าถึงไฟล์ CRL สามารถมีได้หลายค่า OCSP (Online Certificate Status Protocol) เป็นการตรวจสอบสถานะแบบออนไลน์ โดย ผู้ร้องขอทำการส่งคำร้องขอตรวจสอบไปที่ OCSP server โดยระบุ serial number ของใบรับรองที่ต้องการตรวจสอบและ message digest ของชื่อและกุญแจสาธารณะของ CA ที่ออกใบรับรอง OCSP server ส่งผลการตรวจสอบของใบรับรองมีได้ 3 ค่า คือ Good สถานะถูกต้อง Revoked สถานะถูกเพิกถอน Unknown ไม่สามารถตรวจสอบสถานะได้

4.3 การรักษาความมั่นคงปลอดภัยของสารสนเทศตามแบบจำลองโอเอสไอ

Open System Interconnection: OSI เป็นมาตรฐานการสื่อสารคอมพิวเตอร์ระบบเปิด (วิจิตรา โกมาสถตย์: 2556) ซึ่งมีแบบจำลองของการเชื่อมต่อระหว่างระบบแบ่งเป็น 7 ชั้นเพื่อใช้กำหนดเป็นมาตรฐานให้กับระบบต่างๆ ให้สามารถทำงานและติดต่อถึงกันได้โดยชั้นของ OSI Model มีไว้เพื่อใช้อ้างอิงการทำงานในการเชื่อมต่อระหว่างระบบในแต่ละชั้นการทำงานทั้งนี้เพื่อช่วยลดขนาดของปัญหาในการเชื่อมต่อให้เล็กลง การแบ่งชั้นการทำงานทำให้รับรู้ได้ว่าปัญหา

เกิดขึ้นที่ไหน สามารถแก้ไขปัญหาได้ตรงจุด การแก้ปัญหาก็สามารถทำได้รวดเร็วขึ้น และ OSI Model ทำให้ผู้ผลิตแต่ละรายสามารถพัฒนาผลิตภัณฑ์ที่สามารถทำงานร่วมกันได้ และไม่จำเป็นต้องเริ่มต้นการพัฒนาครบทุกองค์ประกอบ สามารถพัฒนาขึ้นมาเพียงชั้นใดชั้นหนึ่งจากจำนวน 7 ชั้น และนำไปใช้งานร่วมกับชั้นที่มีการพัฒนาไว้แล้ว หลักการแต่ละชั้นจะติดต่อกับชั้นในระดับเดียวกันที่อยู่บนเครื่องอีกเครื่องหนึ่ง แต่ในทางปฏิบัติชั้นที่อยู่ติดกัน(บนหรือล่าง)เท่านั้นที่จะมีการติดต่อกันจริง ยกเว้นชั้นล่างสุดคือชั้น Physical จึงจะติดต่อกับชั้น Physical ของอีกเครื่องหนึ่งได้

การรักษาความมั่นคงปลอดภัยของสารสนเทศตามแบบจำลองโอเอสไอ มีแนวทางคือ

1. ลำดับชั้นกายภาพ (Physical Layer) ทำหน้าที่ เกี่ยวข้องกับการสื่อสารข้อมูล ต้องพิจารณาการรักษาความปลอดภัยของสัญญาณที่มีการส่งผ่านข้อมูล จากต้นทางไปให้ถึงปลายทาง ด้วยการเข้ารหัสข้อมูล การรักษาความปลอดภัยทางกายภาพและเทคนิคการส่งผ่านข้อมูลที่มีความปลอดภัย

2. ลำดับชั้นเชื่อมโยงข้อมูล (Data link Layer) ทำหน้าที่ในกระบวนการถ่ายโอนหรือแลกเปลี่ยนข้อมูลกันระหว่างผู้ส่งและผู้รับ โดยผ่านช่องทางสื่อสาร เช่น อุปกรณ์อิเล็กทรอนิกส์หรือคอมพิวเตอร์เป็นตัวกลางในการส่งข้อมูล เพื่อให้ผู้ส่งและผู้รับเกิดความเข้าใจตรงกัน ระหว่างการส่งอาจจะมีสิ่งรบกวนจากภายนอกทำให้ข้อมูลเสียหายไปได้ ต้องมีการรักษาความปลอดภัยของเฟรมข้อมูลและตัวกลางในการสื่อสารที่จะทำให้เกิดการรบกวนน้อยที่สุด

3. ลำดับชั้นเครือข่าย (Network Layer) ทำหน้าที่เลือกเส้นทางการส่งผ่านข้อมูล โดยเป็นผู้ตัดสินใจว่าเส้นทางใดที่ควรส่งข้อมูลไป ทั้งนี้ขึ้นอยู่กับ สภาพของเครือข่ายลำดับความสำคัญของบริการ และปัจจัยอื่นๆ ซอฟต์แวร์ ในลำดับชั้นเครือข่าย ต้องมีการรักษาความปลอดภัยโดยการกำหนดเส้นทางของเฟรมระหว่างเครือข่าย การควบคุมปริมาณการใช้เครือข่ายย่อย การกระจายตัวของเฟรม การแมปที่อยู่จริงแบบตรรกะ และกำหนดบัญชีการใช้งานเครือข่ายย่อย

4. ลำดับชั้นขนส่ง (Transport Layer) ทำหน้าที่ควบคุมคุณภาพของข้อมูลที่ได้รับให้ถูกต้องทั้งรูปแบบ และลำดับถ้ามีความเสียหายเกิดขึ้น ในระบบเครือข่าย และ ถ้าเครือข่ายล้มเหลวซอฟต์แวร์ในลำดับชั้นขนส่ง จะมองหาเส้นทางอื่น ที่จะสามารถไปยังปลายทางหรืออาจจัดเก็บข้อมูลที่ส่งไว้จนกระทั่งการเชื่อมต่อของเครือข่ายถูกสร้างขึ้นใหม่ มีการแบ่งข้อความจากลำดับชั้นส่วนงานที่อยู่ด้านบนเพื่อแบ่งข้อความเป็นหน่วยที่เล็กลงและหน่วยเล็กลงไปยังลำดับชั้นเครือข่ายผ่านการยอมรับ ต้องมีวิธีการรักษาความปลอดภัยโดยการควบคุมข้อมูล การเริ่มต้นของข้อความและค่าสถานะสิ้นสุดข้อความ

5. ลำดับชั้นส่วนงาน (Session Layer) ทำหน้าที่ในการจัดการกับเซสชั่นของโปรแกรม ควบคุมการเชื่อมต่อระหว่างคอมพิวเตอร์หลายตัว บริหารจัดการการเชื่อมต่อการใช้งานระหว่างภายในกับระยะไกล ทำงานแบบ duplex จัดทำวิธีการตรวจสอบ การเสร็จสิ้น การยกเลิกดำเนินการและการเริ่มต้นใหม่ ต้องมีการรักษาความปลอดภัยด้วยการควบคุมการทำงานของเซสชั่น

6. ลำดับชั้นนำเสนอ (Presentation Layer) ทำหน้าที่ในกระบวนการแปลแสดงผลให้กับเครื่องคอมพิวเตอร์ลูกข่าย (client) ที่ใช้งานระบบเว็บเซอร์วิส ควรมีการรักษาความปลอดภัยด้วยการแปลงข้อมูล การบีบอัดข้อมูล การเข้ารหัสลับข้อมูลสำหรับวัตถุประสงค์ด้านการรักษาความปลอดภัย

7. ลำดับชั้นการประยุกต์ (Application Layer) ทำหน้าที่การรับคำสั่งต่างๆ จากผู้ใช้งานและดึงข้อมูลมาแสดงผลบนหน้าจอ ต้องมีการรักษาความปลอดภัยในการเข้าถึงข้อมูลระยะไกลเข้าถึงเครื่องพิมพ์ระยะไกลและเทอร์มินัลเสมือนของเครือข่าย

5. การทดสอบความปลอดภัยและความถูกต้องฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST

กานดา รุณนะพงศา , พงษ์ศักดิ์ ฮุนตระกูล , เสกสิทธิ์ สุวรรณ , ชัยวัฒน์ บุตรไชย และภาณุวัฒน์ คามวัลย์ จากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น ,สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และ ฝ่ายวิจัยและพัฒนาเทคโนโลยีคอมพิวเตอร์เพื่อการคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี สำนักส่งเสริมเครือข่ายวิสาหกิจคอมพิวเตอร์ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ จังหวัดปทุมธานี ได้จัดทำแนวทางในการทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST และ กล่าวว่าเว็บเซอร์วิส (Web Service) เป็นระบบซอฟต์แวร์ที่ออกแบบมาเพื่อสนับสนุนการทำงานระหว่างคอมพิวเตอร์กับคอมพิวเตอร์ผ่านระบบเครือข่าย โดยใช้ภาษาเอ็กซ์เอ็มแอล (XML) เป็นภาษาในการติดต่อสื่อสารระหว่างโปรแกรม ปัจจุบันมีการพัฒนาเว็บเซอร์วิสทั้งแบบ SOAP (Simple Object Access Protocol) และ REST (Representational State Transfer) ถึงแม้ว่าเว็บเซอร์วิสแบบ SOAP จะเป็นมาตรฐานกลางซึ่งเกิดขึ้นมาก่อนเว็บเซอร์วิสแบบ REST แต่ปัจจุบันมีการพัฒนาและเรียกใช้เว็บเซอร์วิสแบบ REST มากขึ้นเนื่องจากเว็บเซอร์วิสแบบ REST นั้นพัฒนาและเรียกใช้ง่ายกว่าแบบ SOAP แต่ทั้งนี้ทั้งนั้นไม่ว่า ผู้พัฒนาเว็บเซอร์วิสจะพัฒนาเว็บเซอร์วิสแบบใด ผู้พัฒนาเว็บเซอร์วิสจำเป็นต้องทดสอบเว็บเซอร์วิสก่อนที่จะเปิดบริการเว็บเซอร์วิสให้ผู้อื่นเรียกใช้ โดยนำเสนอแนวทางในการทดสอบความสมบูรณ์และความถูกต้องของฟังก์ชั่นการทำงานของโอเปอเรชันต่างๆ ของเว็บเซอร์วิสแบบ REST ซึ่งแนวทางในการทดสอบนี้

สามารถนำไปทดสอบกับเว็บเซอร์วิสแบบ REST ใดๆ โดยที่เท่าที่ทราบยังไม่มีบทความใดๆ นำเสนอวิธีทดสอบฟังก์ชั่นการทำงานของโอเปอเรชั่นต่างๆ ของเว็บเซอร์วิสแบบ REST ซึ่งมีแนวทางในการทดสอบฟังก์ชั่นของเว็บเซอร์วิสแบบ REST ดังนี้

เงื่อนไขในการทดสอบฟังก์ชันการทำงานทั่วไป

1. ตรวจสอบความถูกต้องในการเรียกใช้ในแต่ละฟังก์ชัน

- ทดลองส่งค่าตัวแปรที่ถูกต้องให้แต่ละฟังก์ชัน
- ทดลองเรียกใช้งานแต่ละฟังก์ชัน เพื่อดูผลว่า สามารถเรียกใช้ได้หรือไม่

2. ตรวจสอบความครบถ้วนของข้อมูลที่ได้จากการเรียกใช้เว็บเซอร์วิสในแต่ละฟังก์ชัน

- ทดสอบเหมือนข้อ 1
- ตรวจสอบผลลัพธ์ที่ได้จากการเรียกใช้แต่ละฟังก์ชันเทียบกับโครงสร้างข้อมูลในเอกสาร Web Services REST API GUIDE

3. ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งค่าตัวแปรที่ไม่ถูกต้องในแต่ละฟังก์ชัน

- ทดลองใส่ค่าข้อมูลที่ไม่ถูกต้องลงในแต่ละฟังก์ชัน
- สุ่มการใส่ข้อมูลที่ไม่ถูกต้อง แล้วรายงานผล
- ตรวจสอบข้อผิดพลาดที่ได้กับเอกสาร Web Services REST API GUIDE

4. ตรวจสอบการแสดงข้อผิดพลาดเมื่อไม่ส่งค่าตัวแปรในแต่ละฟังก์ชัน

- ไม่ใส่ค่าอินพุตพารามิเตอร์แล้วทำการเรียกใช้แต่ละฟังก์ชัน
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

5. ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งคีย์ Authentication ไม่ถูกต้องในแต่ละฟังก์ชัน

- ทดลองสุ่ม Key Authentication แล้วทำการเรียกใช้แต่ละฟังก์ชัน
- ทดลองแก้ไข Key Authentication เดิม แล้วทำการเรียกใช้แต่ละฟังก์ชัน
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

6. ตรวจสอบการแสดงข้อผิดพลาดเมื่อไม่มีการส่งคีย์ Authentication ในแต่ละฟังก์ชัน

- ทดลองทำการเรียกใช้แต่ละฟังก์ชันโดยไม่ทำการส่ง Key Authentication
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

7. ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าอินพุตไม่ครบตามจำนวนที่ฟังก์ชันต้องการในแต่ละฟังก์ชัน

- ทดลองเรียกใช้แต่ละฟังก์ชัน โดยส่งอินพุตไม่ครบตามจำนวนฟังก์ชันที่ต้องการ

- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

8. ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าอินพุตมากกว่าที่จำนวนที่ฟังก์ชันต้องการในแต่ละฟังก์ชัน

- ทดลองเพิ่มพารามิเตอร์ที่ทำการเรียกใช้แต่ละฟังก์ชัน
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

9. ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าตัวแปรคนละประเภทที่ฟังก์ชันต้องการในแต่ละฟังก์ชัน

- ทดลองส่งค่าตัวแปรที่ต้องการ จากชนิดอื่นเป็น String
- ทดลองส่งค่าตัวแปรที่ต้องการ จากชนิดสลับซับซ้อน (complex type) เป็นชนิดง่าย (simple type)
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

10. ตรวจสอบค่าของข้อมูลเมื่อส่งค่าอินพุตเป็น Null ในแต่ละฟังก์ชัน

- ทดลองส่งค่าตัวแปรเป็น Null ในแต่ฟังก์ชัน
- ระบบต้องไม่มีการแสดงผลข้อมูลที่ถูกต้อง

11. ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งค่าอินพุตเป็น Null ในแต่ละฟังก์ชัน

- ทดลองส่งค่าตัวแปรเป็น Null ในแต่ฟังก์ชัน
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

12. ตรวจสอบความถูกต้องของข้อมูลเมื่อข้อมูลเป็นชนิดข้อมูลที่ซับซ้อนในแต่ละฟังก์ชัน

- ทดลองส่งข้อมูลในรูปแบบซับซ้อน
- ตรวจสอบข้อมูลที่ได้รับ

13. ตรวจสอบการแสดงข้อผิดพลาดเมื่อผู้ใช้ขอบริการข้อมูลที่ไม่มีให้บริการในแต่ละฟังก์ชัน

- ทดลองส่งข้อมูลที่ระบบไม่มีให้บริการ
- ตรวจสอบข้อความแสดงข้อผิดพลาดที่คาดว่าจะได้รับ

14. ตรวจสอบรูปแบบของชนิดข้อมูล XML ว่าถูกต้องตามโครงสร้างของเอกสารหรือไม่ (Valid Document)

- ทดลองส่งค่าตัวแปรที่ถูกต้องให้แต่ละฟังก์ชัน
- ตรวจสอบผลลัพธ์ เทียบกับชนิดข้อมูลในเอกสาร Web Services REST API GUIDE

15. ตรวจสอบข้อมูลที่ได้จากเว็บเซอร์วิสว่ามีรูปแบบตรงตามกฎภาษา XML หรือไม่ (Well-formed XML Document)

- ทดลองส่งค่าตัวแปรที่ถูกต้องให้แต่ละฟังก์ชัน
- ตรวจสอบผลลัพธ์ที่ได้ ถ้าสามารถแสดงผลผ่านทางบราวเซอร์ได้ แสดงว่าเป็น Well-formed XML Document

แนวทางในการทดสอบ

1) เขียนโปรแกรมเรียกใช้เว็บเซอร์วิส โดยใช้ภาษา Java, PHP และ .NET

2) ทำการทดลองเรียกใช้ฟังก์ชัน ตามเงื่อนไขข้างต้น

3) ตรวจสอบผลลัพธ์ และรายงานผลที่ได้

สภาพแวดล้อมการทดสอบ

1) เครื่องเซิร์ฟเวอร์ต้องเปิดอยู่

2) โปรแกรมเว็บเซิร์ฟเวอร์ ที่เป็น IIS หรือ Apache HTTP จะต้องเปิดให้บริการอยู่

3) เว็บเซอร์วิสแบบ REST จะต้องถูกติดตั้งเรียบร้อยแล้วบนเซิร์ฟเวอร์

4) เซิร์ฟเวอร์ที่เป็นฐานข้อมูล จะต้องเปิดให้บริการอยู่

5) เครื่องผู้ทดสอบจะต้องมีโปรแกรมเว็บบราวเซอร์ หรือ สามารถเชื่อมต่ออินเทอร์เน็ตได้

ในการทดสอบความสมบูรณ์และความถูกต้องของฟังก์ชั่นของเว็บเซอร์วิสแบบ REST การทดสอบเว็บเซอร์วิสนั้นจำเป็นต้องมีเพื่อส่งเสริมให้ผู้พัฒนาเว็บเซอร์วิสสามารถพัฒนาเว็บเซอร์วิสได้สมบูรณ์และถูกต้อง ซึ่งจะมีผลทำให้ช่วยสนับสนุนให้เกิดการพัฒนาและการใช้งานเว็บเซอร์วิสอย่างแพร่หลายในประเทศไทย

อย่างไรก็ตาม การทดสอบเว็บเซอร์วิสนั้นไม่ควรจะทดสอบเพียงแค่ฟังก์ชั่นการใช้งานของเว็บเซอร์วิสเท่านั้น อย่างเช่น ควรจะทดสอบความเร็ว (response time) และความปลอดภัยของข้อมูล (security) โดยเฉพาะข้อมูลสุขภาพส่วนบุคคลซึ่งต้องได้รับการคุ้มครองข้อมูลตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 และพระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. 2540 ผู้วิจัยจึงได้ดำเนินการออกแบบและพัฒนาเว็บเซอร์วิสในรูปแบบ REST และมีการออกแบบความปลอดภัยในรูปแบบมาตรฐานในการแลกเปลี่ยนข้อมูล

6. แนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา

สถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ได้กำหนดมาตรฐานการจัดการและแนวทางในการรักษาความปลอดภัยของข้อมูลสำหรับเว็บเซิร์ฟเวอร์ (NIST SP 800-44 Guidelines on Securing Public Web Servers) เพื่อประสิทธิภาพและความเป็นส่วนตัวของสำหรับการแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เน็ต โดยมีข้อกำหนดใน 3 ส่วนหลักคือ

6.1 ข้อกำหนดความปลอดภัยของระบบปฏิบัติการ (Checklist for Securing the Web Server Operating System) เพื่อป้องกันเว็บเซิร์ฟเวอร์ที่เกี่ยวข้องกับระบบปฏิบัติการพื้นฐานแอพลิเคชันเว็บเซิร์ฟเวอร์และเครือข่าย จากการโจมตีโดยตรง ข้อกำหนดเพื่อให้มีการกำหนดค่าอย่างเหมาะสม ตั้งแต่ขั้นตอนการติดตั้ง การอัพเดทแพทช์ต่างๆ ซึ่งเป็นขั้นตอนทั่วไปที่ต้องกระทำในการรักษาความปลอดภัยของระบบปฏิบัติการ

6.2 ข้อกำหนดความปลอดภัยของเว็บเซิร์ฟเวอร์ (Checklist for Securing the Web Server) การรักษาความปลอดภัยการติดตั้งซอฟแวร์เว็บเซิร์ฟเวอร์เริ่มตั้งแต่การศึกษาเอกสารของผู้ผลิตของเว็บเซิร์ฟเวอร์อย่างระมัดระวัง และตั้งค่าตัวเลือกต่างๆ ในขั้นตอนการติดตั้ง เพื่อตรวจสอบว่ามีช่องโหว่และแพทช์ที่เกี่ยวข้องที่สามารถใช้ได้ การติดตั้งเซิร์ฟเวอร์ไม่ควรเชื่อมโยงกับเครือข่ายภายนอก (อินเตอร์เน็ต) หรือผู้ใช้ภายนอกจนกว่าซอฟต์แวร์ทั้งหมดมีการติดตั้งด้วยการกำหนดค่าที่ปลอดภัย

6.3 ข้อกำหนดความปลอดภัยของเนื้อหา (Checklist for Securing Web Content) เพื่อป้องกันการเชื่อมโยงหรือทางลัดในเนื้อหาเว็บสาธารณะ ในระดับไดเรกทอรี หรือปิดกั้นไฟล์ที่ชี้ไปยังไดเรกทอรีหรือไฟล์อื่นๆ บนโฮสต์เซิร์ฟเวอร์หรือระบบแฟ้มเครือข่าย และการกำหนดค่าต่างๆ ไม่ควรอยู่ในไดเรกทอรีสำหรับเนื้อหาของเว็บสาธารณะ และ จำกัดการเข้าถึงเนื้อหาเว็บเฉพาะไดเรกทอรีไฟล์ที่อนุญาต

7. กฎหมายที่เกี่ยวข้อง

7.1 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ภูมิพลอดุลยเดช ป.ร. ให□ไว้□ ณ วันที่ 3 มีนาคม พ.ศ. 2550

มาตรา 7 ข้อมูลด้□านสุขภาพของบุคคลเป□นความลับส่□วนบุคคล ผู□ใดจะนำไปเปิด เผยในประการที่น่าจะทำให้□บุคคลนั้นเสียหายไม่□ได้□ เว้□นแต่□การเปิดเผยนั้นเป็นไปตามความประสงค์□ของบุคคลนั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใดๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข□อมูลข่าวสารของราชการหรือกฎหมายอื่น เพื่อขอเอกสารเกี่ยวกับข้□อมูลด้□านสุขภาพของบุคคลที่ไม่ใช่□ของตนไม่□ได้□

มาตรา 8 ในการบริการสาธารณสุข บุคลากรด้านสาธารณสุขต้องแจ้งข้อมูลด้านสุขภาพที่เกี่ยวข้องกับการให้บริการให้ผู้รับบริการทราบอย่างเพียงพอที่ผู้รับบริการจะใช้ประกอบการตัดสินใจในการรับหรือไม่รับบริการใด และในกรณีที่ผู้รับบริการปฏิเสธไม่รับบริการใดจะให้บริการนั้นมิได้ ในกรณีที่เกิดความเสียหายหรืออันตรายแก่ผู้รับบริการเพราะเหตุที่ผู้รับบริการปกปิดข้อเท็จจริงที่ตนรู้และควรบอกให้แจ้ง หรือแจ้งขอความอันเป็นเท็จ ผู้ให้บริการไม่ต้องรับผิดชอบในความเสียหายหรืออันตรายนั้น เวนแต่เป็นกรณีที่ผู้ให้บริการประมาทเลินเล่ออย่างร้ายแรง ความในวรรคหนึ่งมิให้ใช้บังคับกับกรณีดังต่อไปนี้

(1) ผู้รับบริการอยู่ในภาวะที่เสี่ยงอันตรายถึงชีวิตและมีความจำเป็นต้องให้ความช่วยเหลือเป็นการรีบด่วน

(2) ผู้รับบริการไม่อยู่ในฐานะที่จะรับทราบข้อมูลได้ และไม่อาจแจ้งให้บุคคลซึ่งเป็นทายาทโดยธรรมตามประมวลกฎหมายแพ่งและพาณิชย์ ผู้ปกครอง ผู้ปกครองดูแล ผู้พิทักษ์หรือผู้อนุบาลของผู้รับบริการ แล้วแต่กรณี รับทราบข้อมูลแทนในขณะนั้นได้

มาตรา 9 ในกรณีที่ผู้ประกอบวิชาชีพด้านสาธารณสุขประสงค์จะใช้ผู้รับบริการเป็นส่วนหนึ่งของการทดลองในงานวิจัย ผู้ประกอบวิชาชีพด้านสาธารณสุขต้องแจ้งให้ผู้รับบริการทราบล่วงหน้า และต้องได้รับความยินยอมเป็นหนังสือจากผู้รับบริการก่อนจึงจะดำเนินการได้ ความยินยอมดังกล่าว ผู้รับบริการจะเพิกถอนเสียเมื่อใดก็ได้

มาตรา 10 เมื่อมีกรณีที่จะมีผลกระทบต่อสุขภาพของประชาชนเกิดขึ้น หน่วยงานของรัฐที่มีข้อมูลเกี่ยวกับกรณีดังกล่าว ต้องเปิดเผยข้อมูลนั้นและวิธีป้องกันผลกระทบต่อสุขภาพให้ประชาชนทราบและจัดหาข้อมูลให้โดยเร็ว

การเปิดเผยข้อมูลตามวรรคหนึ่งต้องไม่มีลักษณะเป็นการละเมิดสิทธิส่วนบุคคลของบุคคลใดเป็นการเฉพาะ

7.2 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ภูมิพลอดุลยเดช ป.ร. ให้ไว้ ณ วันที่ 2 กันยายน พ.ศ. 2540

มาตรา 23 หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

7.2.1 ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

7.2.2 พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

7.2.3 จัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

1) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

2) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

3) ลักษณะการใช้ข้อมูลตามปกติ

4) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

5) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

6.) แหล่งที่มาของข้อมูล

7.2.4 ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

7.2.5 จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ

มาตรา 24 หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคล ที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (3) (4) (4) (5) (6) (7) (8) และ (9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

มาตรา 25 ภายใต้บังคับมาตรา 14 และมาตรา 15 บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดู หรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา 9 วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสาร

ส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอ ให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวันนับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ต่อคณะกรรมการ และไม่ว่ากรณีใดๆ ให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา 23 มาตรา 24 และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถหรือเจ้าของข้อมูลที่ถึงแก่กรรมแล้วก็ได้

กฎหมายทั้ง 2 ฉบับให้ความคุ้มครองข้อมูลสุขภาพส่วนบุคคลให้เป็นความลับส่วนบุคคล ซึ่งหน่วยบริการสาธารณสุขที่มีการเรียกใช้ข้อมูลดังกล่าวต้องใช้ความระมัดระวัง ไม่เปิดเผยข้อมูลที่ทำให้เกิดความเสียหายต่อบุคคล ไม่ว่าจะมีเจตนาหรือไม่ ต้องปฏิบัติตามกฎหมายอย่างเคร่งครัด การเรียกใช้หรือการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลนั้น จะต้องมีมาตรฐานความปลอดภัยตามกฎหมายกำหนดมิฉะนั้นอาจถูกผู้ป่วยที่ได้รับความเสียหายจากการเปิดเผยข้อมูลฟ้องร้อง ดำเนินคดีได้ตามกฎหมาย

8. งานวิจัยที่เกี่ยวข้อง

8.1 งานวิจัยในประเทศ

8.1.1 ความมั่นคงปลอดภัยการรับส่งแฟ้มข้อมูลและการจัดการการเข้ารหัสลับภายในองค์กร (ชาลี ธรรมรัตน์ 2554)

บทความวิจัยฉบับนี้เสนอโปรโตคอลที่ใช้ในการถ่ายโอนข้อมูลเพื่อความมั่นคงปลอดภัยที่สูงขึ้น โดยมีการประยุกต์ใช้ใบรับรองดิจิทัลร่วมกับวิทยาการเข้ารหัสลับแบบสมมาตรเพื่อใช้ในการรักษาความลับ และการพิสูจน์ตัวจริง รวมถึงการประยุกต์ใช้เทคนิคการสร้างและกระจายเซสชั่นคีย์แบบออฟไลน์ เพื่อเพิ่มความมั่นคงปลอดภัยในการรับส่งข้อมูลยิ่งขึ้นในการทำธุรกรรมอิเล็กทรอนิกส์ผ่านโปรแกรมประยุกต์ที่พัฒนาขึ้นมาใช้จำนวนมาก โดยวิธีการทำให้โปรโตคอลสำหรับการถ่ายโอนไฟล์ผ่านเครือข่ายมีความมั่นคงปลอดภัยเพียงพอ ระบบการรักษาความมั่นคงปลอดภัยในการจัดการแฟ้มข้อมูล จะใช้งานแอพพลิเคชั่นบนวินโดวส์ (Windows

Application) เป็นตัวกลางในการสื่อสาร ซึ่งจะทำให้การสื่อสารระหว่างกันมีความปลอดภัยมากยิ่งขึ้น เมื่อมีการเชื่อมต่อกันแต่ละฝั่งสามารถเลือกได้ว่าเมื่อใดที่จำเป็นต้องทำการเข้ารหัสลับข้อมล (Data Encryption) และระดับความซับซ้อนของการเข้ารหัส (Level of encryption) ซึ่งการเข้ารหัสลับ (Encryption) และการถอดรหัสลับ (Decryption) จะมีเพียงผู้ที่เชื่อมต่อกันระหว่างผู้รับกับผู้ส่งเท่านั้น จึงเป็นการสะดวกที่ผู้ใช้งานทั่วไปสามารถนำไปใช้งานได้

8.1.2 การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา: บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด (ศราวุฒิ จันทะคัด 2554)

งานวิจัยนี้นำเสนอการจัดทำนโยบายความปลอดภัยให้กับบริษัท แซนด์แอนด์ซอยล์ และหาระบบไฟรวอลล์ (Firewall) ที่เป็น open source คือโปรแกรม Pfsense Firewall ร่วมกับการจดทำนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท มีการทดสอบระบบความปลอดภัยและนโยบายภายในองค์กร และทั้งยังแนะนำโปรแกรมที่ช่วยสนับสนุนโยบายเกี่ยวกับความปลอดภัยภายในระบบคอมพิวเตอร์มาใช้งาน เพื่อลดความเสี่ยงในส่วนต่าง ๆ ของระบบ เพื่อให้องค์กรลดความเสี่ยงและสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

8.1.3 การจัดทำนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร กรณีศึกษาสำหรับบริษัท สินแพทย์ จำกัด (โรงพยาบาลสินแพทย์) (เดชาวัต นิชาญานันท์ 2555)

งานวิจัยนำเสนอความจำเป็นที่โรงพยาบาลต้องหาเครื่องมือทางด้านสารสนเทศ เช่น เซิร์ฟเวอร์ (Server) และ แอพพลิเคชั่น (Application) มาช่วยในการสนับสนุนในการบริหาร และให้บริการต่อลูกค้า เพื่อเกิดความพึงพอใจสูงสุด โรงพยาบาลสินแพทย์ได้นำเครื่องมือมาใช้ ในการกระบวนการบริหารและการให้บริการ ด้วยเช่นกัน เนื่องจากเห็นว่าถ้านโยบายความปลอดภัยมั่นคงระบบสารสนเทศ ยังไม่ครอบคลุม รายละเอียดส่งผลกระทบต่อการดำเนินการธุรกิจ และทำลายภาพลักษณ์ สูญเสียโอกาสทางด้านธุรกิจโรงพยาบาลได้ จงจำเป็นต้องทำให้ระบบสารสนเทศใหม่ความมั่นคงปลอดภัยสูงสด ได้นำวิธีการประเมินความเสี่ยงจากทรัพย์สินด้านสารสนเทศ และข้อกำหนดมาตรฐาน ISO 270001 นำผลมาวิเคราะห์ และนำผลมาจัดทำนโยบายความปลอดภัยมั่นคงระบบสารสนเทศเพื่อเป็นข้อกำหนดและปฏิบัติงานของเจ้าหน้าที่เป็นทิศทางเดียวกัน ส่งให้ผลให้ ความเสี่ยงลดลง หรือบรรเทา หรอไม่เกิดซ้ำ ส่งผลให้ระบบสารสนเทศมีความมั่นคงปลอดภัยเพิ่มขึ้น และเป็นเครื่องมือช่วยในการให้บริการลูกค้าได้อย่างเต็มประสิทธิภาพ ทำให้การดำเนินธุรกิจทางโรงพยาบาลเป็นไปอย่างราบรื่น และเป็นที่ยอมรับและไว้วางใจของลูกค้า

8.2 งานวิจัยต่างประเทศ

8.2.1 Recep Baci (2011), Development of A Web Services Security Architecture Based on .Net Framework

งานวิจัยนี้ศึกษา Service Oriented Architecture (SOA) ซึ่งเป็นรูปแบบสถาปัตยกรรมหนึ่งที่ช่วยให้applicationต่างๆ สามารถทำงานร่วมกันได้บนแพลตฟอร์ม ภาษาการดำเนินงาน และสถานที่ที่แตกต่างกัน โดยการใช้ประโยชน์จาก generic และความน่าเชื่อถือของระบบ services ที่สามารถนำไปใช้ในการสร้างบล็อกapplication ได้ SOA จะต้องรวมเอากระบวนการและกลวิธีต่างๆ เพื่อที่จะสามารถพัฒนา application และระบบข้อมูลที่ซับซ้อนได้ สถาปัตยกรรมของ SOA มีลักษณะและข้อกำหนดทางสถาปัตยกรรมที่เฉพาะตัว ซึ่งจำเป็นต้องได้รับการวิเคราะห์และแยกแยะประเภท เพื่อที่จะสามารถใส่ข้อมูลที่จำเป็นในโมเดลทางสถาปัตยกรรมของ SOA ได้อย่างถูกต้อง เพื่อการพัฒนาการใช้งานในทางการบริการ เทคโนโลยีล่าสุดของ SOA คือ web service ซึ่งมีความสำคัญมากขึ้นเป็นลำดับ เนื่องจากเป็นเทคโนโลยีเพื่อการพัฒนาการใช้งานด้านการบริการแบบกระจาย (distributed service) web service เป็นกระบวนทัศน์ที่เพิ่งเกิดขึ้นสำหรับการใช้งานใน web ในการประสานงานทางธุรกิจ แต่ละ service จะติดต่อสื่อสารกันผ่านทาง protocols มาตรฐาน ที่สามารถบ่งบอกถึงศักยภาพของการทำงานร่วมกันของ services ปริญญานิพนธ์นี้จะเริ่มด้วยการสืบค้นหาหลักการของ platform .NET ซึ่งเป็นส่วนสำคัญในความปลอดภัยทางการติดต่อสื่อสาร กรณีตัวอย่างได้แสดงให้เห็นถึงการรักษาความปลอดภัยระหว่าง web service กับผู้ใช้บริการด้วยการใช้ระเบียบวิธีแบบ RIJNDAEL 3DES และ RSA ซึ่งใช้งานบนโครงสร้างแบบ code ที่ใช้เอกลักษณ์แบบ token ซึ่งได้มาจากเอกลักษณ์แบบ web service เพื่อการตรวจสอบเอกลักษณ์ของผู้ใช้บริการ และสถานที่ web service แสดงออกมา เพื่อการตรวจสอบสถานะผู้ใช้งาน การทดสอบได้มีการทำหลายครั้งโดยใช้ลำดับขั้นตอนในการสร้างรหัสลับ และกำหนดค่าระบบที่ต่างกันในการติดต่อสื่อสารเพื่อให้ได้มาซึ่งค่าการใช้งานของลำดับขั้นนี้

8.2.1 Omar Slomic (2011), A message-level security approach for RESTful services.

งานวิจัยนี้ศึกษา เทคโนโลยี Web Services ได้ถูกวางให้เป็นเทคโนโลยีชั้นนำทางด้านเทคโนโลยีการกระจายหรืออีกชื่อหนึ่งว่าเทคโนโลยีเครือข่าย เทคโนโลยีชนิดนี้ซึ่งได้รับการสนับสนุนจากบริษัท IT ชั้นนำ มีข้อได้เปรียบหลายอย่างในสิ่งแวดล้อมแบบกระจายเช่นการเชื่อมต่อและติดต่อข้อความที่แข็งแกร่ง การค้นหาการบริการ ความน่าเชื่อถือของการแลกเปลี่ยนข้อความและกลไกการรักษาความปลอดภัยขั้นสูง ในทางกลับกันข้อมูลจำเพาะทั้งหมดเหล่านี้ทำให้ Web Services security มีความซับซ้อนมาก ทำให้อุตสาหกรรมซอฟต์แวร์ต่างๆ เกิดปัญหาในการใช้งาน REST based services หรือที่เรียกอีกอย่างว่า RESTful services ซึ่งใช้พื้นฐานของ HTTP ได้ขึ้นมา

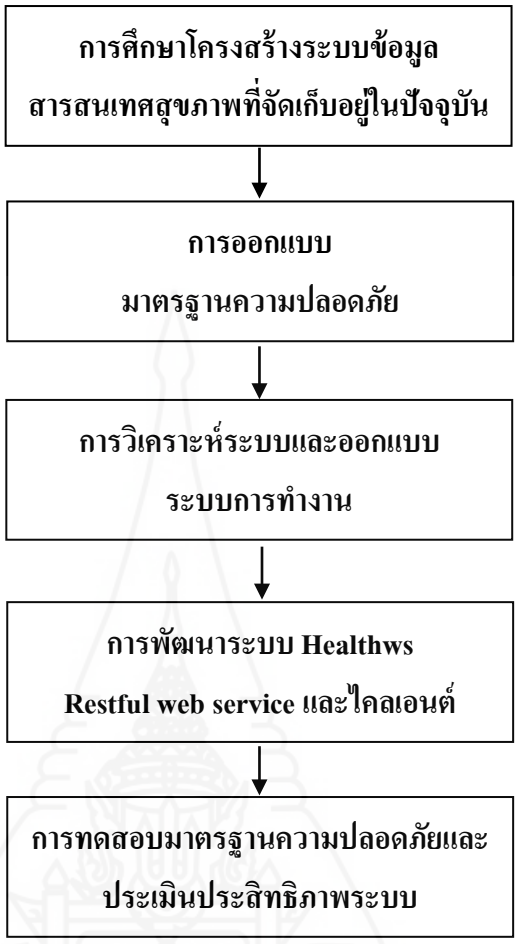
เป็นคู่แข่งของ Web security ซึ่งมีสาเหตุหลักมาจากความเรียบง่ายในการใช้งาน REST based services กำลังถูกนำมาใช้อย่างกว้างขวางโดย บริษัทอุตสาหกรรมขนาดใหญ่รวมทั้ง Microsoft, Yahoo และ Google ซึ่งไม่นิยมการใช้งานของ Web security เนื่องจากข้อดีที่กล่าวไปของ REST based services อย่างไรก็ตาม REST based services ได้รับการวิพากษ์วิจารณ์ว่าขาดฟังค์ชั่นการทำงานที่ Web Services มีโดยเฉพาะอย่างยิ่งระดับการรักษาความปลอดภัยของข้อความ เนื่องจากการรักษาความปลอดภัยเป็นฟังก์ชั่นที่สำคัญมาก จึงอาจทำให้ความแพร่หลายของการใช้งาน REST based services เบนไปในทิศทางเชิงลบ งานวิจัยนี้ได้นำเสนอต้นแบบของการแก้ปัญหาด้านระดับการรักษาความปลอดภัยของข้อความสำหรับ REST based services ส่วนใหญ่ของวิธีการแก้ปัญหานี้ใช้ในการแก้ปัญหาทางเทคนิคและการใช้งานซึ่งรู้จักกันดีคือ กลไกการผสมผสานแพลตฟอร์ม (cross-platform) ซึ่งจะถูกประกอบรวมเข้าด้วยกัน ในขณะที่ส่วนน้อยของการแก้ปัญหากล่าวถึงวิธีการที่ไม่ใช่ด้านเทคนิคเกี่ยวกับการกระจายโทเค็น การพัฒนาต้นแบบโดยส่วนใหญ่จะมุ่งเน้นไปที่การปรับใช้วิธีการแก้ปัญหาจากหลักการและแนวทางของ REST ซึ่งได้แก่ multi-format support (XML or JSON) and light-weight, ความสามารถในการอ่านข้อความได้โดยง่ายของมนุษย์

บทที่ 3
วิธีดำเนินการวิจัย

การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส ดำเนินการตามมาตรฐานตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) และประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ 7 มกราคม 2556 วิธีดำเนินการวิจัยมี 5 ขั้นตอนดังนี้

1. การศึกษาโครงสร้างระบบข้อมูลสารสนเทศสุขภาพที่จัดเก็บอยู่ในปัจจุบัน
2. การออกแบบมาตรฐานความปลอดภัย
3. การวิเคราะห์ระบบและออกแบบระบบการทำงาน
4. การพัฒนาระบบ Healthws Web service System และไคลเอนต์
5. การทดสอบมาตรฐานความปลอดภัย

มีขั้นตอนดำเนินงานตามภาพที่ 3.1



ภาพที่ 3.1 วิธีดำเนินการวิจัยการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส

1. การศึกษาโครงสร้างระบบข้อมูลสารสนเทศสุขภาพที่จัดเก็บอยู่ในปัจจุบัน

โครงสร้างระบบข้อมูลสารสนเทศสุขภาพของจังหวัดนราธิวาสที่จัดเก็บอยู่ในปัจจุบันในระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยจัดเก็บในรูปแบบอิเล็กทรอนิกส์ไฟล์ตามมาตรฐาน 2 รูปแบบ คือ

1.1 โครงสร้างฐานข้อมูลการให้บริการผู้ป่วยนอก การสร้างเสริมสุขภาพและป้องกันโรคในรูปแบบ 21 แฟ้มมาตรฐาน (สำนักนโยบายและยุทธศาสตร์: 2556) ปีงบประมาณ 2556 เวอร์ชั่น 5.0 วันที่ 1 ตุลาคม 2555 กำหนดมาตรฐานโดยสำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข มีข้อมูลที่จัดเก็บดังนี้

1) แฟ้ม PERSON เก็บรายละเอียดข้อมูลบุคคล

2) แฟ้ม DEATH เก็บรายละเอียดการเสียชีวิตของบุคคล

3) แฟ้ม CHRONIC เก็บประวัติการเจ็บป่วยด้วยโรคเรื้อรังของบุคคล (โรคเรื้อรัง หมายถึง โรคติดต่อเรื้อรังและโรคไม่ติดต่อเรื้อรัง)

4) แฟ้ม CARD เก็บรายละเอียดการมีหลักประกันสุขภาพของบุคคล

5) แฟ้ม SERVICE เก็บรายละเอียดการมารับบริการของบุคคลทุกคนทั้งที่อาศัยอยู่ในเขต และที่มาจากนอกเขตรับผิดชอบ

6) แฟ้ม DIAG เก็บรายละเอียดการวินิจฉัยโรคของบุคคลที่มารับบริการทุกคน

7) แฟ้ม APPOINT เก็บรายละเอียดการนัดมารับบริการครั้งต่อไปของบุคคลที่มารับบริการ

8) แฟ้ม SURVEIL เก็บรายละเอียดของข้อมูลโรคที่ต้องเฝ้าระวังจากบุคคลที่มารับบริการ

9) แฟ้ม DRUG เก็บรายละเอียดการให้เวชภัณฑ์แก่ผู้ที่มารับบริการ

10) แฟ้ม PROCED เก็บรายละเอียดการให้บริการหัตถการแก่ผู้ที่มารับบริการ

11) แฟ้ม WOMEN เก็บข้อมูลหญิงวัยเจริญพันธุ์ที่แต่งงานแล้วอยู่กินกับสามี อายุระหว่าง 15-49 ปี

12) แฟ้ม FP เก็บรายละเอียดการให้บริการวางแผนครอบครัว

13) แฟ้ม EPI เก็บรายละเอียดการให้บริการสร้างเสริมภูมิคุ้มกันโรค ทั้งผู้มารับบริการในสถานบริการ และการให้บริการนอกสถานที่

14) แฟ้ม NUTRI เก็บรายละเอียดภาวะโภชนาการของประชากรที่อาศัยอยู่ในเขตรับผิดชอบ (การให้บริการด้านส่งเสริมสุขภาพ)

15) แฟ้ม ANC เก็บรายละเอียดการให้บริการฝากครรภ์

16) แฟ้ม PP เก็บรายละเอียดการให้บริการการดูแลเด็กหลังคลอด

17) แฟ้ม MCH เก็บรายละเอียดประวัติการตั้งครรภ์ การคลอด และการดูแลมารดาหลังคลอด

18) แฟ้ม HOME เก็บรายละเอียดข้อมูลหลังคาเรือนในเขตรับผิดชอบ

19) แฟ้ม NCDSCREEN เก็บข้อมูลการให้บริการคัดกรองโรคเบาหวานและความดันโลหิตสูงสำหรับผู้ที่มารับบริการ และประวัติการได้รับบริการคัดกรองโรคเบาหวาน

20) แฟ้ม CHRONICFU เก็บข้อมูลการตรวจติดตามผู้ป่วยโรคเรื้อรัง (เบาหวาน, ความดันโลหิตสูง)

21) แฟ้ม LABFU เก็บข้อมูลการตรวจทางห้องปฏิบัติการของผู้ป่วยโรคเรื้อรัง (เบาหวาน, ความดันโลหิตสูง)

1.2 โครงสร้างมาตรฐานข้อมูลด้านการแพทย์และสุขภาพ และการส่งต่อผู้ป่วย version 1.0 (สำนักนโยบายและยุทธศาสตร์: 2556) วันที่ 16 มี.ค. 2555

1) แฟ้ม PERSON หมายถึง ข้อมูลทั่วไปของประชาชนในเขตรับผิดชอบและผู้ที่มาใช้บริการ

2) แฟ้ม ADDRESS หมายถึง ข้อมูลที่อยู่ของผู้ที่มารับบริการที่อาศัยอยู่นอกเขตรับผิดชอบ หรือประชาชนที่อาศัยในเขตรับผิดชอบแต่มีทะเบียนบ้านอยู่นอกเขตรับผิดชอบ

3) แฟ้ม DEATH หมายถึง ข้อมูลประวัติการเสียชีวิตของประชาชนทุกคนที่อาศัยในเขตรับผิดชอบ และผู้ป่วยที่มารับบริการ

4) แฟ้ม CHRONIC หมายถึง ข้อมูลผู้ป่วยโรคเรื้อรัง ทุกคนที่อาศัยอยู่ในเขตรับผิดชอบ

5) แฟ้ม CARD หมายถึง ข้อมูลประวัติการมีหลักประกันสุขภาพของประชาชนทุกคนที่อาศัยในเขตรับผิดชอบ และผู้ป่วยที่มารับบริการ

6) แฟ้ม SERVICE หมายถึง ข้อมูลประวัติการมารับบริการของผู้ที่มารับบริการและการให้บริการนอกสถานพยาบาล

7) แฟ้ม DIAGNOSIS_OPD หมายถึง ข้อมูลวินิจฉัยโรคของผู้ป่วยนอกและผู้มารับบริการ

8) แฟ้ม APPOINTMENT หมายถึง ข้อมูลการนัดมารับบริการครั้งต่อไปของผู้ที่มารับบริการ

9) แฟ้ม SURVEILLANCE หมายถึง ข้อมูลผู้ป่วยด้วยโรคที่ต้องเฝ้าระวังที่มารับบริการ

10) แฟ้ม DRUG_OPD หมายถึง ข้อมูลการจ่ายยาสำหรับผู้ป่วยนอกและผู้มารับบริการ

11) แฟ้ม PROCEDURE_OPD หมายถึง ข้อมูลการให้บริการหัตถการและผ่าตัดของผู้ป่วยนอกและผู้มารับบริการ

12) แฟ้ม WOMEN หมายถึง ข้อมูลหญิงวัยเจริญพันธุ์ที่สมรสแล้วทุกคนที่อาศัยอยู่ในเขตรับผิดชอบ

13) แฟ้ม FP หมายถึง ข้อมูลการให้บริการวางแผนครอบครัวกับผู้ที่มารับบริการและหญิงวัยเจริญพันธุ์ในเขตรับผิดชอบ และบริการในสถานพยาบาล

14) แฟ้ม EPI หมายถึง ข้อมูลการให้บริการวัคซีนกับผู้ที่มารับบริการ และประชาชนกลุ่มเป้าหมายของการฉีดวัคซีนในเขตรับผิดชอบ

15) แฟ้ม NUTRITION หมายถึง ข้อมูลการวัดระดับโภชนาการและพัฒนาการเด็กอายุ 0-5 ปี และนักเรียนในเขตรับผิดชอบ

16) แฟ้ม ANC หมายถึง ข้อมูลการให้บริการฝากครรภ์กับหญิงตั้งครรภ์ที่มารับบริการ และประวัติการฝากครรภ์ของหญิงตั้งครรภ์ในเขตรับผิดชอบ

17) แฟ้ม NEWBORN หมายถึง ข้อมูลประวัติการคลอดของทารก ในเขตรับผิดชอบ

18) แฟ้ม NEWBORNCARE หมายถึง ข้อมูลการดูแลทารกหลังคลอด ในเขตรับผิดชอบ

19) แฟ้ม PRENATAL หมายถึง ข้อมูลประวัติการตั้งครรภ์ ของหญิงตั้งครรภ์ในเขตรับผิดชอบ และหญิงตั้งครรภ์ผู้มารับบริการ

20) แฟ้ม LABOR หมายถึง ข้อมูลประวัติการคลอด ของหญิงคลอดในเขตรับผิดชอบ และหญิงคลอดผู้มารับบริการ

21) แฟ้ม POSTNATAL หมายถึง ข้อมูลประวัติการดูแลมารดาหลังคลอด ของหญิงคลอดในเขตรับผิดชอบ และหญิงคลอดผู้มารับบริการ

22) แฟ้ม HOMEหมายถึง ข้อมูลที่ตั้งและสุขาภิบาลของหลังคาเรือนในเขตรับผิดชอบ

23) แฟ้ม NCDSCREEN หมายถึง ข้อมูลการให้บริการคัดกรองโรคเบาหวานและความดันโลหิตสูงสำหรับผู้ที่มารับบริการ และประวัติการได้รับบริการคัดกรองโรคเบาหวานและ

24) แฟ้ม CHRONICFU หมายถึง ข้อมูลการตรวจติดตามผู้ป่วยโรคเรื้อรัง (เบาหวาน ความดันโลหิตสูง)

25) แฟ้ม LABFU หมายถึง ข้อมูลการตรวจทางห้องปฏิบัติการของผู้ป่วยโรคเรื้อรัง (เบาหวาน ความดันโลหิตสูง)

26) แฟ้ม CHARGE_OPD หมายถึง ข้อมูลค่าใช้จ่ายของบริการแต่ละรายการสำหรับผู้ป่วยนอกผู้มารับบริการ

27) แฟ้ม ADMISSION หมายถึง ข้อมูลประวัติการรับผู้ป่วยไว้รักษาในโรงพยาบาล

28) แฟ้ม CHARGE_IPD หมายถึง ข้อมูลค่าใช้จ่ายของบริการแต่ละรายการสำหรับผู้ป่วยใน

29) แฟ้ม DIAGNOSIS_IPD หมายถึง ข้อมูลการจ่ายยาสำหรับผู้ป่วยใน

30) แฟ้ม DRUG_IPD หมายถึง ข้อมูลการจ่ายยาสำหรับผู้ป่วยใน

31) แฟ้ม PROCEDURE_IPD หมายถึง ข้อมูลการให้บริการหัตถการและผ่าตัดของผู้ป่วยใน

32) แฟ้ม PROVIDER หมายถึง ข้อมูลผู้ให้บริการของสถานพยาบาล

33) แฟ้ม SPECIALPP หมายถึง ข้อมูลการให้บริการส่งเสริมสุขภาพป้องกันโรคเฉพาะสำหรับผู้ที่มารับบริการ และประวัติการได้รับบริการส่งเสริมสุขภาพป้องกันโรคเฉพาะ

34) แฟ้ม VILLAGE หมายถึง ข้อมูลทั่วไปและข้อมูลที่เกี่ยวข้องกับสุขภาพของชุมชนที่อยู่ในเขตรับผิดชอบ

35) แฟ้ม ACCIDENT หมายถึง ข้อมูลผู้ป่วยอุบัติเหตุ ที่มารับบริการที่แผนกฉุกเฉิน (ER) ของโรงพยาบาล และแผนกทั่วไปของ รพ.สต.

36) แฟ้ม COMMUNITY_ACTIVITY หมายถึง ข้อมูลการให้บริการในชุมชนสำหรับกลุ่มเป้าหมายในเขตรับผิดชอบ และผู้ป่วยนอกเขตรับผิดชอบ

37) แฟ้ม COMMUNITY_SERVICE หมายถึง ข้อมูลกิจกรรมในชุมชนที่อยู่ในเขตรับผิดชอบ แฟ้ม DENTAL หมายถึง ข้อมูลการตรวจสภาวะทันตสุขภาพของฟันทุกซี่ และข้อมูลวางแผนการส่งเสริม ป้องกันและรักษา ของผู้ที่มารับบริการ ซึ่ง

38) แฟ้ม DISABILITY หมายถึง ข้อมูลผู้พิการ ทุกคนที่อาศัยอยู่ในเขตรับผิดชอบ

39) แฟ้ม DRUGALLERGY หมายถึง ข้อมูลประวัติการแพ้ยาของผู้ป่วยที่มารับบริการ

40) แฟ้ม FUNCTIONAL หมายถึง ข้อมูลการตรวจประเมินความบกพร่องทางสุขภาพ

41) แฟ้ม I CF หมายถึง ข้อมูลการประเมินสภาวะสุขภาพ ความสามารถ และปัจจัยอื่นๆ กลุ่มเป้าหมายที่มารับบริการในโรงพยาบาล

42) แฟ้ม REHABILITATION หมายถึง ข้อมูลการให้บริการฟื้นฟูสมรรถภาพ (ผู้พิการหรือผู้สูงอายุ ที่ช่วยตัวเองไม่ได้)

43) แฟ้ม CARE_REFER หมายถึง ข้อมูลการให้การดูแลผู้ป่วยขณะส่งต่อ หรือส่งกลับ

44) แฟ้ม CLINICAL_REFER หมายถึง ข้อมูลการประเมินทางคลินิกของผู้ป่วยที่ได้รับการส่งต่อ ส่งกลับ หรือตอบกลับ

45) แฟ้ม DRUG_REFER หมายถึง ข้อมูลประวัติการได้รับยา ของผู้ป่วยที่ได้รับการส่งต่อ ส่งกลับ หรือตอบกลับ

46) แฟ้ม INVESTIGATION_REFER หมายถึง ข้อมูลการตรวจทางห้องปฏิบัติการและการตรวจวินิจฉัยอื่นๆ ของผู้ป่วยที่ได้รับการส่งต่อ ส่งกลับ หรือตอบกลับ

47) แฟ้ม PROCEDURE_REFER หมายถึง ข้อมูลประวัติการได้รับการทำหัตถการและผ่าตัด ของผู้ป่วยที่ได้รับการส่งต่อ ส่งกลับ หรือตอบกลับ

48) แฟ้ม REFER_HISTORY หมายถึง ข้อมูลประวัติการส่งต่อผู้ป่วย

49) แฟ้ม REFER_RESULT หมายถึง ข้อมูลผลการตอบรับการส่งต่อ/ส่งกลับ ผู้ป่วย

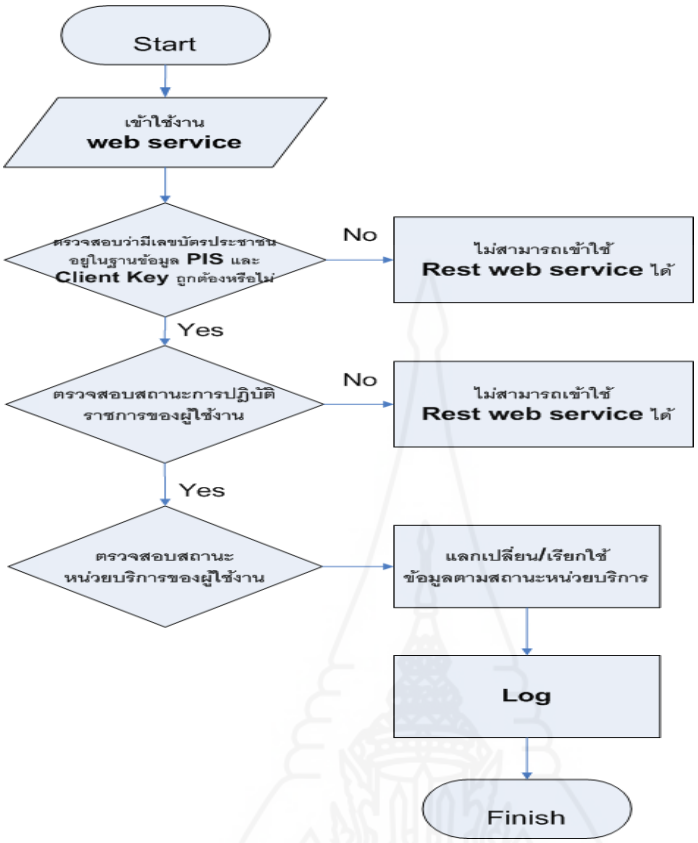
2. การออกแบบมาตรฐานความปลอดภัย

จากที่กล่าวไว้ในบทที่ 1 หัวข้อ 1.1 สถาปัตยกรรมของระบบงานเดิมแล้วว่า การเรียกใช้ข้อมูลผ่านระบบแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสที่ใช้งานอยู่แล้ว (PROVIS web service) เมื่ออ้างอิงตามแบบจำลองโอเอสไอ พบว่าไม่เป็นไปตามตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ที่สมบูรณ์ ดังนั้น ผู้วิจัยจึงได้พัฒนาระบบแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสขึ้นใหม่เพื่อแก้ไขปัญหาที่เกิดขึ้น เรียกว่า ระบบ Healthws System โดยดำเนินการในลำดับชั้นขนส่ง (Transport Layer) ลำดับชั้นส่วนงาน (Session Layer) ลำดับชั้นนำเสนอ (Presentation Layer) และลำดับชั้นการประยุกต์ (Application Layer) รายละเอียดตามหัวข้อ 3.2.1- 3.2.4

2.1 การออกแบบ Flowchart การทำงานของเว็บเซอร์วิส

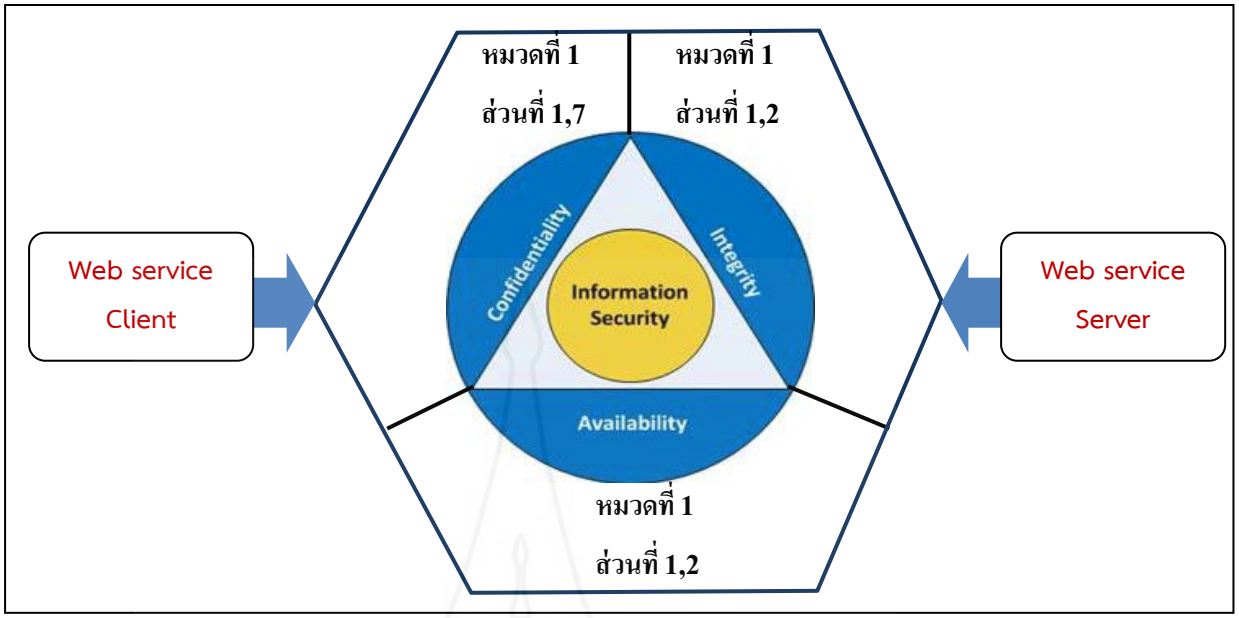
ระบบจะทำการตรวจสอบผู้เข้าใช้งานเว็บเซอร์วิสว่ามีเลขบัตรประจำตัวประชาชนอยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสและค่า Client Key ตรงกับค่า Client Key ของเซิร์ฟเวอร์หรือไม่ ตามภาพที่ 3-2 ถ้าไม่พบข้อมูลเลขบัตรประจำตัวประชาชน หรือค่า Client Key ไม่ถูกต้อง ก็จะไม่อนุญาตให้เข้าใช้งาน ถ้าพบข้อมูลก็จะตรวจสอบว่ายังมีสถานการณ์ปฏิบัติงานอยู่ ณ ปัจจุบันหรือไม่ ถ้าสถานะของการปฏิบัติงานไม่ได้ปฏิบัติงานแล้ว ก็จะไม่อนุญาตให้เข้าใช้งาน ถ้ายังปฏิบัติงานอยู่ก็จะตรวจสอบว่าปฏิบัติงานอยู่ในหน่วยบริการสาธารณสุขแห่งไหน และสถานะของหน่วยบริการสาธารณสุข มีขอบเขตในการแลกเปลี่ยนข้อมูลและการเรียกใช้ข้อมูลเป็นอย่างไร (ตารางที่ 3.4)

ขั้นตอนการทำงานต่อไป ระบบจะให้สิทธิในการเข้าใช้งานเรียกใช้ข้อมูลตามตารางการเรียกใช้ข้อมูลและสถานะหน่วยบริการ (ตารางที่ 3.4 และ ตารางที่ 3.5) หรือ แลกเปลี่ยนข้อมูลตามตารางการแลกเปลี่ยนข้อมูลและสถานะหน่วยบริการ (ตารางที่ 3.6)



ภาพที่ 3.2 Flowchart แสดงการทำงานการเข้าใช้งานของระบบ Healthws System

จากการวิเคราะห์รูปแบบการเรียกใช้และแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส จากภาพที่ 3.3 ผู้วิจัยได้ออกแบบมาตรฐานความปลอดภัยตามมาตรฐานเรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ 7 มกราคม 2556



ภาพที่ 3.3 การออกแบบกรอบงานมาตรฐานความปลอดภัยเว็บเซอร์วิสของสำนักงานสาธารณสุขจังหวัดนราธิวาส

2.2 การรักษาความลับของสารสนเทศ (Confidentiality) มีการควบคุมการเข้าถึงข้อมูลสุขภาพส่วนบุคคลที่เป็นความลับไม่เปิดเผยกับผู้ไม่มีสิทธิ บุคคลผู้มีสิทธิเข้าถึงข้อมูลดังกล่าว คือ เจ้าหน้าที่สาธารณสุขที่มีสถานะของการปฏิบัติงาน ณ ปัจจุบันในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสโดยตรวจสอบค่าเลขบัตรประจำตัวประชาชนและค่า Client Key ที่ถูกต้องเท่านั้น จึงจะสามารถทำการแลกเปลี่ยนหรือเรียกใช้ข้อมูลจากระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล (Healthws System) ได้ ผู้มีสิทธิเข้าถึงข้อมูล มีการทำงาน 2 รูปแบบ คือ

1) การเรียกใช้ข้อมูล สามารถเรียกดูข้อมูลได้เฉพาะข้อมูลของประชาชนที่ขึ้นทะเบียนกับหน่วยบริการนั้น เท่านั้น สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลและนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข โดยมีความสอดคล้องกันดังตารางที่ 3.1

2) การแลกเปลี่ยนข้อมูล สามารถแลกเปลี่ยนกันได้ระหว่างหน่วยบริการสาธารณสุขทุกแห่งภายในจังหวัดนราธิวาส

ตารางที่ 3.1 ความสอดคล้องกันระหว่าง **CIA** Triangle กับนโยบายความปลอดภัย

CIA Triangle	**โยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย านสารสนเทศของกระทรวงสาธารณสุข**
การรักษาความลับของสารสนเทศ (Confidentiality)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

การรักษาความลับของข้อมูลสุขภาพส่วนบุคคล มีการดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุขตามหมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ กำหนดให้ บุคคลผู้มีสิทธิเข้าถึงข้อมูลสุขภาพส่วนบุคคล จะต้องผ่านการตรวจสอบผู้ใช้งาน (Authentication) ต้องเป็นเจ้าหน้าที่สาธารณสุขที่มีสถานะของการปฏิบัติงาน ณ ปัจจุบันในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสโดยตรวจสอบค่าเลขบัตรประจำตัวประชาชนและค่า Client Key ที่ถูกต้องเท่านั้น และต้องมีการพิสูจน์ตัวตนทุกครั้งก่อนเข้าใช้งาน และต้องรับผิดชอบทุกการกระทำ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) ตามภาพที่ 3-4

ภาพที่ 3.4 การรักษาความลับของข้อมูลสุขภาพส่วนบุคคล

การดำเนินการในส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) นั้น ผู้วิจัยได้ออกแบบมาตรฐานความปลอดภัยในการรักษาความลับของสารสนเทศ (Confidentiality) ในลำดับชั้นขนส่ง (Transport Layer) ใช้มาตรฐาน SSL 3.0 / TLS 1.0 เป็นระบบรักษาความปลอดภัยของเว็บเซอร์วิสเซิร์ฟเวอร์เข้ารหัส (encrypt) ข้อมูล ลำดับชั้นส่วนงาน (Session Layer) ใช้การจัดการ Session ลำดับชั้นนำเสนอ

(Presentation Layer) มีการแปลงข้อมูลให้อยู่ในรูปแบบ JSON ด้วยเครื่องมือ PHP Slim Framework และ ลำดับชั้นการประยุกต์ (Application Layer) มีการตรวจสอบผู้ใช้งานร่วมกับฐานข้อมูลระบบบริหารงานบุคคล (PIS)

ผู้วิจัยทำการติดตั้ง openssl-1.0.0d-1.fc13.x86_64 บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ระบบปฏิบัติการ Fedora release 13 (Goddard) ร่วมกับเว็บเซิร์ฟเวอร์ apache 2.2.17 เพื่อการใช้งาน SSL (Secure Sockets Layer) และ TLS (Transport Layer Security)

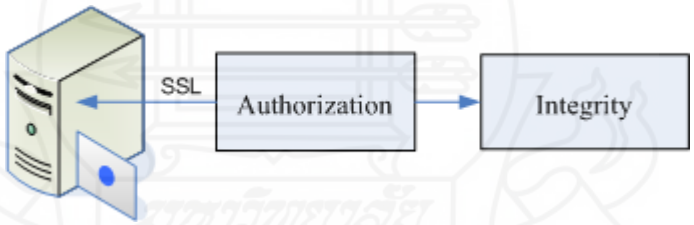
ขั้นตอนการใช้งานเริ่มจาก ผู้ใช้งานเริ่มกระบวนการติดต่อมายังเว็บเซิร์ฟเวอร์ที่มีระบบ SSL หลังจากนั้นเซิร์ฟเวอร์จะส่งใบรับรอง (Server Certificate) รูปแบบมาตรฐาน X.509 กลับไปพร้อมกับการเข้ารหัสด้วยกุญแจสาธารณะ (Public Key) ของเซิร์ฟเวอร์ จากนั้นคอมพิวเตอร์ของผู้รับจะทำการตรวจสอบใบรับรองอีกครั้งหนึ่ง เพื่อตรวจสอบตัวตนของผู้ส่ง และจะทำการสร้างกุญแจสมมาตร (Symmetric Key) โดยการสุ่มและทำการเข้ารหัสกุญแจสมมาตรด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ที่ได้รับมาเพื่อส่งกลับไปยังเซิร์ฟเวอร์ เมื่อได้รับแล้วก็จะทำการถอดรหัสด้วยกุญแจส่วนตัว (Private Key) ก็จะได้กุญแจสมมาตรของผู้รับมาใช้ในการติดต่อสื่อสาร เพื่อให้การติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้อย่างปลอดภัย

2.3 การจัดการด้านความสมบูรณ์ของสารสนเทศ (Integrity) เพื่อเป็นการรับประกันว่าข้อมูลสารสนเทศที่ได้จากเว็บเซอร์วิสระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System นั้นถูกต้องตามความเป็นจริง ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต ได้รับการเข้าถึงหรือปรับปรุงโดยผู้ได้รับสิทธิ (Authorization) เท่านั้น ตามตารางที่ 3.4 แสดงการกำหนดสถานะของหน่วยบริการสาธารณสุข ,ตารางที่ 3.3 แสดงการกำหนดรูปแบบของการแลกเปลี่ยนข้อมูลและสถานะหน่วยบริการ ตารางที่ 3.4 แสดงการกำหนดรูปแบบการเรียกใช้ข้อมูลและสถานะหน่วยบริการ และ ตารางที่ 3.5 แสดงการกำหนดสถานะของการเรียกใช้ข้อมูล สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข โดยมีความสอดคล้องกันตามตารางที่ 3.2

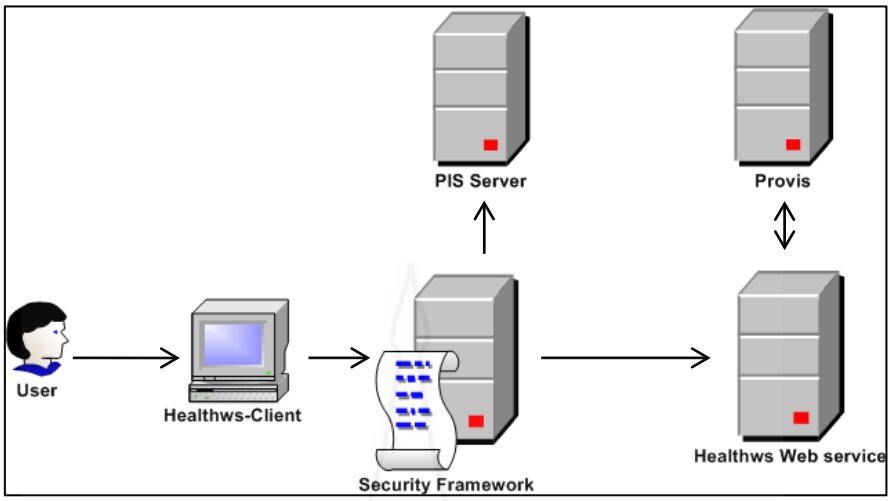
ตารางที่ 3.2 ความสอดคล้องกันระหว่าง **CIA Triangle** กับนโยบายความปลอดภัย

CIA Triangle	**โยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย านสารสนเทศของกระทรวงสาธารณสุข**
ความสมบูรณ์ของสารสนเทศ (Integrity)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (access control) ส่วนที่ 2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน(user access management)

การจัดการด้านความสมบูรณ์ของข้อมูลสุขภาพส่วนบุคคล มีการดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข ตาม หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศในส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (access control) และส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) มีการกำหนดสิทธิการเข้าถึงข้อมูลสุขภาพส่วนบุคคลตามสถานะของหน่วยบริการสาธารณสุขที่ผู้ใช้งานปฏิบัติงานอยู่ ณ ปัจจุบัน โดยตรวจสอบจากฐานข้อมูลระบบบริหารงานบุคคล (PIS) ตามมาตรฐานความปลอดภัยที่ออกแบบไว้ดังภาพที่ 3.5



ภาพที่ 3.5 การจัดการด้านความสมบูรณ์ของข้อมูลสุขภาพส่วนบุคคล



ภาพที่ 3.6 สถาปัตยกรรมของมาตรฐานความปลอดภัยการเรียกใช้ข้อมูลสุขภาพจังหวัดนราธิวาสผ่านเว็บเซอร์วิส

จากภาพที่ 3.6 สถาปัตยกรรมของมาตรฐานความปลอดภัยของการเรียกใช้ข้อมูลสารสนเทศสุขภาพจังหวัดนราธิวาสผ่านเว็บเซอร์วิสมีรูปแบบและขั้นตอนการทำงาน ดังนี้

1) ผู้ใช้งานป้อนชื่อผู้ใช้งาน และรหัสผ่านผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws Client

2) ระบบจะทำการตรวจสอบผู้ใช้งาน และรหัสผ่านมีอยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS) หรือไม่ และค่า Client Key ถูกต้องหรือไม่

3) เมื่อผู้ใช้งานทำการร้องขอข้อมูล จะให้สิทธิในการเข้าถึงข้อมูลตามสถานะของหน่วยบริการที่ผู้ใช้งานนั้นปฏิบัติงานอยู่ โดยกำหนดการแลกเปลี่ยนข้อมูลและและสถานะของหน่วยบริการตามตารางที่ 3.3 จำแนกเป็น 5 สถานะ คือ

ตารางที่ 3.3 สถานะของหน่วยบริการสาธารณสุข

รหัสสถานะ	หน่วยบริการ
1	โรงพยาบาลส่งเสริมสุขภาพตำบลในเครือข่ายบริการเดียวกัน
2	โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลในเครือข่ายบริการเดียวกัน
3	โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลนอกเครือข่ายบริการ
4	โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลนอกเครือข่ายบริการ
5	สำนักงานสาธารณสุขจังหวัดและสำนักงานสาธารณสุขอำเภอ

ผู้วิจัยกำหนดรูปแบบการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลให้ขึ้นอยู่กับสถานะหน่วยบริการสาธารณสุข โดยหน่วยบริการที่มีสถานะเท่ากับ 1 คือโรงพยาบาลส่งเสริมสุขภาพตำบลในเครือข่ายบริการเดียวกัน และหน่วยบริการที่มีสถานะเท่ากับ 2 คือโรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลในเครือข่ายบริการเดียวกัน สามารถเรียกใช้ข้อมูลการรับบริการผู้ป่วยนอก ข้อมูลการบริการสร้างเสริมภูมิคุ้มกันโรคและการรับบริการดูแลหลังคลอดได้เนื่องจากทุกหน่วยบริการมีการให้บริการสาธารณสุขแก่ผู้รับบริการโดยไม่จำกัดภูมิลำเนา รายละเอียดตามตารางที่ 3.4 และตารางที่ 3.5

หน่วยบริการที่มีสถานะเท่ากับ 3 คือ โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลนอกเครือข่ายบริการ หน่วยบริการที่มีสถานะเท่ากับ 4 คือ โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลนอกเครือข่ายบริการ และหน่วยบริการที่มีสถานะเท่ากับ 5 คือ สำนักงานสาธารณสุขจังหวัดและสำนักงานสาธารณสุขอำเภอ สามารถเรียกใช้ข้อมูลการรับบริการผู้ป่วยนอก ข้อมูลการบริการสร้างเสริมภูมิคุ้มกันโรคและการรับบริการดูแลหลังคลอดได้ แต่มีการปกปิดข้อมูลที่ได้รับการคุ้มครอง คือ เลขรหัสบัตรประจำประชาชน , ชื่อ , สกุลไว้ ยกเว้นข้อมูลตามมาตรา 7 ที่หากมีการเปิ□ดเผยแล้วทำให้บุคคลนั้นเสียหายแห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 จะไม่อนุญาตให้มีการเรียกใช้ทุกกรณี

ตารางที่ 3.4 การเรียกใช้ข้อมูลและสถานะหน่วยบริการ

การเรียกใช้ข้อมูล / แฟ้มข้อมูล สถานะสถานบริการ*	การรับบริการผู้ป่วยนอก	การบริการสร้างเสริมภูมิคุ้มกันโรค	การรับบริการดูแลหลังคลอด	หมายเหตุ
1	All	All	All	ไม่เปิดเผยข้อมูลตามมาตรา 7 แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550
2	All	All	All	
3	Any	Any	Any	
4	Any	Any	Any	
5	Any	Any	Any	

ตารางที่ 3.5 สถานะของการเรียกใช้ข้อมูล

สถานะ	การเรียกใช้ข้อมูล
All	สามารถเรียกใช้ข้อมูลของตนเองและข้อมูลของผู้รับบริการทั้งหมด
Any	สามารถเรียกใช้ข้อมูลของตนเองและข้อมูลของผู้รับบริการทั้งหมดแต่มีการปกปิดข้อมูลที่ได้รับการคุ้มครองไว้บางส่วน เช่น เลขรหัสบัตรประจำประชาชน , ชื่อ , สกุล
Deny	สามารถเรียกใช้ข้อมูลของตนเองและไม่สามารถเรียกใช้ข้อมูลของผู้รับบริการได้

ตารางที่ 3.6 การแลกเปลี่ยนข้อมูลและสถานะหน่วยบริการ

การแลกเปลี่ยนข้อมูล / แฟ้มข้อมูล สถานะสถานบริการ*	การรับบริการผู้ป่วยนอก	การบริการสร้างเสริมภูมิคุ้มกันโรค	การรับบริการดูแลหลังคลอด	หมายเหตุ
1	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนได้	แลกเปลี่ยนไม่ได้	
2	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนได้	แลกเปลี่ยนไม่ได้	
3	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนได้	แลกเปลี่ยนไม่ได้	
4	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนได้	แลกเปลี่ยนไม่ได้	
5	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนไม่ได้	แลกเปลี่ยนไม่ได้	

จากตารางที่ 3.6 ผู้วิจัยกำหนดรูปแบบการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลให้ขึ้นอยู่กับสถานะหน่วยบริการสาธารณสุข โดยหน่วยบริการที่มีสถานะเท่ากับ 1 คือโรงพยาบาลส่งเสริมสุขภาพตำบลในเครือข่ายบริการเดียวกัน หน่วยบริการที่มีสถานะเท่ากับ 2 คือโรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลในเครือข่ายบริการเดียวกัน หน่วยบริการที่มีสถานะเท่ากับ 3 คือ โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลส่งเสริมสุขภาพตำบลนอกเครือข่ายบริการ หน่วยบริการที่มีสถานะเท่ากับ 4 คือ โรงพยาบาลส่งเสริมสุขภาพตำบลกับโรงพยาบาลนอกเครือข่ายบริการ สามารถแลกเปลี่ยนข้อมูลการบริการสร้างเสริมภูมิคุ้มกันโรคได้เนื่องจากทุกหน่วยบริการมีการให้บริการสาธารณสุขแก่ผู้รับบริการโดยไม่จำกัดภูมิลำเนา และหน่วยบริการที่มีสถานะเท่ากับ 5 คือ สำนักงานสาธารณสุขจังหวัดและสำนักงานสาธารณสุขอำเภอ ไม่สามารถแลกเปลี่ยนข้อมูลการบริการสร้างเสริมภูมิคุ้มกันโรคเนื่องจากเป็นหน่วยสนับสนุนการปฏิบัติงานที่ไม่มีการให้บริการสาธารณสุข ส่วนข้อมูลการรับบริการผู้ป่วยนอกและข้อมูลการรับบริการดูแลหลังคลอด ยังไม่สามารถแลกเปลี่ยนได้เนื่องจากข้อจำกัดของการวิจัยในบทที่ 1

การออกแบบความปลอดภัยการในการรักษาความคงสภาพของสารสนเทศ (Integrity) พัฒนาด้วยชุดคำสั่งเว็บเซอร์วิสเซิร์ฟเวอร์ พัฒนาด้วยภาษา PHP ที่ชื่อว่า PHP Slim Framework เนื่องจากรองรับการใช้ primary key แบบคีย์ผสม (compound key) ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) และมีการตรวจสอบ Client Key ที่ใช้ในการเชื่อมต่อระหว่างเว็บเซอร์วิสเซิร์ฟเวอร์ กับเว็บเซอร์วิสไคลเอนต์ทุกการให้บริการในการแลกเปลี่ยนข้อมูลกับระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS)

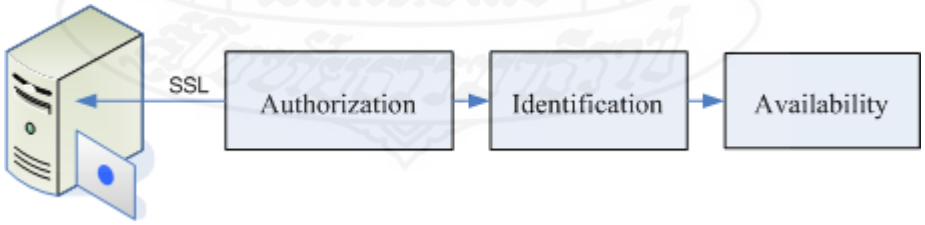
2.4 การจัดการด้านความพร้อมใช้ (Availability) ข้อมูลสารสนเทศที่ได้จากเว็บเซอร์วิสระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System เป็นการรักษาความพร้อมในการใช้งานของข้อมูลสำคัญต่างๆ ที่ต้องพร้อมใช้งานในเวลาที่ต้องการ ซึ่งเป็นข้อมูลที่สามารถเปิดเผยให้ผู้มีสิทธิ์รับทราบได้ เพื่อประโยชน์ในการนำข้อมูลไปใช้งาน สารสนเทศจะถูกเข้าใช้งานหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้นและผ่านการพิสูจน์ตัวตน(Authentication) หากเป็นผู้ใช้ระบบที่ไม่ได้รับอนุญาต การเข้าถึงก็จะล้มเหลวถูกขัดขวาง และการมีการให้สิทธิ์ (Authorization) ตามสถานะของสถานบริการที่ผู้ใช้งานปฏิบัติงานอยู่ในปัจจุบัน โดยด้านกายภาพมีการติดตั้งเครื่องสำรองไฟฟ้า ขนาด 10 กิโลวัตต์ ร่วมกับการบำรุงรักษาเซิร์ฟเวอร์สอดคล้องกับหลักการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข โดยมีความสอดคล้องกันดังตารางที่ 3.7

ตารางที่ 3.7 ความสอดคล้องกันระหว่าง **CIA Triangle** กับนโยบายความปลอดภัย

CIA Triangle	**นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข**
ความพร้อมใช้ (Availability)	หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (access control) ส่วนที่ 2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน(user access management)

การจัดการด้านความพร้อมใช้ของข้อมูลสุขภาพส่วนบุคคล มีการดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข ตาม หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ในส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (Access Control) และส่วนที่ 2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) โดยออกแบบให้

1) ต้องผ่านการพิสูจน์ตัวตน (Identification) มีการพิสูจน์การที่ผู้รับสามารถระบุตัวตนหรือที่มาของข้อมูลได้ว่าผู้ใช้งานเป็นผู้ที่มีสิทธิ์ในการเรียกใช้และแลกเปลี่ยนข้อมูลจากเว็บเซอร์วิส จะต้องเป็นเจ้าหน้าที่สาธารณสุขที่มีข้อมูลอยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสและมีสถานะของการปฏิบัติงานอยู่ในปัจจุบันเท่านั้น ซึ่งวิธีการที่ใช้ระบุตัวตน คือการให้ผู้ใช้กรอกชื่อผู้ใช้ รหัสผ่าน และ Client Key ก่อนเข้าใช้ระบบ ตามภาพที่ 3.7

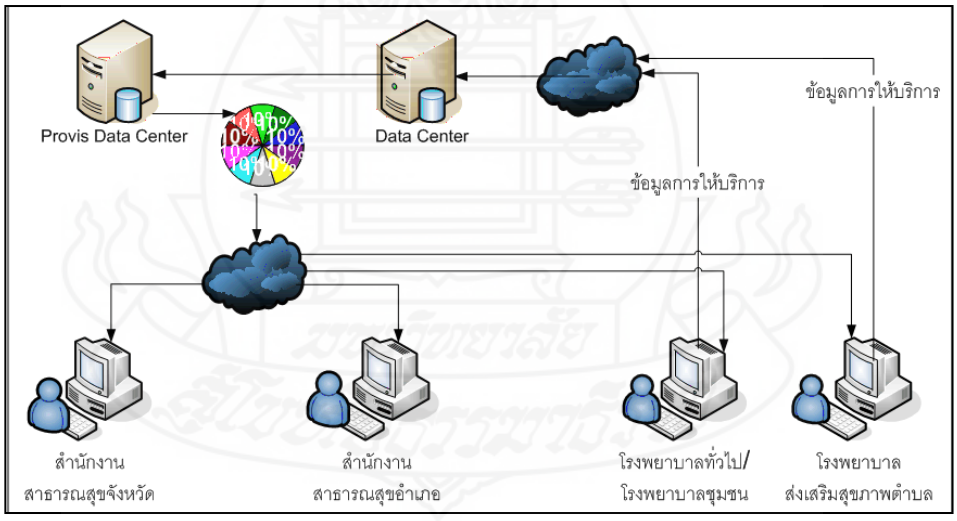


ภาพที่ 3.7 การจัดการด้านความพร้อมใช้ของข้อมูลสุขภาพส่วนบุคคล

2) การให้สิทธิ์ (Authorization) การกำหนดสิทธิ์ให้กับผู้ใช้ที่ผ่านการพิสูจน์ตัวตนว่าสามารถเข้าถึงทรัพยากรที่อยู่ในระบบแลกเปลี่ยนข้อมูลจากเว็บเซอร์วิสได้ และสามารถเข้าถึงข้อมูลอะไรได้บ้าง สามารถลบ หรือแก้ไขข้อมูลได้หรือไม่ เป็นต้น มีการจัดกลุ่มของผู้ใช้งานสถานะสถานบริการเพื่อแบ่งว่าผู้ใช้แต่ละกลุ่มได้รับสิทธิ์อะไรบ้าง โดยผู้ใช้อยู่ในสถานะสถานบริการเท่ากับ 1 จะมีสิทธิ์เข้าถึงส่วนต่างๆ ของระบบแลกเปลี่ยนข้อมูลได้สูงสุด

3. การวิเคราะห์ระบบและออกแบบระบบการทำงาน

การออกแบบระบบอ้างอิงตามการออกแบบมาตรฐานความปลอดภัยในหัวข้อ 3.2 สถานบริการสาธารณสุขในจังหวัดนราธิวาสมีการส่งข้อมูลการให้บริการเข้าสู่ Data Center จังหวัดตลอดเวลา และ Data Center จังหวัดจะทำหน้าที่ประมวลผลข้อมูลข้อมูลให้อยู่ในรูปแบบ 21 แฟ้ม และรูปแบบ 43 แฟ้ม เจ้าหน้าที่ผู้ดูแลระบบฐานข้อมูลจังหวัดจะส่งต่อข้อมูลในรูปแบบ 21 แฟ้ม มาตรฐาน ดังกล่าวไปยังสำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุข และสำนักงานหลักประกันสุขภาพแห่งชาติ เป็นประจำทุกเดือนภายใน 30 วันของเดือนถัดไป ดังภาพที่ 3.8



ภาพที่ 3.8 รูปแบบการส่งข้อมูลจากหน่วยบริการสาธารณสุขกับระบบคลังข้อมูลสุขภาพ (Data Center) ที่ใช้งานปัจจุบัน

ส่วนข้อมูลในรูปแบบ 43 แฟ้ม จะมีระบบงานที่ทำหน้าที่ส่งข้อมูลอัตโนมัติไปยังสำนักนโยบายและยุทธศาสตร์ กระทรวงสาธารณสุขตามกำหนดเวลาที่สามารถตั้งค่าได้ในระบบนี้

การแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลผ่านเว็บเซอร์วิส ตามโครงสร้างฐานข้อมูลการให้บริการผู้ป่วยนอก การสร้างเสริมสุขภาพและป้องกันโรคในรูปแบบ 21 แฟ้มมาตรฐาน ปีงบประมาณ 2556 เวอร์ชั่น 5.0 วันที่ 1 ตุลาคม 2555 จำนวน 1 แฟ้ม คือ แฟ้ม EPI (ข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค)

3.1 ข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค วัคซีนต่างๆ เช่น โปลิโอ คอตีบ ไอกรน บาดทะยัก ฯลฯ ของประชาชนที่ขึ้นทะเบียนไว้กับสถานบริการสาธารณสุขแห่งนี้ แต่ไปรับบริการในสถานบริการสาธารณสุขอื่นๆ ของจังหวัดนราธิวาส เมื่อมีการร้องขอข้อมูลดังกล่าวระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล (Healthws System) เว็บเซอร์วิสจะทำการตรวจสอบข้อมูลและสร้างเป็นชุดข้อมูลอิเล็กทรอนิกส์ในรูปแบบ JSON ส่งกลับมายังฐานข้อมูลการรับบริการของสถานบริการสาธารณสุขที่ประชาชนขึ้นทะเบียนไว้ ทำให้ระบบข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันของโรงพยาบาลส่งเสริมสุขภาพตำบลเป็นปัจจุบัน สามารถประมวลผลรายงานและความครอบคลุมการให้บริการสร้างเสริมภูมิคุ้มกันโรค ตามเกณฑ์เป้าหมายสำนักงานหลักประกันสุขภาพแห่งชาติ เขต 12 สงขลา เช่น เด็กอายุ 1 ปี ที่ได้รับวัคซีนป้องกันโรคคอตีบ ไอกรน บาดทะยัก ซึ่งจะต้องรายงานการได้รับวัคซีน DTP ครบตามเกณฑ์

ข้อมูลที่มีการแลกเปลี่ยน ประกอบด้วยข้อมูลดังนี้

3.1.1 รหัสสถานบริการ

3.1.2 ทะเบียนบุคคล

3.1.3 ลำดับที่

3.1.4 วันที่ให้บริการ

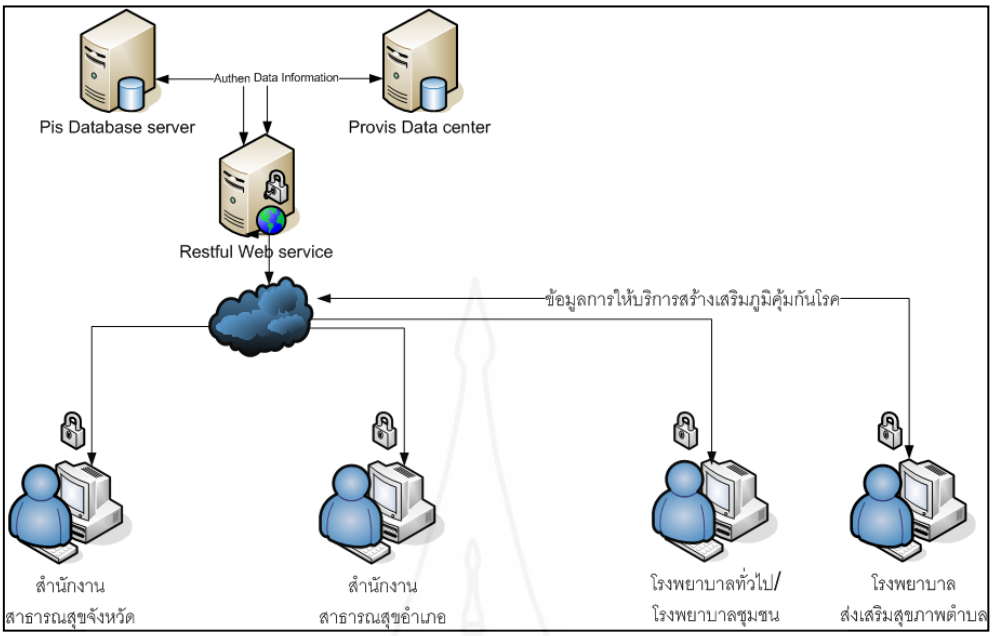
3.1.5 รหัสกิจกรรมวัคซีน

3.1.6 สถานที่รับวัคซีน

3.1.7 วันเดือนปีที่ปรับปรุง

3.1.8 เลขที่บัตรประชาชน

การออกแบบการเรียกใช้และแลกเปลี่ยนข้อมูลขึ้นใหม่ ตามภาพที่ 3.9 โดยมีการตรวจสอบผู้ใช้งานจากระบบบริหารงานบุคคล (PIS) เพื่อให้มีข้อมูลความปลอดภัย และผู้ที่เป็นเจ้าหน้าที่สาธารณสุขของหน่วยบริการสาธารณสุขของจังหวัดนราธิวาสเท่านั้นที่จะมีสิทธิในการเรียกใช้และแลกเปลี่ยนข้อมูลสุขภาพ



ภาพที่ 3.9 การออกแบบรูปแบบเรียกใช้และแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสแบบ REST

การเรียกใช้และแลกเปลี่ยนข้อมูลระหว่างสถานบริการสาธารณสุขที่เป็นโรงพยาบาลทั่วไป โรงพยาบาลชุมชนและโรงพยาบาลส่งเสริมสุขภาพตำบลนั้นเป็นการสื่อสารแลกเปลี่ยนข้อมูลผ่าน REST web service โดยข้อมูลจะอยู่ในรูปแบบ JSON (JavaScript Object Notation) โดยรูปแบบของข้อมูลที่ใช้สำหรับแลกเปลี่ยนข้อมูลที่มีขนาดเล็ก ทำให้มีความรวดเร็วในการรับส่งข้อมูล ผู้ที่มีสิทธิ์ในการเรียกใช้และแลกเปลี่ยนข้อมูลจะต้องเป็นเจ้าหน้าที่สาธารณสุขที่มีชื่ออยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสและมีสถานะการปฏิบัติงานอยู่ในปัจจุบันเท่านั้น และมีการออกแบบความปลอดภัยของชุดโปรแกรมคำสั่งของเว็บเซอร์วิสเซิร์ฟเวอร์ ด้วยวิธีการ Security REST Web Service

3.2 ขั้นตอนการทำงานของการเรียกใช้และแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรคของโรงพยาบาลส่งเสริมสุขภาพตำบล ประกอบไปด้วยลำดับขั้นตอนตามภาพที่ 3.10 ครอบคลุมการให้บริการดังนี้

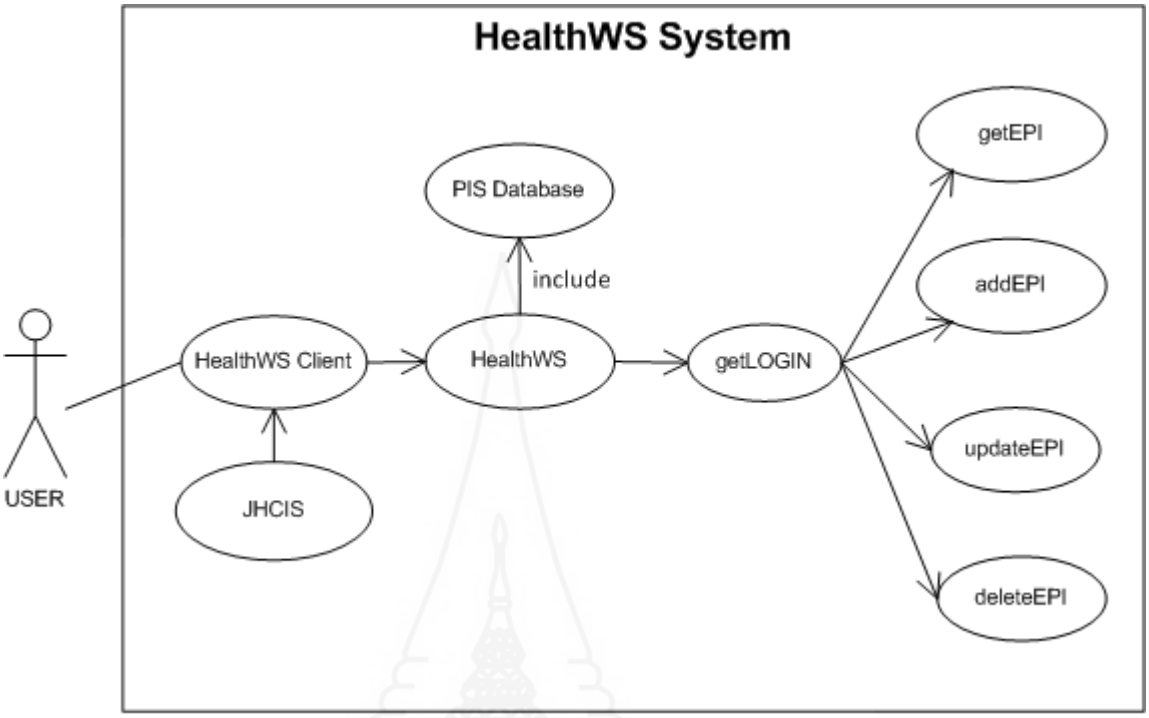
1) getLOGIN ให้บริการตรวจสอบผู้ใช้งาน

2) getEPI ให้บริการเรียกดูข้อมูล

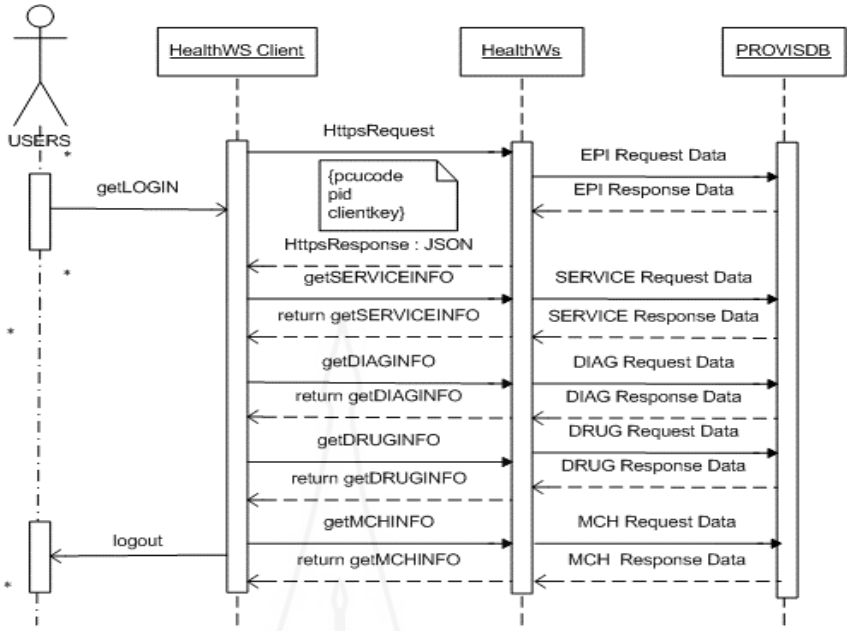
3) addEPI ให้บริการเพิ่มข้อมูล

4) updateEPI ให้บริการแก้ไขข้อมูล

5) deleteEPI ให้บริการลบข้อมูล



ภาพที่ 3.10 แผนภาพยูสเคส (User Case Diagram) ของการเรียกใช้และแลกเปลี่ยนข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล



ภาพที่ 3.11 แผนภาพลำดับเหตุการณ์ (Sequence Diagram) ของการเรียกใช้ข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล

3.3 จากภาพที่ 3.11 เป็นการแสดงลำดับการดำเนินงานของการเรียกใช้ข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล ซึ่งมีขั้นตอนดังนี้

3.3.1 searchEPI ผู้ใช้งาน ทำการร้องขอข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ทั้งหมดโดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลกลับมาแสดงที่ https://healthws.ntwo.moph.go.th

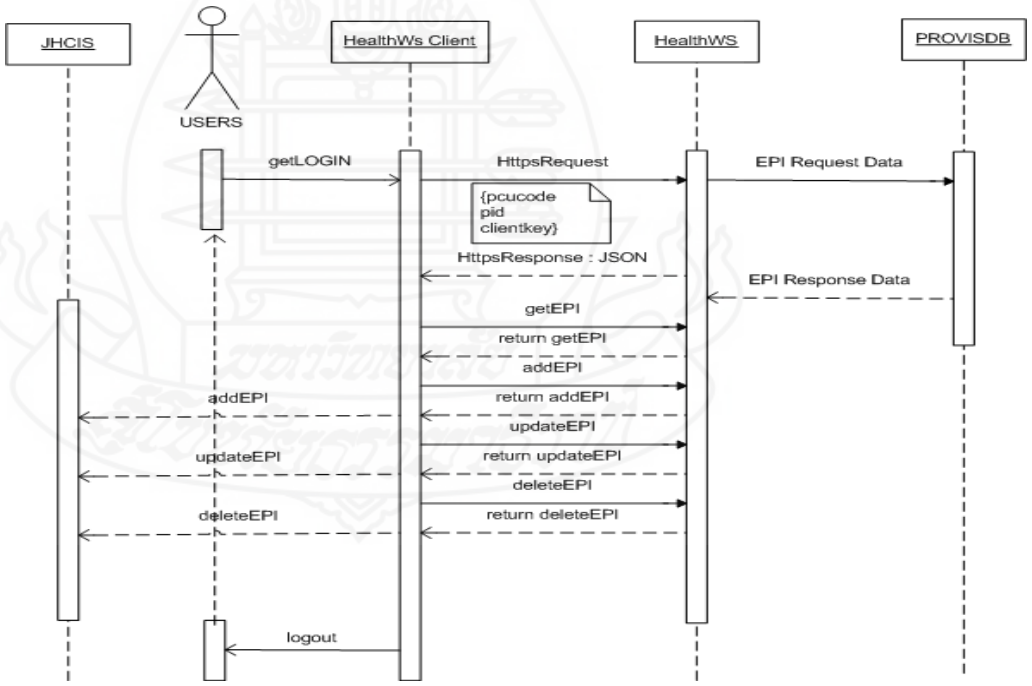
3.3.2 getSERVICEINFO ผู้ใช้งาน ทำการร้องขอข้อมูลการรับบริการรักษาพยาบาลของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ทั้งหมดโดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลวันที่รับบริการ ลำดับที่รับบริการ และหน่วยบริการสาธารณสุขที่ได้รับบริการ กลับมาแสดงที่ https://healthws.ntwo.moph.go.th

3.3.3 getDIAGINFO ผู้ใช้งาน ทำการร้องขอข้อมูลการรับบริการรักษาพยาบาลของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ทั้งหมดโดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ

และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลการวินิจฉัยโรค กลับมาแสดงที่ https://healthws.ntwo.moph.go.th

3.3.4 getDRUGINFO ผู้ใช้งาน ทำการร้องขอข้อมูลการรับบริการรักษาพยาบาลของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ทั้งหมดโดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลการรับเวชภัณฑ์ กลับมาแสดงที่ https://healthws.ntwo.moph.go.th

3.3.5 getMCHINFO ผู้ใช้งานทำการร้องขอข้อมูลการรับบริการดูแลมารดาหลังคลอดของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ทั้งหมดโดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลการรับบริการดูแลมารดาหลังคลอด กลับมาแสดงที่ https://healthws.ntwo.moph.go.th



ภาพที่ 3.12 แผนภาพลำดับเหตุการณ์ (Sequence Diagram) ของการแลกเปลี่ยนข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล

จากภาพที่ 3.12 เป็นการแสดงลำดับการดำเนินงานของการแลกเปลี่ยนข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล ซึ่งมีขั้นตอนดังนี้

ก. getLOGIN ทุกบริการที่มีการร้องขอข้อมูลจะต้องผ่านการตรวจสอบการยืนยันตัวตนกับโอเปอเรชันนี้ โดยจะทำการตรวจสอบว่าเป็นเจ้าหน้าที่สาธารณสุขที่มีข้อมูลอยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS: Personal Information System) ของสำนักงานสาธารณสุขจังหวัดนราธิวาสจึงจะได้รับสิทธิในการร้องขอบริการอื่นๆ จากเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System

ข. getEPI ผู้ใช้งาน ทำการร้องขอข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขอื่นๆ ในจังหวัดนราธิวาส โดยสืบค้นจากรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน โดยผู้ใช้งานสามารถเลือกช่วงเวลาที่ต้องการได้ และเว็บเซอร์วิสเซิร์ฟเวอร์ Healthws System จะส่งข้อมูลกลับมาให้เว็บเซอร์วิสไคลเอนต์ HealthWS Client เพื่อนำเข้ามูลเข้าในฐานข้อมูล JHCIS ของโรงพยาบาลส่งเสริมสุขภาพตำบล และรายงานผลการนำเข้าข้อมูลให้ทราบ

ค. addEPI ผู้ใช้งาน ทำการเพิ่มข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขอื่นๆ ในจังหวัดนราธิวาส ในกรณีที่ยังไม่มีข้อมูลนั้นในแฟ้มข้อมูล EPI ของระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยเพิ่มข้อมูลรหัสหน่วยบริการที่ขึ้นทะเบียน เลขประจำตัวผู้รับบริการ และเลขบัตรประจำตัวประชาชน ชนิดของภูมิคุ้มกันโรคที่ได้รับ และหน่วยบริการที่ได้รับภูมิคุ้มกันโรค และรายงานผลการเพิ่มข้อมูลให้ทราบ

ง. updateEPI ผู้ใช้งาน ทำการปรับปรุง แก้ไขข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่มีอยู่ในฐานข้อมูล JHCIS ของโรงพยาบาลส่งเสริมสุขภาพตำบลและ ระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยปรับปรุง ชนิดของภูมิคุ้มกันโรคที่ได้รับ และหน่วยบริการที่ได้รับภูมิคุ้มกันโรค และรายงานผลการปรับปรุงข้อมูลให้ทราบ

จ. deleteEPI ผู้ใช้งาน ทำการลบข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่มีอยู่ ในฐานข้อมูล JHCIS ของโรงพยาบาลส่งเสริมสุขภาพตำบล และ และรายงานผลการลบข้อมูลให้ทราบ

3.5 ฐานข้อมูลโปรแกรมระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบล พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศ กระทรวงสาธารณสุข ระบบจัดการฐานข้อมูล คือ MySQL 5.0.51b ตารางข้อมูลที่มีการแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิส คือ ตาราง visitepi มีโครงสร้างตามตารางที่ 3.8

ตารางที่ 3.8 โครงสร้างข้อมูลการให้บริการเสริมสร้างภูมิคุ้มกันโรค (visitepi)

ลำดับที่	ชื่อฟิลด์	คีย์	ชนิดข้อมูล	คำอธิบาย
1	pcucodeperson	PK	varchar(9)	รหัสสถานบริการบุคคล
2	Pid	PK	int(11)	รหัสบุคคล
3	dateepi	PK	Date	วันที่รับวัคซีน
4	vaccinecode	PK	char(24)	รหัสวัคซีนที่ได้รับ
5	pcucode	FK	varchar(9)	รหัสสถานบริการ
6	visitno		int(11)	รหัสการบริการ
7	Lotno		varchar(15)	ล็อตวัคซีน
8	datevacineexpire		Date	วันหมดอายุของวัคซีน
9	hosservice	FK	varchar(9)	สถานบริการที่ให้บริการ
10	flag18fileexpo		varchar(1)	สถานะการส่งออก 18 แฟ้ม
11	dateupdate		Datetime	วันที่ปรับปรุงข้อมูลล่าสุด
12	costPKce		decimal(11,0)	ราคาทุน/หน่วย (ของวัคซีน)
13	realPKce		decimal(11,0)	ราคาขาย/หน่วย (ของวัคซีน)

4. การพัฒนาระบบ Healthws Web Service System และไคลเอนต์

มีการออกแบบในส่วนของการตัวให้บริการและตัวเรียกใช้บริการดังนี้

4.1 สร้างเว็บเซอร์วิสเซิร์ฟเวอร์ ด้วยเครื่องมือ PHP Slim Framework

สร้าง http โปรโตคอล ติดต่อสื่อสาร โดยใช้ PHP Slim Framework เพื่อตอบกลับข้อมูลในรูปแบบ JSON กลับไปยังผู้ร้องขอ

4.1.1 เว็บเซอร์วิสเซิร์ฟเวอร์ ให้บริการแลกเปลี่ยนข้อมูล ประกอบด้วย

EPIINFO เซอร์วิส เป็นตัวบริการเว็บที่ให้บริการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคประกอบด้วย Operation ดังต่อไปนี้

getEPI Operation ให้บริการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค โดยสืบค้นจาก รหัสหน่วยบริการ เลขประจำตัวผู้ป่วย และ เลขบัตรประจำตัวประชาชน

addEPI Operation ให้บริการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคโดยการเพิ่มข้อมูลความครอบคลุมการรับบริการ รหัสหน่วยบริการ เลขประจำตัวผู้ป่วย และเลขบัตรประจำตัวประชาชน ชนิดภูมิคุ้มกันโรคที่ได้รับ และหน่วยบริการสาธารณสุขที่ได้รับภูมิคุ้มกันโรค

updateEPI Operation ให้บริการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคโดยปรับปรุงข้อมูล ชนิดภูมิคุ้มกันโรคที่ได้รับ และหน่วยบริการสาธารณสุขที่ได้รับภูมิคุ้มกันโรค

deleteEPI Operation ให้บริการแลกเปลี่ยนข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคโดยลบข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค

searchEPI Operation ให้บริการสืบค้นข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคโดยลบข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค

4.1.2 เว็บเซอร์วิสเซิร์ฟเวอร์ ให้บริการสืบค้นข้อมูล ประกอบด้วย

SERVICEINFO เซอร์วิส เป็นตัวบริการสืบค้นข้อมูลการรับบริการ ประกอบด้วย Operation ดังต่อไปนี้

getSERVICEINFO Operation ให้บริการสืบค้นข้อมูลการรับบริการรักษาพยาบาลทั่วไป ประวัติการรับบริการวินิจฉัยโรค การได้รับยา โดยสืบค้นจาก รหัสหน่วยบริการ เลขประจำตัวผู้ป่วย และ เลขบัตรประจำตัวประชาชน

getMCHINFO Operation ให้บริการสืบค้นข้อมูลการรับบริการดูแลมารดาหลังคลอด โดยสืบค้นจาก รหัสหน่วยบริการ เลขประจำตัวผู้ป่วย และ เลขบัตรประจำตัวประชาชน

4.2 สร้างเว็บเซอร์วิสไคลเอนต์

การสร้างเว็บเซอร์วิสไคลเอนต์สำหรับการร้องขอข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์เริ่มตั้งแต่การประกาศที่อยู่ของ web service และ เชื่อมต่อด้วย Library javax.net.ssl.HttpsURLConnection และ javax.net.ssl.SSLSocketFactory ด้วยมาตรฐานความปลอดภัย SSL รวมทั้งมีการตรวจสอบ Client Key ว่าถูกต้องตรงกันหรือไม่ ถ้าถูกต้อง จะนำข้อมูลส่งเข้าไปในตัวแปร JSON ด้วย Library org.json.JSONArray org.json.JSONException และ org.json.JSONObject ตอบกลับให้กับผู้ร้องขอ

5. การทดสอบมาตรฐานความปลอดภัย

ผู้วิจัยมีการประเมินผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบมาตรฐานความปลอดภัย ของสารสนเทศ (C.I.A) ทั้ง 3 ด้าน ดังนี้

5.1 ด้านการรักษาความลับ (Confidentiality) ทดสอบการเข้าถึงข้อมูล โดยผู้พัฒนาระบบทำการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีและไม่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ทดสอบการเข้าสู่ระบบระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ในรูปแบบต่างๆ การแลกเปลี่ยนข้อมูลด้วย Client Key ที่ถูกต้องและไม่ถูกต้อง

5.2 ด้านการคงสภาพของข้อมูล (Integrity) โดยผู้พัฒนาระบบทำการทดสอบด้วยวิธีการทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี ผู้พัฒนาระบบทำการทดสอบการยืนยันตัวตน การตรวจสอบคีย์ที่ใช้ยืนยันการขอใช้บริการเว็บเซอร์วิส ทดสอบด้วยการดึงข้อมูลทดสอบของผู้รับบริการ โดยจะทดสอบส่วนการร้องขอข้อมูลไปยังเว็บเซอร์วิสเซิร์ฟเวอร์ และส่วนการตอบกลับข้อมูล โดยการเชื่อมต่อด้วยอินเตอร์เน็ต

5.3 ด้านความพร้อมในการใช้งาน (Availability) โดยผู้พัฒนาระบบทดสอบการเข้าไปเรียกใช้ข้อมูลโดยการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล ทดสอบการเรียกใช้ และแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล ผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System

5.4 การประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ (NIST SP 800-44 Guidelines on Securing Public Web Servers) ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ด้วยเครื่องมือ PuTTY version 0.63 , Google Chrome Advanced Rest Client version: 3.1.9 และ Google Chrome Version 45.0.2454.85 m ทำการประเมิน 3 ส่วนคือ

5.4.1 ข้อกำหนดความปลอดภัยของระบบปฏิบัติการ (Checklist for Securing the Web Server Operating System) จากการประเมินระบบปฏิบัติการ Fedora release 13 (Goddard)

5.4.2 ข้อกำหนดความปลอดภัยของเว็บเซิร์ฟเวอร์ (Checklist for Securing the Web Server) จากการประเมิน Apache Web Server version 2.2.17

5.4.3 ข้อกำหนดความปลอดภัยของเนื้อหา (Checklist for Securing Web Content) จากการประเมินระบบ Healthws System

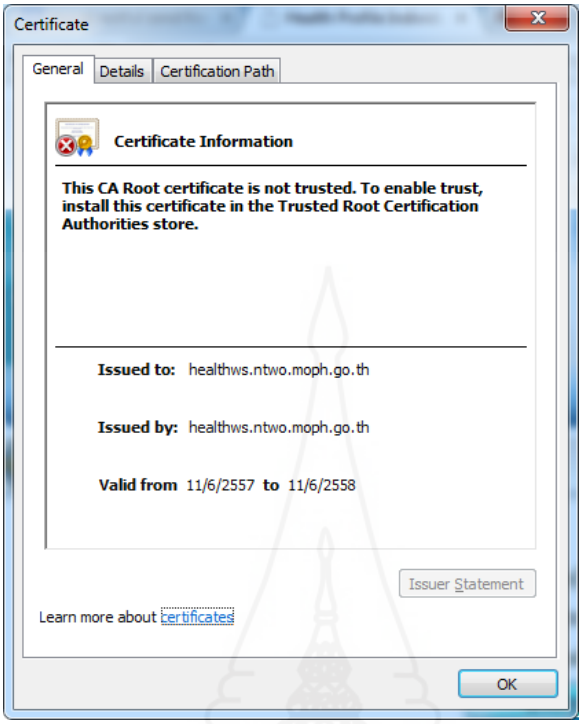
บทที่ 4
ผลการดำเนินงาน

การดำเนินงานออกแบบมาตรฐานความปลอดภัยของการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลผ่านเว็บเซอร์วิสนั้นได้ทำตามขั้นตอนการดำเนินงานต่างๆ ตามแผนที่ได้วางไว้จนเสร็จสมบูรณ์ และผลการดำเนินงานทั้งหมด มีรายละเอียดการดำเนินงานดังนี้

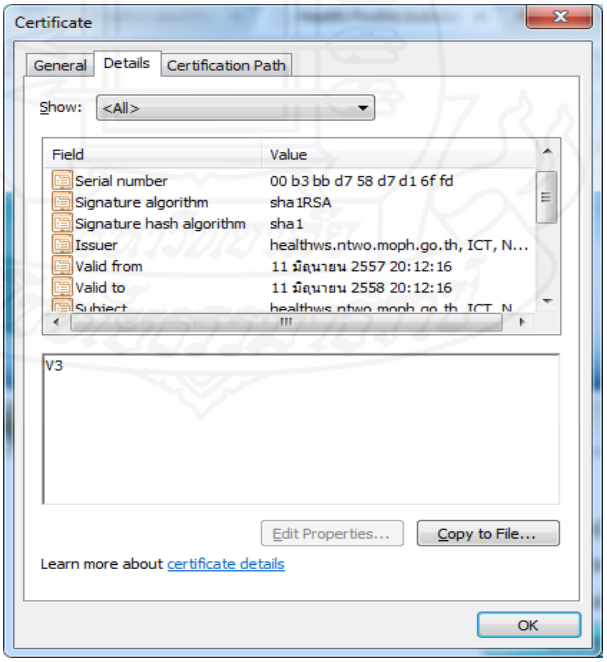
1. ผลการออกแบบมาตรฐานความปลอดภัย
2. ผลการพัฒนาระบบ
3. ผลการทดสอบมาตรฐานความปลอดภัย

1. ผลการออกแบบมาตรฐานความปลอดภัย

จากบทที่ 2 เมื่อศึกษาเทคโนโลยี SSL/TLS และ X.509 Certificate แล้ว ผู้วิจัยได้พัฒนาเว็บเซอร์วิสเซิร์ฟเวอร์เพื่อใช้ในการออกแบบมาตรฐานความปลอดภัย และติดตั้งโปรโตคอล SSL 3.0 และ TLS 1.0 เข้ารหัสด้วยการเข้ารหัสแบบ 128 บิต ใช้ชุดวิธีการเข้ารหัสสำหรับการเชื่อมต่อโดยใช้ AES_128_CBC โดยการเข้ารหัส SHA1 เป็นการเข้ารหัสทางเดียว ไม่สามารถถอดออกมาได้โดยตรง และกลไกการแลกเปลี่ยนกุญแจด้วย DHE_RSA เมื่อนำไปใช้งานจริงสามารถตรวจสอบข้อมูลได้ดังภาพที่ 4.1 และภาพที่ 4.2



ภาพที่ 4.1 ข้อมูลทั่วไปโปรโตคอล SSL/TLS ของเว็บเซอร์วิสเซิร์ฟเวอร์



ภาพที่ 4.2 รายละเอียดโปรโตคอล SSL/TLS ของเว็บเซอร์วิสเซิร์ฟเวอร์

2. ผลการพัฒนาระบบ

จากผลการวิเคราะห์และออกแบบมาตรฐานความปลอดภัยของการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลผ่านเว็บเซอร์วิส และการศึกษาการรักษาความมั่นคงปลอดภัยของสารสนเทศ ผู้วิจัยได้พัฒนาเว็บเซอร์วิสแล้วเสร็จสามารถใช้งานได้จริง ทุกเซอร์วิสที่จะเรียกใช้งานต้องผ่านการพิสูจน์ตัวตน (Authentication) มีการควบคุม Session ที่เข้าใช้งาน ร่วมกับการใช้ Client Key ที่ผู้ดูแลระบบสามารถกำหนดและเปลี่ยนแปลงได้ตลอดเวลา และเซอร์วิสที่มีการเขียนและปรับปรุงข้อมูลจะมีการให้สิทธิ์ (Authorization) เฉพาะผู้ใช้งานที่มีสิทธิ์ในเขียนและปรับปรุงข้อมูลเท่านั้น เพื่อให้เป็นไปตามมาตรฐานความปลอดภัยที่ออกแบบไว้ ผลการพัฒนาระบบมีรายละเอียดดังนี้

2.1 ผลการพัฒนาด้านเว็บเซอร์วิสเซิร์ฟเวอร์

การพัฒนาเว็บเซอร์วิสที่ใช้ในการเรียกใช้และการแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล มีการสร้างเว็บเซอร์วิส ตามองค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ทั้ง 3 ด้าน มีเซอร์วิส getLOGIN ทำหน้าที่ตรวจสอบผู้ใช้งานทุกคน ก่อนที่จะเข้าใช้ไปใช้งานเซอร์วิสอื่นๆ เพื่อแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรค หรือเรียกดูข้อมูลประวัติการรักษาพยาบาลได้ รายละเอียดดังนี้

2.1.1 เซอร์วิส getLOGIN ทำหน้าที่ให้บริการตรวจสอบข้อมูลผู้ใช้งานว่าเป็นเจ้าหน้าที่สาธารณสุขที่มีข้อมูลอยู่ในฐานข้อมูลระบบบริหารงานบุคคล (PIS: Personal Information System) ของสำนักงานสาธารณสุขจังหวัดนราธิวาส มีการทำงานที่ถูกต้องและมีการตอบกลับข้อมูลได้ปกติ

2.1.2 เซอร์วิส getEPI ทำหน้าที่ให้บริการข้อมูลสร้างเสริมภูมิคุ้มกันโรค และส่งผลจากการร้องขอข้อมูลไปยังระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

2.1.3 เซอร์วิส addEPI ทำหน้าที่เพิ่มข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคเข้าไปในฐานข้อมูลระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) ของโรงพยาบาลส่งเสริมสุขภาพตำบล และระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) พร้อมทั้งรายงานผลการเพิ่มข้อมูลให้ทราบ มีการทำงานที่ถูกต้อง

2.1.4 เซอร์วิส updateEPI ทำหน้าที่ปรับปรุง แก้ไขข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่มีอยู่ในฐานข้อมูลระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) ของโรงพยาบาลส่งเสริมสุขภาพตำบล และระบบ

สารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) พร้อมทั้งรายงานผลการปรับปรุง แก้ไขข้อมูลให้ทราบ มีการทำงานที่ถูกต้อง

2.1.5 เซอร์วิส deleteEPI ทำหน้าที่ลบข้อมูลความครอบคลุมการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่มีอยู่ในฐานข้อมูลระบบงานโรงพยาบาลส่งเสริมสุขภาพตำบลและศูนย์สุขภาพชุมชน (JHCIS) ของโรงพยาบาลส่งเสริมสุขภาพตำบล และระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) พร้อมทั้งรายงานผลการลบข้อมูลให้ทราบ มีการทำงานที่ถูกต้อง

2.1.6 เซอร์วิส searchEPI ทำหน้าที่ร้องขอข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ที่มีอยู่ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

2.1.7 เซอร์วิส getSERVICEINFO ทำหน้าที่ร้องขอข้อมูลการรับบริการรักษาพยาบาล วันที่รับบริการ ลำดับที่รับบริการ หน่วยบริการสาธารณสุขที่รับบริการ ของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาสที่มีอยู่ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

2.1.8 เซอร์วิส getDIAGINFO ทำหน้าที่ร้องขอข้อมูลการรับบริการรักษาพยาบาล การวินิจฉัยโรคของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ที่มีอยู่ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

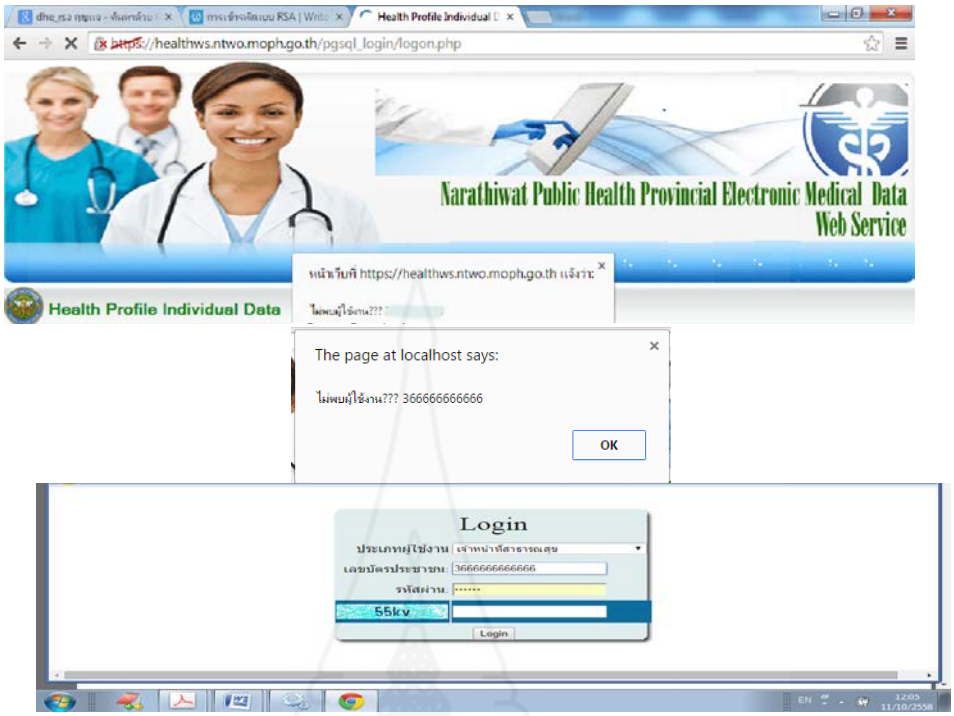
2.1.9 เซอร์วิส getDRUGINFO ทำหน้าที่ร้องขอข้อมูลการรับบริการรักษาพยาบาล ข้อมูลการรับเวชภัณฑ์ ของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ที่มีอยู่ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

2.1.10 เซอร์วิส getMCHINFO ทำหน้าที่ร้องขอข้อมูลการรับบริการดูแลมารดาหลังคลอดของผู้รับบริการที่ขึ้นทะเบียนในหน่วยบริการของตนเองที่ไปรับบริการที่หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส ที่มีอยู่ในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) มีการทำงานที่ถูกต้องและต่อเนื่องกันและมีการแสดงผลข้อมูลได้ปกติ

2.2 ผลการพัฒนาด้านเว็บแอปพลิเคชัน (Web Application)

2.2.1 การเข้าสู่ระบบ เป็นหน้าจอเพื่อให้ผู้ใช้งานกรอกชื่อผู้ใช้งาน และรหัสผ่าน เพื่อทำการยืนยันเข้าใช้งานระบบ โดยสิทธิ์ในการใช้งานระบบ มี 2 กลุ่ม คือ ผู้ดูแลระบบ และกลุ่มผู้ใช้งานทั่วไป แต่ละกลุ่มจะมีเมนูในการใช้งานแตกต่างกัน ภาพที่ 4.3 แสดงหน้าจอการใช้งาน โดยต้องระบุชื่อผู้ใช้ รหัสผ่าน และรหัสสุ่มโดยระบบ (CAPCHA) ให้ถูกต้องและทำการเข้าสู่ระบบ กรณีที่มีการระบุข้อมูลใดไม่ถูกต้องจะมีหน้าต่างข้อความแจ้งเตือนดังภาพที่ 4.4

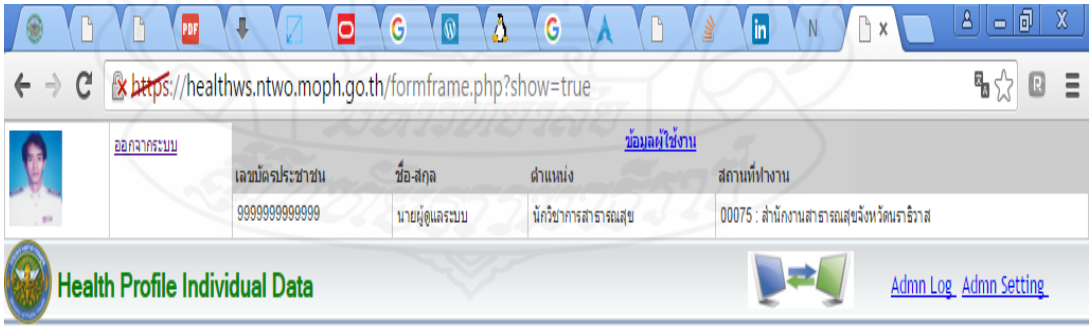
ภาพที่ 4.3 หน้าจอการเข้าสู่ระบบ



ภาพที่ 4.4 หน้าจอแจ้งเตือนเมื่อผู้ใช้งานกรอกข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน

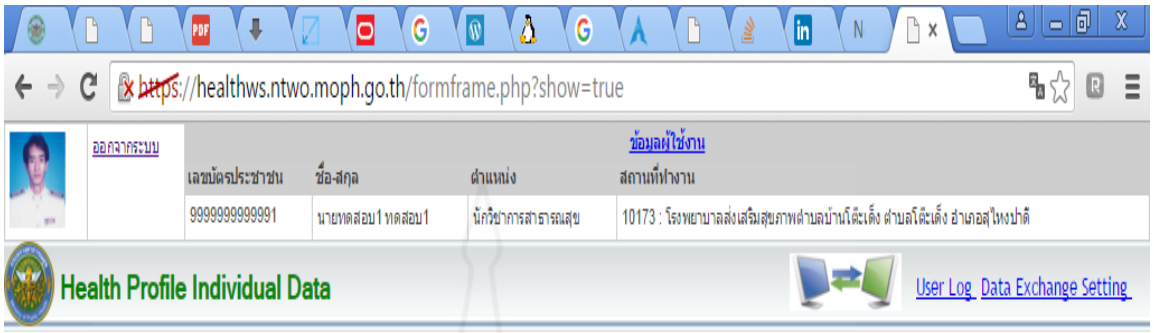
2.2.2 หน้าหลักของระบบ โดยระบบจะแสดงเมนูตามสิทธิ์ของผู้ใช้งาน 2 กลุ่ม คือ

1) ผู้ดูแลระบบ มีเมนูหลัก คือ Admin Setting และ Admin Log ดังภาพที่ 4.5



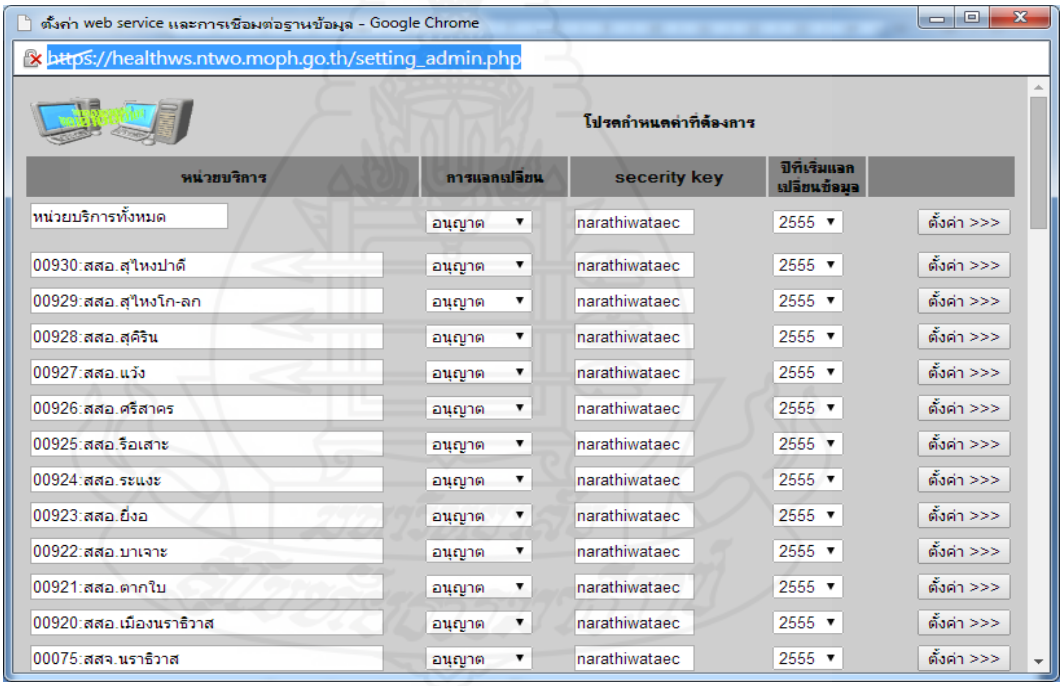
ภาพที่ 4.5 หน้าจอ เมนูหลักผู้ดูแลระบบ

2) ผู้ใช้งาน มีเมนูหลัก คือ Data Exchange Setting และ User Log ดังภาพที่ 4.6



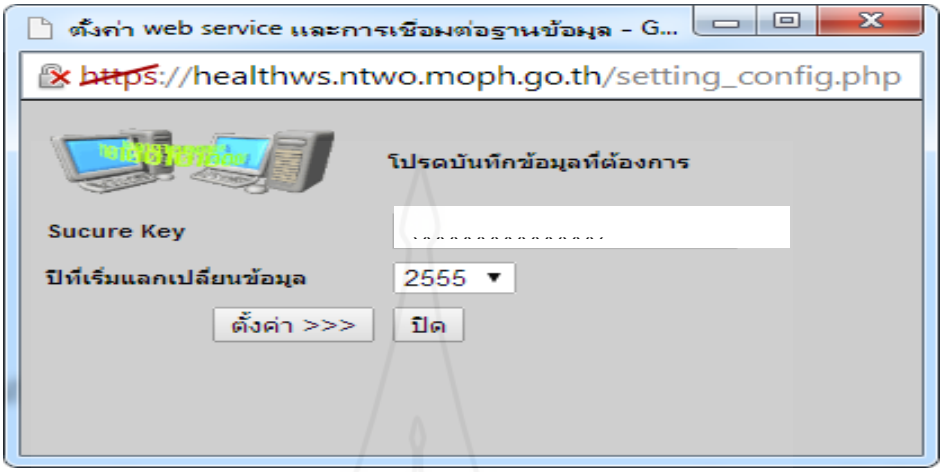
ภาพที่ 4.6 หน้าจอ เมนูหลักผู้ใช้งาน

3) หน้าจอ เมนู Admin Setting ของผู้ดูแลระบบ ดังภาพที่ 4.7



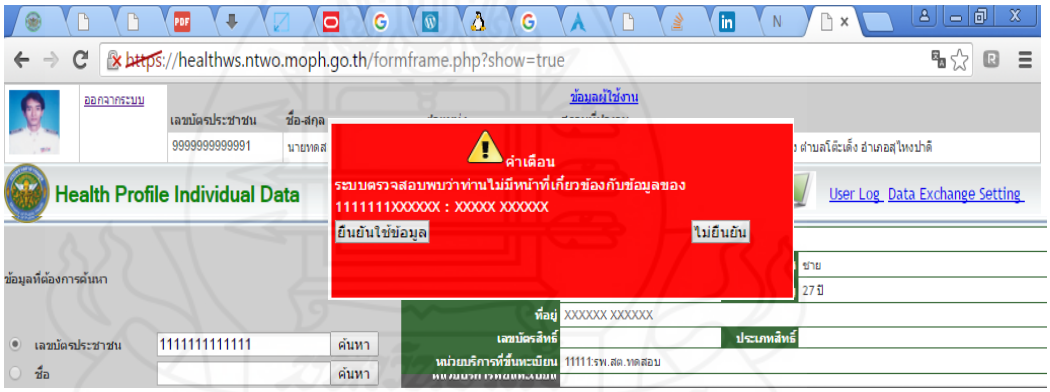
ภาพที่ 4.7 หน้าจอหลักในสิทธิ์ผู้ดูแลระบบ เมนู Admin Setting

ง) หน้าจอ เมนู Data Exchange Setting ของผู้ใช้งาน ดังภาพที่ 4.8



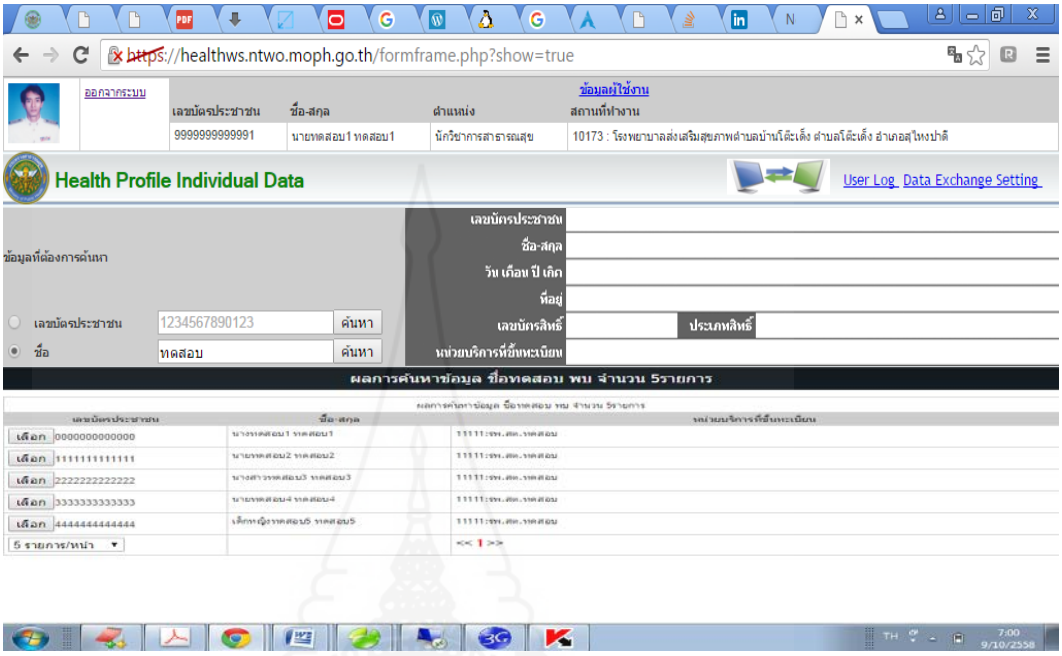
ภาพที่ 4.8 หน้าจอหลักในสิทธิ์ผู้ใช้งาน เมนู Data Exchange Setting

2.2.3 จากภาพที่ 4.9 แสดงการค้นหาข้อมูลโดยใช้เลขบัตรประชาชน



ภาพที่ 4.9 ตัวอย่างการค้นหาข้อมูลโดยใช้เลขบัตรประชาชน

2.2.4 จากภาพที่ 4.10 แสดงการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ



ภาพที่ 4.10 ตัวอย่างการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ

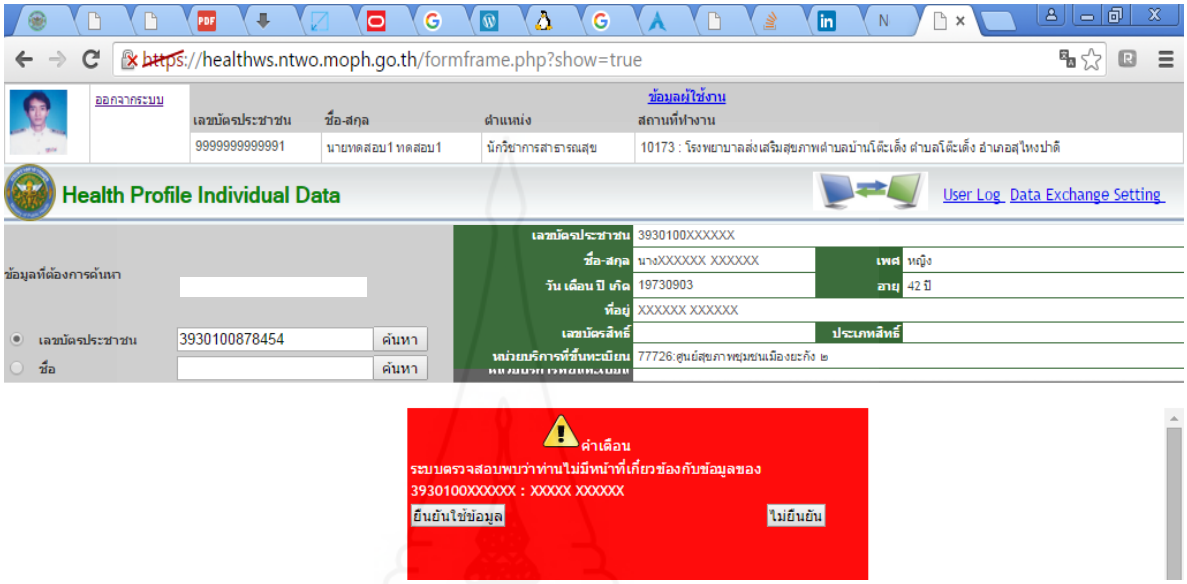
การเรียกใช้ข้อมูลทุกครั้งจะมีการบันทึกข้อมูลเลขบัตรประชาชนผู้ใช้งาน วัน เดือน ปี ที่เรียกใช้ เลขบัตรประชาชนผู้ที่ถูกเรียกดูข้อมูล หมายเลขแมค แอดเดรสที่อยู่ของเครื่องคอมพิวเตอร์ หรือ อุปกรณ์ที่เรียกดูข้อมูล หมายเลขไอพี แอดเดรส ที่อยู่ของเครื่องคอมพิวเตอร์ หรือ อุปกรณ์ที่เรียกดู ไว้ทุกครั้งสำหรับผู้ใช้งาน หรือ ผู้ดูแลระบบจะตรวจสอบประวัติการเรียกดูข้อมูลได้ภายหลัง ตลอดเวลา

จากภาพที่ 4.11 แสดงข้อมูลผู้รับบริการ คือ เลขบัตรประจำตัวปะชาชน ชื่อ-สกุล เพศ วันเดือนปีเกิด อายุ ที่อยู่ เลขที่บัตรสิทธิ์ประกันสุขภาพ ประเภทสิทธิ์ประกันสุขภาพ และหน่วยบริการที่ขึ้นทะเบียนรับผิดชอบไว้ ตามสิทธิ 2 แบบ คือ

1) ผู้ใช้งานเป็นผู้มีสิทธิในการเข้าถึงข้อมูลแบบ All ระบบจะแสดงข้อมูลผู้รับบริการ คือ เลขบัตรประจำตัวปะชาชน ชื่อ-สกุล เพศ วันเดือนปีเกิด อายุ ที่อยู่ เลขที่บัตรสิทธิ์ประกันสุขภาพ ประเภทสิทธิ์ประกันสุขภาพ และหน่วยบริการที่ขึ้นทะเบียนรับผิดชอบไว้

2) ผู้ใช้งานเป็นผู้มีสิทธิในการเข้าถึงข้อมูลแบบ Any เนื่องจากผู้ที่ใช้งานระบบและข้อมูลที่ค้นหาไม่ใช่บุคคลเดียวกัน ระบบจะมีหน้าจอเตือนผู้ที่เข้าใช้งานก่อนเข้าเรียกดูและไม่แสดง

ข้อมูลเลขบัตรประชาชน ชื่อ สกุลและที่อยู่ และให้ยืนยัน หรือไม่ยืนยันการเรียกดูข้อมูลและเก็บข้อมูลของผู้เข้าใช้งานระบบไว้ทั้ง 2 กรณี



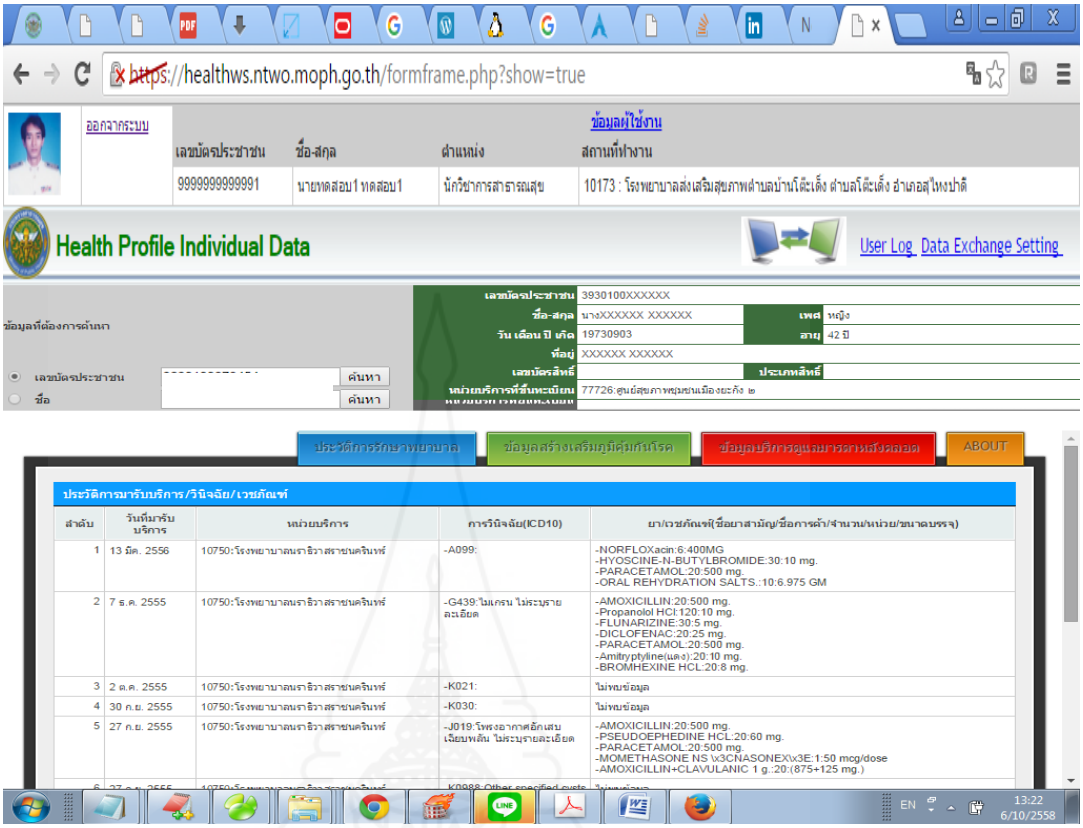
ภาพที่ 4.11 ตัวอย่างผลการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ

จากภาพที่ 4.12 ,4.13 และ 4.14 หากผู้เข้าใช้ระบบยืนยันการเรียกดูข้อมูล ระบบจะแสดงข้อมูลผู้รับบริการ 3 ส่วน คือ

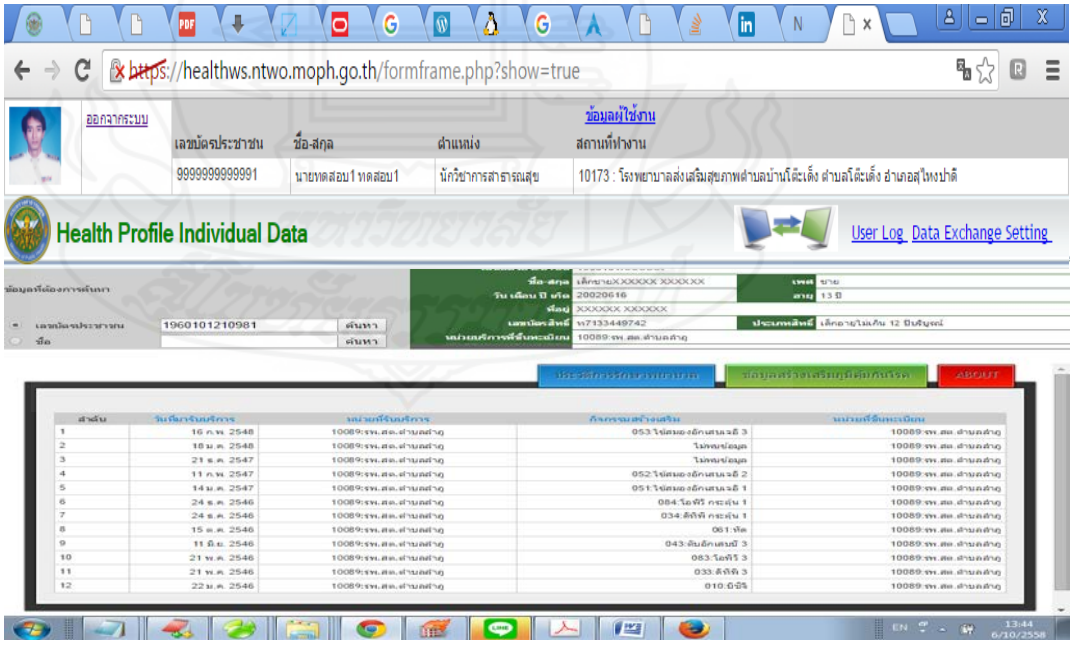
ส่วนที่ 1 ประวัติการรับบริการรักษาพยาบาล ย้อนหลัง 10 ครั้งที่มารับบริการ

ส่วนที่ 2 ประวัติการรับบริการสร้างเสริมภูมิคุ้มกันโรค ย้อนหลัง 10 ครั้งที่มารับบริการ

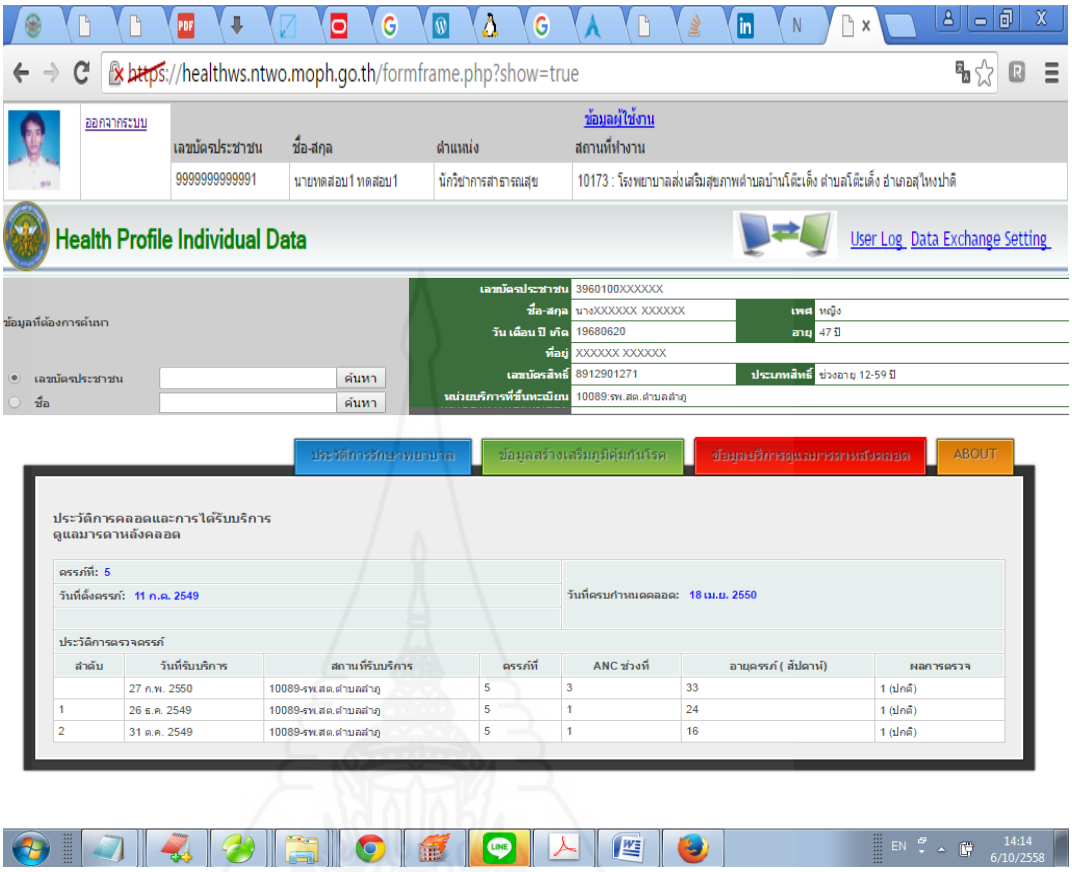
ส่วนที่ 3 ประวัติการรับบริการดูแลมารดาหลังคลอด ย้อนหลัง 10 ครั้งที่มารับบริการ



ภาพที่ 4.12 ข้อมูลประวัติการรับบริการรักษาพยาบาล



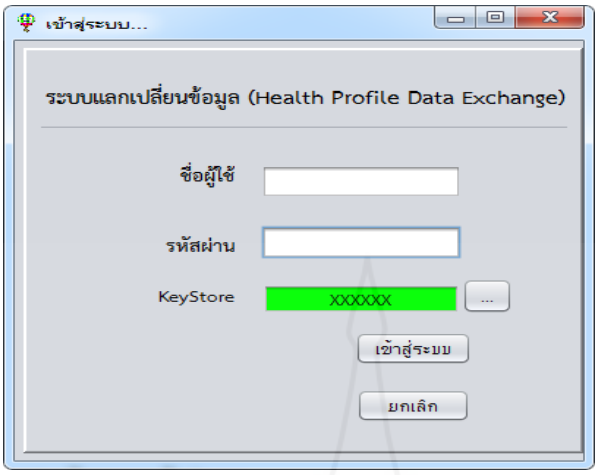
ภาพที่ 4.13 ข้อมูลประวัติการรับบริการสร้างเสริมภูมิคุ้มกันโรค



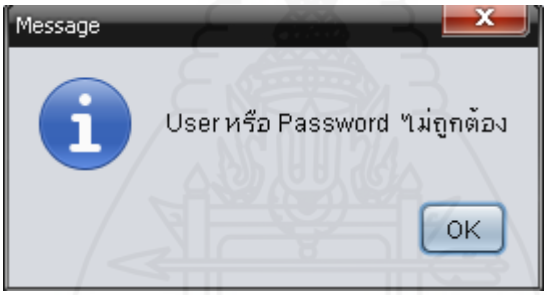
ภาพที่ 4.14 ข้อมูลประวัติการรับบริการดูแลมารดาหลังคลอด

2.3 ผลการพัฒนาด้านแอปพลิเคชัน (Java Application)

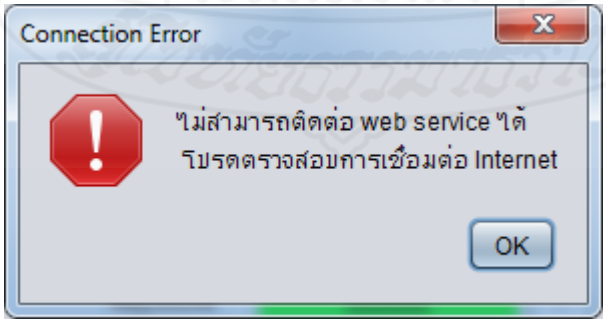
2.3.1 การเข้าสู่ระบบ เป็นหน้าจอเพื่อให้ผู้ใช้งานกรอกชื่อผู้ใช้งาน และรหัสผ่านเพื่อทำการยืนยันเข้าใช้งานระบบ โดยสิทธิ์ในการใช้งานระบบ มี 2 กลุ่ม คือ ผู้ดูแลระบบ และกลุ่มผู้ใช้งานทั่วไป ตามภาพที่ 4.15 แสดงหน้าจอการใช้งานเข้าสู่ระบบ โดยต้องระบุชื่อผู้ใช้ รหัสผ่าน และไฟล์ healthws.keystore ซึ่งใช้ในการติดต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์โดย สามารถติดตั้งไฟล์ healthws.keystore ได้จากผู้ดูแลระบบเว็บเซอร์วิสเซิร์ฟเวอร์ ให้ถูกต้องและทำการเข้าสู่ระบบ กรณีที่มีการระบุข้อมูลใดไม่ถูกต้องจะมีหน้าต่างข้อความแจ้งเตือนดังภาพที่ 4.16 หากไม่สามารถเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ได้ จะมีหน้าจอแจ้งเตือนความผิดพลาดดังภาพที่ 4.17



ภาพที่ 4.15 หน้าจอการเข้าสู่ระบบ HealthwsClient

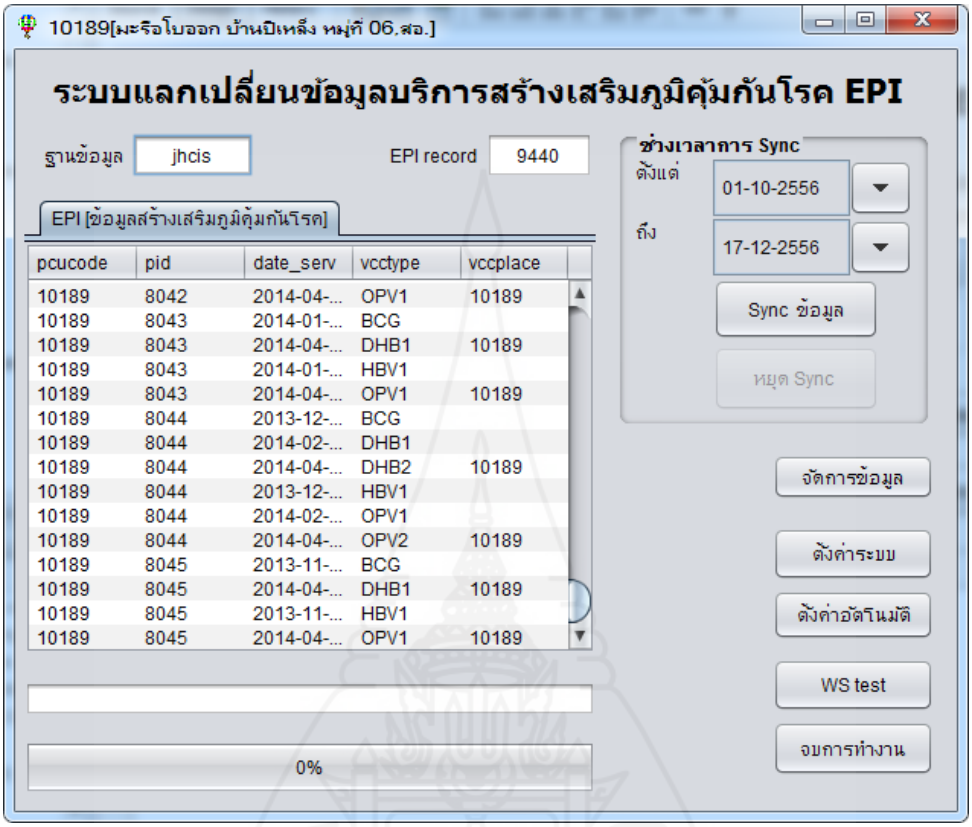


ภาพที่ 4.16 หน้าจอแจ้งเตือนเมื่อผู้ใช้งานกรอกข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน



ภาพที่ 4.17 หน้าจอแจ้งเตือนเมื่อไม่สามารถเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ได้

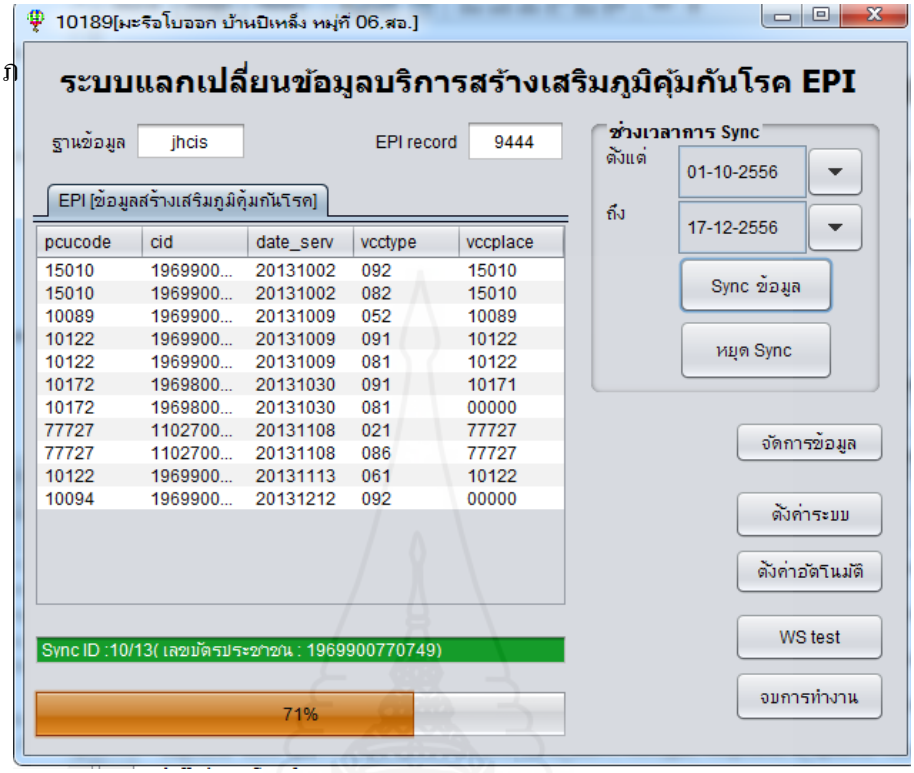
2.3.2 การดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์เข้าสู่ระบบ หน้าจอดังภาพที่ 4.18



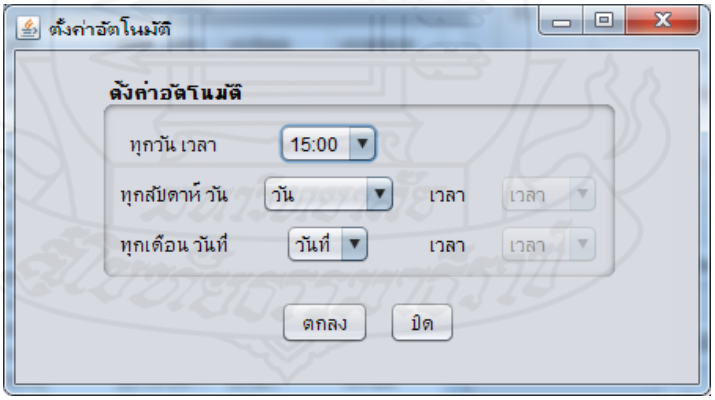
ภาพที่ 4.18 หน้าจอเตรียมพร้อมดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์

ตามภาพที่ 4.19 หากต้องการดึงข้อมูลตามช่วงเวลาที่กำหนด กดปุ่ม Sync ข้อมูล ระบบจะดึงข้อมูลผู้รับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการในเขตรับผิดชอบที่ไปรับบริการที่หน่วยบริการสาธารณสุขอื่นๆ ในจังหวัดนราธิวาสเข้ามาในฐานข้อมูล JHCISDB ของโรงพยาบาลส่งเสริมสุขภาพตำบลทันที โดยใช้ค่า Configuration ที่บันทึกไว้ จากการตั้งค่าจาก ปุ่มตั้งค่าระบบ หรือสามารถตั้งเวลาเพื่อให้ระบบทำการดึงข้อมูลอัตโนมัติได้จากปุ่ม ตั้งค่าอัตโนมัติ ตามภาพที่ 4.20 ซึ่งสามารถตั้งค่าได้ตาม 3 รูปแบบ คือ

1) ดึงข้อมูลอัตโนมัติทุกวัน ต้องระบุเวลา
2) ดึงข้อมูลอัตโนมัติทุกสัปดาห์ ต้องระบุวันและระบุเวลา
3) ดึงข้อมูลอัตโนมัติทุกเดือน ต้องระบุวันที่และระบุเวลา

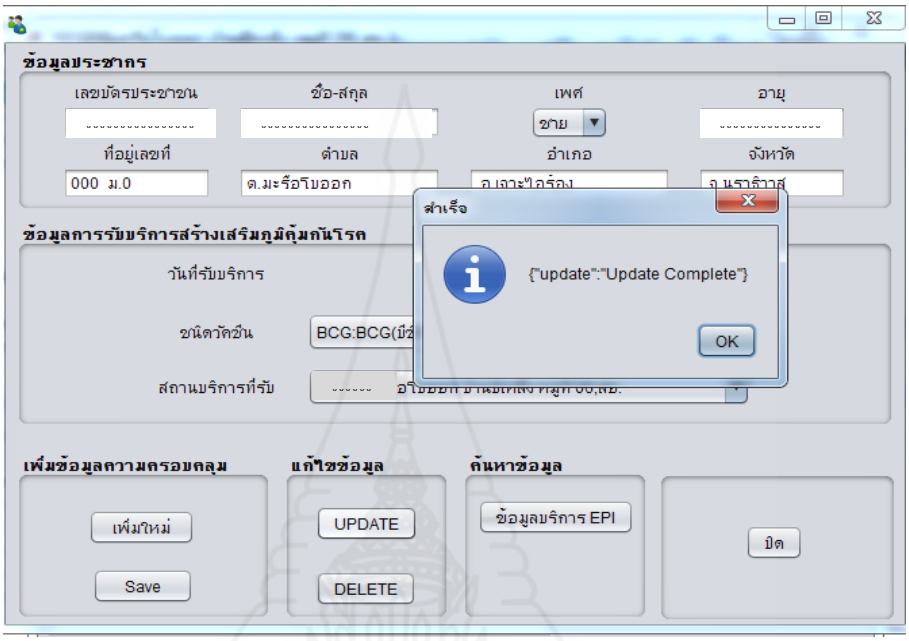


ภาพที่ 4.19 หน้าจอระบบกำลังทำงานดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์



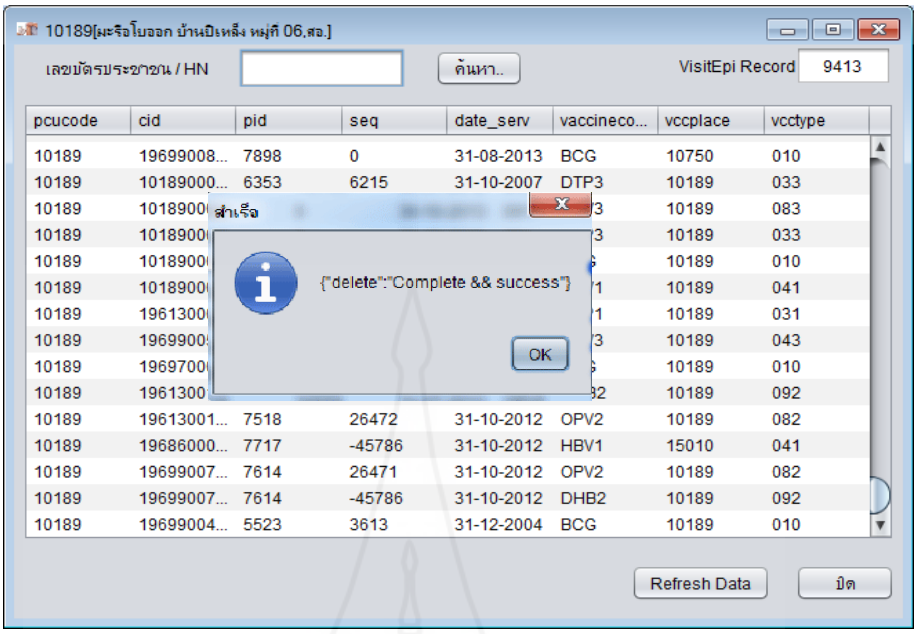
ภาพที่ 4.20 หน้าจอตั้งค่าการดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์โดยอัตโนมัติ

ระบบสามารถทำงานกับ Operation อื่นๆ ของเว็บเซอร์วิสเซิร์ฟเวอร์ได้ เช่น การเพิ่มข้อมูล การปรับปรุงข้อมูล การลบข้อมูลและการค้นหาข้อมูล จากภาพที่ 4.21 เป็นการทำงานโดยเรียกใช้บริการ updateEPI Operation จากเว็บเซอร์วิสเซิร์ฟเวอร์ และข้อมูล



ภาพที่ 4.21 หน้าจอการเรียกใช้ updateEPI Operation จากเว็บเซอร์วิสเซิร์ฟเวอร์

จากภาพที่ 4.21 เป็นการทำงาน โดยเรียกใช้บริการ deleteEPI Operation จากเว็บเซอร์วิสเซิร์ฟเวอร์



ภาพที่ 4.22 หน้าจอการเรียกใช้ deleteEPI Operation จากเว็บเซอร์วิสเซิร์ฟเวอร์

3. ผลการทดสอบการทดสอบมาตรฐานความปลอดภัย

การทดสอบมาตรฐานความปลอดภัยโดยบุคลากรสาธารณสุขที่ปฏิบัติงานประจำโรงพยาบาลส่งเสริมสุขภาพตำบล ของจังหวัดนราธิวาส จำนวน 9 คน (ภาคผนวก ฉ) มีผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบความปลอดภัยของสารสนเทศ

3.1 ด้านการรักษาความลับ (Confidentiality) ทดสอบการเข้าถึงข้อมูล เพื่อทดสอบการเข้าสู่ระบบและการเข้าถึงข้อมูล

3.1.1 ทดสอบระบบ Healthws-Client โดยบุคลากรสาธารณสุข จำนวน 9 คนๆละ 3 ครั้งทดสอบการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่ไม่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ผลการทดสอบไม่สามารถเข้าสู่ระบบได้ และทดสอบการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ผลการทดสอบสามารถเข้าสู่ระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

3.1.2 ทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์ https://healthws.ntwo.moph.go.th/serviceapi/epiinfo.php โดยบุคลากรสาธารณสุข จำนวน 5 คนๆ ละ 3 ครั้ง ด้วยเครื่องมือ Google Chrome Advanced Rest Client ทดสอบการเข้าถึงข้อมูลด้วย Client Key ที่ไม่ถูกต้อง ผลการทดสอบไม่สามารถเข้าถึงข้อมูล

ได้ และ ทดสอบการเข้าถึงข้อมูลด้วย Client Key ที่ถูกต้อง ผลการทดสอบสามารถเข้าถึงข้อมูลสุขภาพส่วนบุคคล ได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

3.2 ด้านการคงสภาพของข้อมูล (Integrity) โดยบุคลากรสาธารณสุข จำนวน 10 คนๆ ละ 3 ครั้ง ทำการทดสอบด้วยวิธีการทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี ผู้พัฒนาระบบทำการทดสอบการยืนยันตัวตน การตรวจสอบคีย์ที่ใช้ยืนยันการขอใช้บริการเว็บเซอร์วิส ทดสอบด้วยการดึงข้อมูลทดสอบของผู้รับบริการ โดยจะทดสอบส่วนการร้องขอข้อมูลไปยังเว็บเซอร์วิสเซิร์ฟเวอร์ และส่วนการตอบกลับข้อมูล โดยการเชื่อมต่อด้วยอินเตอร์เน็ตและอินตราเน็ท ด้วยเครื่องมือ Google Chrome Advanced Rest Client ปรากฏผลการทดสอบตามตารางที่ 4-1 ถึงตารางที่ 4-9

3.2.1 ผลการทดสอบการเรียกใช้เว็บเซอร์วิสจาก URL ที่ทดสอบhttps://healthws.ntwo.moph.go.th/serviceapi/epiinfo.php

1) หมายเลขกรณีทดสอบ SE01 ทดสอบโดย นางผจงพร ทองเชื้อ จำนวน 3 ครั้ง ตามตารางที่ 4.1

ตารางที่ 4.1 กรณีทดสอ SE01

หมายเลขกรณีทดสอบ	SE01	ชื่อ	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น getEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getEPI 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getEPI - Client Key มีค่า ********** - pcucode มีค่า XXXXX		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นางผจงพร ทองเชื้อ		

2) หมายเลขกรณีทดสอบ SE02 ทดสอบโดย นายมะรอซา กูโน จำนวน 3 ครั้ง ตามตารางที่ 4.2

ตารางที่ 4.2 กรณีทดสอบ SE02

หมายเลขกรณีทดสอบ	SE02 ชื่อ ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น addEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน addEPI
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน addEPI 3. กรอกข้อมูลที่ถูกต้องและไม่มีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า addEPI - Client Key มีค่า ********** - pcucode มีค่า 11111 - cid มีค่า 9999999999999 - pid มีค่า 1111111 - date_serv มีค่า 20140623 - vcctype มีค่า 073 - vccplace มีค่า 33333
เงื่อนไขในการทดสอบ	ระบบต้องเพิ่มค่าข้อมูลที่ทำการป้อน
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบต้องเพิ่มค่าข้อมูลที่ทำการป้อนได้
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE
กรณีผิดพลาด	-
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
หมายเหตุ	
ผู้ทดสอบ	นายมะรอซา กูโน

3) หมายเลขกรณีทดสอบ SE03 ทดสอบโดย นายซำสุดิน หามะ จำนวน 3 ครั้ง ตามตารางที่ 4.3

ตารางที่ 4.3 กรณีทดสอบ SE03

หมายเลขกรณีทดสอบ	SE03	ชื่อ	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น updateEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน updateEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน updateEPI 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า updateEPI - Client Key มีค่า ********** - pcucode มีค่า 11111 - cid มีค่า 9999999999999 - pid มีค่า 1111111 - seq มีค่า 123456 - date_serv มีค่า 20140623 - vcctype มีค่า 073 - vccplace มีค่า 33333		
เงื่อนไขในการทดสอบ	ระบบต้องแก้ไขค่าข้อมูลที่ต้องการ		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบต้องแก้ไขค่าข้อมูลที่ต้องการได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นายซำสุดิน หามะ		

4) หมายเลขกรณีทดสอบ SE04 ทดสอบโดย นางสาวสาลินี จงเจตดี จำนวน 3 ครั้ง ตามตารางที่ 4.4

ตารางที่ 4.4 กรณีทดสอบ SE04

หมายเลขกรณีทดสอบ	SE04	**ชื่อ**	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น deleteEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน deleteEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน deleteEPI 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า deleteEPI - Client Key มีค่า ********** - pcucode มีค่า 11111 - pid มีค่า 1111111 - date_serv มีค่า 20140623 - vcctype มีค่า 073		
เงื่อนไขในการทดสอบ	ระบบต้องลบข้อมูลที่ต้องการ		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบต้องลบข้อมูลที่ต้องการได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน		☐ ไม่ผ่าน
หมายเหตุ			
ผู้ทดสอบ	นางสาวสาลินี จงเจตดี		

5) หมายเลขกรณีทดสอบ SE05 ทดสอบโดย นางจันทร์ยา จันทร์คง ตามตารางที่ 4.5

ตารางที่ 4.5 กรณีทดสอบ SE05

หมายเลขกรณีทดสอบ	SE05	ชื่อ	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น searchEPI
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน searchEPI		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน searchEPI 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า searchEPI - Client Key มีค่า ********** - pcucode มีค่า 11111 - pid มีค่า 1111111		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นางจันทร์ยา จันทร์คง		

ผลการทดสอบเว็บเซอร์วิสจาก URL ที่ทดสอบ

https://healthws.ntwo.moph.go.th/serviceapi/servicews.php

6) หมายเลขกรณีทดสอบ SE06 ทดสอบโดย นายอยุทธ มือเสาะ ดังตารางที่ 4.6

ตารางที่ 4.6 กรณีทดสอบ SE06

หมายเลขกรณีทดสอบ	SE06	**ชื่อ**	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น getSERVICEINFO
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getSERVICEINFO		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getSERVICEINFO 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getSERVICEINFO - Client Key มีค่า ********** - pcucode มีค่า 11111 - pid มีค่า 1111111		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน		☐ ไม่ผ่าน
หมายเหตุ			
ผู้ทดสอบ	นายอยุทธ มือเสาะ		

7) หมายเลขกรณีทดสอบ SE07 ทดสอบโดย นายฮุสนัน เจ๊ะอารง ตามตารางที่ 4.7

ตารางที่ 4.7 กรณีทดสอบ SE07

หมายเลขกรณีทดสอบ	SE07	**ชื่อ**	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น getDIAGINFO
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getDIAGINFO		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getDIAGINFO 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getDIAGINFO - Client Key มีค่า ********** - pcucode มีค่า 11111 - seq มีค่า 123456		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นายฮุสนัน เจ๊ะอารง		

8) หมายเลขกรณีทดสอบ SE08 ทดสอบโดย นายเชาวลิต ภู่ทับทิม ตามตารางที่ 4.8

ตารางที่ 4.8 กรณีทดสอบ SE08

หมายเลขกรณีทดสอบ	SE08	ชื่อ	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น getDRUGINFO
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getDRUGINFO		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getDRUGINFO 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getDRUGINFO - Client Key มีค่า ********** - pcucode มีค่า 11111 - seq มีค่า 123456		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นายเชาวลิต ภู่ทับทิม		

9) หมายเลขกรณีทดสอบ SE09 ทดสอบโดย นางสาวจิลาวรรณ เพ็ชรรัตน์ ตามตารางที่ 4.9

ตารางที่ 4.9 กรณีทดสอบ SE09

หมายเลขกรณีทดสอบ	SE09	ชื่อ	ตรวจสอบความถูกต้องในการเรียกใช้ฟังก์ชั่น getMCHINFO
ทดสอบความต้องการ	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน getMCHINFO		
วัตถุประสงค์	เพื่อทดสอบความถูกต้องของข้อมูลที่ได้รับ เมื่อมีการเรียกใช้ฟังก์ชัน ว่ามีความถูกต้องตามที่ระบุไว้ในคู่มือจริงหรือไม่		
คำอธิบาย	1. เขียนโปรแกรมเรียกใช้งานเว็บเซอร์วิส 2. เรียกใช้ฟังก์ชัน getMCHINFO 3. กรอกข้อมูลที่ถูกต้องและมีในฐานข้อมูล โดยให้ค่าของตัวแปรดังนี้ - Operation มีค่า getMCHINFO - Client Key มีค่า ********** - pcucode มีค่า 11111 - cid มีค่า 9999999999999 - pid มีค่า 1111111		
เงื่อนไขในการทดสอบ	ระบบต้องมีค่าข้อมูลที่ทำการค้นหา		
ผลลัพธ์ที่คาดว่าจะได้รับ	ระบบคืนค่าข้อมูลที่ถูกต้องได้		
ผลลัพธ์ที่เกิดขึ้นจริง	ระบบคืนค่าข้อมูลที่ถูกต้อง ตามรูปแบบในเอกสาร A2Z Web Services REST API GUIDE		
กรณีผิดพลาด	-		
ผลการทดสอบ	☑ ผ่าน	☐ ไม่ผ่าน	
หมายเหตุ			
ผู้ทดสอบ	นางสาวจิลาวรรณ เพ็ชรรัตน์		

3.2.2 สรุปผลการทดสอบมาตรฐานความปลอดภัยแยกตามกรณีทดสอบ

ตรวจสอบความถูกต้องของข้อมูล โดยบุคลากรสาธารณสุข จำนวน 14 คนๆ ละ 3 ครั้ง โดยเรียกใช้ในแต่ละฟังก์ชัน การทดสอบกรณีนี้ ในส่วนของการเรียกใช้ข้อมูลจากตาราง EPI ของระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) ทุกฟังก์ชัน ดังนั้น หากฟังก์ชันใดมีจำนวนอิลีเมนต์ขาดหรือเกิน ถือว่าไม่ผ่านในหัวข้อนี้ ผลการทดสอบตามตารางที่ 4.10 ถึง ตารางที่ 4.23 พบว่าผ่านมาตรฐานความปลอดภัยทุกกรณีทดสอบ

ตารางที่ 4.10 การทดสอบความครบถ้วนของข้อมูล

หัวข้อการทดสอบ	a)ตรวจสอบความครบถ้วนของข้อมูลที่ได้จากการเรียกใช้เว็บเซอร์วิส
วิธีการทดสอบ	ใช้การอ้างอิงจากผลลัพธ์ที่ได้ ซึ่งถ้าไม่มีข้อความแสดงข้อผิดพลาด ถือว่าเป็นผลลัพธ์ที่ถูกต้อง และครบถ้วน
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางผจงพร ทองเชื้อ

ตารางที่ 4.11 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	b) ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งค่าข้อมูลที่ไม่ถูกต้องในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบโดยการส่งค่าอินพุตที่ระบบไม่มีผลลัพธ์ เพื่อให้ระบบแสดงข้อความแสดงข้อผิดพลาดกลับมา แล้วตรวจสอบข้อความที่แสดงข้อผิดพลาดกับเอกสารว่ามีความถูกต้องตามเอกสารหรือไม่
ผลการทดสอบ	☑ ผ่าน(ทุกฟังก์ชันมีการส่งข้อความที่แสดงข้อผิดพลาดได้ถูกต้องตามเอกสาร) ☐ ไม่ผ่าน
ผู้ทดสอบ	นายมะรอซา กูโน

ตารางที่ 4.12 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	c)ตรวจสอบการแสดงข้อผิดพลาดเมื่อไม่ส่งค่าข้อมูลในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบโดยไม่ทำการส่งค่าเข้าไปในฟังก์ชัน และคาดหวังให้ระบบแสดงข้อความแสดงข้อผิดพลาดออกมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายซำสุดิน หามะ

ตารางที่ 4.13 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	d)ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งคีย์ Authentication ไม่ถูกต้องในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบโดยการส่งค่า Client Key Authentication ที่ผิดไปให้ระบบ และคาดหวังให้ระบบแจ้งข้อความแสดงข้อผิดพลาดออกมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางสาวสาลินี จงเจตดี

ตารางที่ 4.14 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	e)ตรวจสอบการแสดงข้อผิดพลาดเมื่อไม่มีการส่งคีย์ Authentication ในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบโดยที่ไม่ทำการส่งค่า Client Key Authentication เข้าไปในฟังก์ชัน แต่ยังคงใส่ข้อมูลต่างๆ ครบทุกตัว
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางประจิกศักดิ์ เพชรช่วย

ตารางที่ 4.15 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	f)ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าอินพุตไม่ครบตามจำนวนที่ฟังก์ชันต้องการ
วิธีการทดสอบ	ทดสอบโดยส่งอินพุตไม่ครบ และอ้างอิงตามเอกสาร โดยดูว่าเป็นตัวแปรที่จำเป็นต้องมี (required variables) หรือเป็นตัวแปรที่มีหรือไม่มีก็ได้ (optional variables)
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายอยุทธ มือเสาะ

ตารางที่ 4.16 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	g) ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าอินพุตมากกว่าที่จำนวนที่ฟังก์ชันต้องการในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบกรณีนี้ เพื่อดูผลว่า หากมีการส่งค่าตัวแปรเกินกว่าที่ฟังก์ชันต้องการ หรือส่งค่าตัวแปรที่ซ้ำกันมาให้ ระบบควรจะแสดงข้อความแสดงข้อผิดพลาดกลับมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายสุสนัน เจ๊ะอารง

ตารางที่ 4.17 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	h)ตรวจสอบการแสดงข้อผิดพลาด เมื่อส่งค่าข้อมูลคนละประเภทที่ฟังก์ชันต้องการในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทำการทดลองใส่ค่าตัวแปรคนละประเภทที่ฟังก์ชันต้องการ เช่น จากประเภท num ส่งเป็น String, ประเภท Data ส่งเป็น String ประเภท complex type ส่งเป็น simple type และดู error message
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายเชาวลิต ภู่ทับทิม

ตารางที่ 4.18 การทดสอบค่าของข้อมูล

หัวข้อการทดสอบ	i)ตรวจสอบค่าของข้อมูลเมื่อส่งค่าอินพุตเป็น Null ในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทำการทดลองใส่ค่าที่ฟังก์ชันต้องการให้เป็นค่าเป็น “Null” ฟังก์ชันไม่ควรที่จะทำงานได้ตามปกติ และควรส่ง error message กลับมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางสาวจิลาวรรณ เพ็ชรรัตน์

ตารางที่ 4.19 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	j) ตรวจสอบการแสดงข้อผิดพลาดเมื่อส่งค่าอินพุตเป็น Null ในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทำการทดลองเมื่อส่งค่าอินพุตเป็น “Null” ฟังก์ชันไม่ควรที่จะทำงานได้ตามปกติ และควรส่ง error message กลับมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายแอมะ มะเซ็ง

ตารางที่ 4.20 การทดสอบความถูกต้องของข้อมูล

หัวข้อการทดสอบ	k) ตรวจสอบความถูกต้องของข้อมูลเมื่อข้อมูลเป็นชนิดข้อมูลที่ซับซ้อนในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดสอบผลลัพธ์ที่ได้ในแต่ละฟังก์ชันว่าเป็นข้อมูลชนิดซับซ้อนหรือไม่
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางประจิกศักดิ์ เพชรช่วย

ตารางที่ 4.21 การทดสอบการแสดงข้อผิดพลาด

หัวข้อการทดสอบ	l)ตรวจสอบการแสดงข้อผิดพลาดเมื่อผู้ใช้ขอบริการข้อมูลที่ไม่มีให้บริการในแต่ละฟังก์ชัน
วิธีการทดสอบ	ทดลองใส่ข้อมูลที่ฟังก์ชันไม่มีผลลัพธ์ให้ และจะต้องทำการส่งข้อความแสดงข้อผิดพลาดกลับมา
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นางอุไร พจน์เพริศ

ตารางที่ 4.22 การทดสอบรูปแบบของชนิดข้อมูล JSON

หัวข้อการทดสอบ	m) ตรวจสอบรูปแบบของชนิดข้อมูล JSON ว่าถูกต้องตามโครงสร้างของข้อมูลหรือไม่ ชนิดข้อมูลที่ได้กลับมา มีความถูกต้องหรือไม่
วิธีการทดสอบ	ทดสอบเรียกใช้ข้อมูลจากเว็บเซอร์วิส ผลลัพธ์รูปแบบของชนิดข้อมูล JSON ว่าถูกต้องตามโครงสร้างของข้อมูลหรือไม่ ชนิดข้อมูลที่ได้กลับมา มีความถูกต้องหรือไม่
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายสุวัฒน์ ทองเล็ก

ตารางที่ 4.23 การทดสอบความพร้อมในการใช้งาน

หัวข้อการทดสอบ	n)ทดสอบความพร้อมในการใช้งาน (Availability)
วิธีการทดสอบ	ทดสอบการเข้าไปเรียกใช้ข้อมูลโดยการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ทดสอบการเรียกใช้ และ แลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคลผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System
ผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
ผู้ทดสอบ	นายมูฮัมมัดตารมีซี สาแม

3.2.3 ผลการประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ โดยการประเมินตามข้อกำหนด NIST SP 800-44 Guidelines on Securing Public Web Servers ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ประเมินโดย นักวิชาการคอมพิวเตอร์ สำนักงานสาธารณสุขจังหวัดนราธิวาส (ภาคผนวก ฉ) ทำการประเมิน 3 ส่วน ปรากฏผลดังนี้

1) ข้อกำหนดความปลอดภัยของระบบปฏิบัติการ (Checklist for Securing the Web Server Operating System) จำนวน 20 ข้อกำหนด จากการประเมินระบบปฏิบัติการ Fedora release 13 (Goddard) โดยใช้เครื่องมือ PuTTY version 0.63 มีการดำเนินการครบทุกข้อกำหนด รายละเอียดตามตารางที่ 4.24

ตารางที่ 4.24 ผลการประเมินมาตรฐานความปลอดภัยของระบบปฏิบัติการ

ผลการประเมิน	กิจกรรม
	ซอฟต์แวร์เพิ่มเติม และการปรับปรุงระบบปฏิบัติการ
ดำเนินการ	1.สร้างเอกสารและการติดตั้งซอฟต์แวร์เพิ่มเติม
ดำเนินการ	2.ตัดการเชื่อมต่อของเซิร์ฟเวอร์จากเครือข่ายจนกว่าซอฟต์แวร์เพิ่มเติมทั้งหมดได้รับ
	การติดตั้งเสร็จ
ดำเนินการ	3.ตรวจสอบ / ติดตั้งโปรแกรมที่จำเป็นทั้งหมดและอัพเกรดระบบปฏิบัติการ
ดำเนินการ	4.ตรวจสอบ/ติดตั้งซอฟต์แวร์ปรับปรุงที่จำเป็นทั้งหมดและอัพเกรดโปรแกรม
	ประยุกต์และเซอร์วิสที่มาพร้อมกับระบบปฏิบัติการ
ดำเนินการ	5.ระบุและปิดช่องโหว่ที่ยังไม่ได้แก้ไขใด ๆ
	การถอดถอนหรือปิดบริการที่ไม่จำเป็นและการใช้งาน
ดำเนินการ	6.ปิดการใช้งานโปรแกรมประยุกต์หรือลบเซอร์วิสที่ไม่จำเป็นและการใช้งาน
	การกำหนดค่าเพื่อการตรวจสอบผู้ใช้ระบบปฏิบัติการ
ดำเนินการ	7.ลบหรือปิดการใช้งานของผู้ใช้งานที่ไม่จำเป็นและกลุ่มที่ไม่จำเป็น
ดำเนินการ	8.ปิดการใช้งานผู้ใช้งานที่ไม่มีกิจกรรมการใช้งาน
ดำเนินการ	9.สร้างกลุ่มผู้ใช้งานสำหรับคอมพิวเตอร์เพื่อแยกกลุ่ม
ดำเนินการ	10.สร้างรายชื่อผู้ใช้งานสำหรับคอมพิวเตอร์
ดำเนินการ	11.กำหนดนโยบายรหัสผ่านองค์กรและตั้งรหัสผ่าน (เช่น จำนวนอักษร,ความยาก)
ดำเนินการ	12.ป้องกันการคาดเดารหัสผ่าน (เช่น เพิ่มช่วงระหว่างความพยายามเข้าสู่ระบบ
	หรือ ปฏิเสธการเข้าสู่ระบบหลังจากเกินจำนวนครั้งที่ความพยายามที่ล้มเหลว)
ดำเนินการ	13.ติดตั้งและกำหนดกลไกการรักษาความปลอดภัยอื่นๆเพื่อตรวจสอบการเข้าสู่ระบบ
	การกำหนดค่าการควบคุมการใช้ทรัพยากรให้เหมาะสม
ดำเนินการ	14.ปฏิเสธการเข้าถึงและการอ่านไฟล์และไดเรกทอรีที่ไม่จำเป็น
ดำเนินการ	15.ปฏิเสธการเข้าถึงและการเขียนไฟล์และไดเรกทอรีที่ไม่จำเป็น
ดำเนินการ	16.บริหารจัดการสิทธิ์การทำงานของเครื่องมือสำหรับระบบการดูแลระบบ

ตารางที่ 4.24 (ต่อ)

ผลการประเมิน	กิจกรรม
	การติดตั้งและตั้งค่าการควบคุมการรักษาความปลอดภัยเพิ่มเติม
ดำเนินการ	17. เลือก ติดตั้งและกำหนดค่าซอฟต์แวร์เพิ่มเติมที่จำเป็นที่ไม่รวมอยู่ในระบบ
	ปฏิบัติการ เช่น ซอฟต์แวร์ป้องกันไวรัส, ป้องกันสปายแวร์ซอฟแวร์,ซอฟแวร์ตรวจจับ
	rootkit ,ซอฟแวร์ตรวจจับการบุกรุกโฮสต์ ,ซอฟแวร์ป้องกันโฮสต์ ซอฟต์แวร์
	ไฟร์วอลล์และซอฟต์แวร์การจัดการแก้ไขซอฟแวร์เพิ่มเติม
	ทดสอบความปลอดภัยของระบบปฏิบัติการ
ดำเนินการ	18.ระบุตัวผู้ใช้งานที่เข้าใช้ระบบที่เชื่อมต่อ
ดำเนินการ	19.ทดสอบระบบปฏิบัติการหลังจากที่เริ่มต้นการติดตั้งเพื่อตรวจสอบช่องโหว่
ดำเนินการ	20.ทดสอบระบบปฏิบัติการเป็นระยะ ๆ (เช่นรายไตรมาส) เพื่อตรวจสอบช่องโหว่ใหม่

2) ข้อกำหนดความปลอดภัยของเว็บเซิร์ฟเวอร์ (Checklist for Securing the Web Server) จำนวน 32 ข้อกำหนด จากการประเมิน Apache Web Server version 2.2.17 โดยใช้เครื่องมือ PuTTY version 0.63 และ Google Chrome Version 45.0.2454.85 m มีการดำเนินการ 30 ข้อกำหนด ไม่ได้ดำเนินการ 2 ข้อกำหนด คือ ข้อกำหนดที่ 18 เนื่องจากไม่อนุญาตให้ผู้ใช้งานมีการ uploads files ไปยังเว็บเซิร์ฟเวอร์ และข้อกำหนดที่ 31 เนื่องจากไม่มีความจำเป็นต้องใช้ robots.txt file รายละเอียดตามตารางที่ 4.25

ตารางที่ 4.25 ผลการประเมินมาตรฐานความปลอดภัยของเว็บเซิร์ฟเวอร์

ผลการประเมิน	กิจกรรม
	ความปลอดภัยในการติดตั้งเว็บเซิร์ฟเวอร์
ดำเนินการ	1.ติดตั้งซอฟต์แวร์เว็บเซิร์ฟเวอร์ในพื้นที่เฉพาะหรือเซิร์ฟเวอร์เสมือนที่มีระบบปฏิบัติการ
ดำเนินการ	2.ติดตั้งซอฟต์แวร์ปรับปรุงใดๆ หรือการอัพเกรดเพื่อแก้ไขช่องโหว่ที่ทราบ
ดำเนินการ	3.สร้างพื้นที่ดิสก์ทางกายภาพเฉพาะหรือแยกพาร์ทิชัน (แยกต่างหากจากระบบปฏิบัติการและ เว็บเซิร์ฟเวอร์ใช้งาน) สำหรับจัดเก็บเนื้อหาของเว็บ
ดำเนินการ	4.ยกเลิกหรือปิดบริการทั้งหมดที่ติดตั้งโดยการประยุกต์ใช้เว็บเซิร์ฟเวอร์ ที่ไม่จำเป็นต้องใช้งาน (เช่น gopher, FTP, การ Remote ควบคุมเซิร์ฟเวอร์ระยะไกล)
ดำเนินการ	5.ยกเลิกหรือปิดการใช้งานของผู้ใช้งานที่ไม่จำเป็น ที่ถูกสร้างขึ้นจากการติดตั้งเซิร์ฟเวอร์
ดำเนินการ	6.ลบเอกสารคู่มือการใช้งานอิเลคทรอนิคส์ทั้งหมดออกจากเซิร์ฟเวอร์
ดำเนินการ	7.ลบตัวอย่างไฟล์หรือไฟล์ทดสอบทั้งหมดออกจากเซิร์ฟเวอร์รวมทั้งสคริปต์และรหัส ปฏิบัติการ
ดำเนินการ	8.มีการรักษาความปลอดภัยที่เหมาะสม หรือติดตั้ง hardening ในเซิร์ฟเวอร์
ดำเนินการ	9.เซิร์ฟเวอร์ รุ่น ประเภทของระบบปฏิบัติการ
	การกำหนดค่าเพื่อควบคุมการเข้าถึงระบบปฏิบัติการและเว็บเซิร์ฟเวอร์
ดำเนินการ	10.กำหนดค่าการจำกัดการใช้งาน สิทธิ์ เพื่อการทำงานเว็บเซิร์ฟเวอร์สำหรับผู้ใช้
ดำเนินการ	11.กำหนดค่าเว็บเซิร์ฟเวอร์เพื่อให้แฟ้มเนื้อหาของเว็บสามารถอ่านได้ แต่เขียนไม่ได้โดยบริการที่เรียกใช้

ตารางที่ 4.25 (ต่อ)

ผลการประเมิน	กิจกรรม
ดำเนินการ	12.กำหนดค่าเว็บเซิร์ฟเวอร์เพื่อให้บริการที่เรียกใช้ไม่สามารถเขียนไฟล์ในไดเรกทอรีที่เก็บเนื้อหาของเว็บสาธารณะที่ถูกเก็บไว้
ดำเนินการ	13.กำหนดค่าเว็บเซิร์ฟเวอร์เพื่อให้การบริการแบบ administration เท่านั้นสามารถเขียนไฟล์เนื้อหาของเว็บเซิร์ฟเวอร์ได้
ดำเนินการ	14.กำหนดค่าเพื่อให้เว็บเซิร์ฟเวอร์สามารถเขียนไฟล์ข้อมูลการเข้าสู่ระบบ แต่อ่านไม่ได้
ดำเนินการ	15.กำหนดค่าระบบปฏิบัติการเพื่อให้แฟ้มชั่วคราวที่สร้างขึ้นโดยโปรแกรมเว็บเซิร์ฟเวอร์ถูกจำกัดอยู่ในไดเรกทอรีย่อยที่ระบุไว้เท่านั้น และมีการป้องกันอย่างเหมาะสม
ดำเนินการ	16.กำหนดค่าระบบปฏิบัติการเพื่อให้เข้าถึงไฟล์ชั่วคราวที่สร้างขึ้น ให้สามารถเข้าถึงได้โดยโปรแกรมเว็บเซิร์ฟเวอร์ที่เป็นตัวสร้างไฟล์ชั่วคราวเท่านั้น
ดำเนินการ	17.ติดตั้งเนื้อหาของเว็บบนฮาร์ดไดรฟ์อื่นหรือพาร์ทิชันอื่น ที่ไม่ใช่ระบบปฏิบัติการและแอพลิเคชัน
ไม่จำเป็น	18.ถ้ามีการอนุญาตให้เว็บเซิร์ฟเวอร์สามารถ upload ข้อมูลได้ ต้องกำหนดค่าเพื่อจำกัดขนาดของไฟล์ และจำนวนของพื้นที่ฮาร์ดไดรฟ์ และควรจะอยู่ในพาร์ทิชันที่แยกต่างหาก
ดำเนินการ	19.ไฟล์ข้อมูลการเข้าใช้งาน ต้องจะถูกเก็บไว้ในขนาดเหมาะสม และไฟล์ควรจะเก็บอยู่บนพาร์ติชันที่แยกต่างหาก
ดำเนินการ	20.กำหนดค่าจำนวนสูงสุดของโปรเซสเว็บเซิร์ฟเวอร์ และ จำกัดจำนวนการเชื่อมต่อเครือข่ายที่เชื่อมต่อกับเว็บเซิร์ฟเวอร์
ดำเนินการ	21.ตรวจสอบผู้ใช้งานชั่วคราว ให้ดำเนินการตามรายการตรวจสอบนี้
ดำเนินการ	22.ตรวจสอบผู้ใช้และผู้ดูแลระบบให้สามารถที่จะเปลี่ยนรหัสผ่านได้
ดำเนินการ	23.ปิดการใช้งานของผู้ใช้หลังจากไม่มีการใช้งานในระยะเวลาที่กำหนด

ตารางที่ 4.25 (ต่อ)

ผลการประเมิน	กิจกรรม
ดำเนินการ	24. ผู้ใช้แต่ละคนและผู้ดูแลระบบต้องมีชื่อบัญชีไม่ซ้ำกัน
	การกำหนดค่าไดเรกทอรีเนื้อหาเว็บที่มีความปลอดภัย
ดำเนินการ	25. ติดตั้งฮาร์ดไดรฟ์หรือพาร์ทิชันเดี่ยว และสร้างไดเรกทอรีที่เกี่ยวข้องเฉพาะสำหรับ เว็บเซิร์ฟเวอร์ไฟล์เนื้อหารวมทั้งกราฟิก แต่ไม่รวมสคริปต์และโปรแกรมอื่น ๆ
ดำเนินการ	26.กำหนดไดเรกทอรีเดียวเฉพาะสำหรับสคริปต์ภายนอกทั้งหมดหรือโปรแกรมที่เป็นส่วนหนึ่งของเนื้อหาเว็บเซิร์ฟเวอร์ (เช่น CGI, ASP)
ดำเนินการ	27.ปิดการทำงานของสคริปที่ไม่ได้เรียกใช้ภายใต้การควบคุมของผู้ดูแลระบบ
ดำเนินการ	28.ปิดการใช้การเชื่อมโยงไปยังคำสั่งอื่น (เช่นทางลัดสำหรับ Windows)
ดำเนินการ	29.ออกแบบให้จำกัดการเข้าถึงเนื้อหาของเว็บที่สมบูรณ์ ระบุโฟลเดอร์และไฟล์เอกสารภายในเว็บเซิร์ฟเวอร์ และสามารถเข้าถึง (และโดยใคร)
ดำเนินการ	30.ตรวจสอบนโยบายรหัสผ่านขององค์กรและการตั้งค่ารหัสผ่านของบัญชีให้เหมาะสม(เช่นความยาว ความซับซ้อน)
ไม่จำเป็น	31.ใช้ไฟล์ robots.txt ตามความเหมาะสม
ดำเนินการ	32.ติดตั้งค่าป้องกันสแปมตามความเหมาะสม (เช่น CAPTCHAs, nofollow หรือการกรองคำสำคัญ)

3) ข้อกำหนดความปลอดภัยของเนื้อหา (Checklist for Securing Web Content) จำนวน 64 ข้อกำหนด จากการประเมินระบบ Healthws System ด้วยเครื่องมือ Google Chrome Advanced Rest Client version: 3.1.9 และ Google Chrome Version 45.0.2454.85 m มีการดำเนินการ 61 ข้อกำหนด ไม่ได้ดำเนินการ 3 ข้อกำหนด คือ ข้อกำหนดที่ 9 ,10 เนื่องจากไม่ใช่ข้อมูลด้านการสืบสวนและการเงิน ข้อกำหนดที่ 32 เนื่องจากไม่มีความจำเป็นต้องใช้ลายมือชื่ออิเล็กทรอนิกส์ รายละเอียดตามตารางที่ 4.25

ตารางที่ 4.26 ผลการประเมินมาตรฐานความปลอดภัยของเนื้อหา

ผลการประเมิน	กิจกรรม
	ตรวจสอบให้แน่ใจว่าไม่มีประเภทของข้อมูลต่อไปนี้ที่มีอยู่หรือเข้าถึงได้ผ่านทางเว็บเซิร์ฟเวอร์สาธารณะ
ดำเนินการ	1.ข้อมูลการโฆษณา
ดำเนินการ	2.กฎระเบียบภายในสำกรับบุคลากรและวิธีการทำงาน
ดำเนินการ	3.ข้อมูลที่กระทบความรู้สึกหรือข้อมูลที่มีลิขสิทธิ์
ดำเนินการ	4.ข้อมูลส่วนบุคคลภายในองค์กร
ดำเนินการ	5.หมายเลขโทรศัพท์ ที่อยู่อีเมล หรือ ข้อมูลทั่วไปของพนักงานเว้นแต่จำเป็นที่จะต้องตอบสนองความต้องการขององค์กร
ดำเนินการ	6.กำหนดเวลากิจกรรมของผู้บริหารองค์กรหรือสถานทำงาน (ไม่ว่าจะในหรือนอกสถานที่)
ดำเนินการ	7.ข้อมูลส่วนประกอบสำหรับการเตรียมการหรือการใช้งานของวัสดุอันตรายหรือสารพิษ
ดำเนินการ	8.ข้อมูลที่มีผลกระทบเกี่ยวข้องกับศูนย์บัญชาการการรักษาความปลอดภัย
ไม่จำเป็น	9.ข้อมูลการบันทึกสืบสวน
ไม่จำเป็น	10.ข้อมูลบันทึกทางการเงิน (นอกเหนือจากที่เปิดเผยต่อสาธารณชนอยู่แล้ว)
ดำเนินการ	11.ข้อมูลเวชระเบียน
ดำเนินการ	12.ข้อมูลทางกายภาพและขั้นตอนการรักษาความปลอดภัย
ดำเนินการ	13.ข้อมูลเกี่ยวกับเครือข่ายขององค์กรและโครงสร้างระบบสารสนเทศพื้นฐาน
ดำเนินการ	14.ข้อมูลที่ระบุหรือแสดงถึงช่องโหว่ความปลอดภัยทางกายภาพ
ดำเนินการ	15.ข้อมูลแผนงาน, แผนที่, แผนภาพ, ภาพถ่ายทางอากาศและวัฒนธรรมองค์กรโครงสร้างของแผนงาน
ดำเนินการ	16.ข้อมูลไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของ
ดำเนินการ	17.ข้อมูลความลับหรือนโยบายการรักษาความปลอดภัยที่บ่งบอกถึงประเภทของมาตรการรักษาความปลอดภัย ที่อาจจะเป็นประโยชน์ในการโจมตี

ตารางที่ 4.26 (ต่อ)

ผลการประเมิน	กิจกรรม
	เอกสารที่เป็นทางการและนโยบายขั้นตอนในการเผยแพร่เนื้อหาของเว็บสาธารณะดังต่อไปนี้
ดำเนินการ	19.มีการระบุกลุ่มเป้าหมาย
ดำเนินการ	20.ระบุเชิงลบที่เป็นไปได้จากการเผยแพร่ข้อมูล
ดำเนินการ	21.ระบุที่ผู้รับผิดชอบในการสร้าง, การเผยแพร่และการบำรุงรักษาข้อมูลโดยเฉพาะ
ดำเนินการ	22.ให้คำแนะนำเกี่ยวกับรูปแบบและรูปแบบที่เหมาะสมสำหรับการเผยแพร่ข้อมูลเว็บ
ดำเนินการ	23.มีวิธีการสำหรับการตรวจสอบความเหมาะสมของข้อมูลที่ความรวดเร็วและการจัดจำหน่าย /การควบคุม (รวมถึงความรวดเร็วในการรวบรวมข้อมูล)
ดำเนินการ	24.มีวิธีการการเข้าถึงที่เหมาะสมและมีการควบคุมความปลอดภัย
ดำเนินการ	25.ป้องกันข้อมูลไม่ให้เห็นภาษาโปรแกรมที่มาของเนื้อหาเว็บ การรักษาความเป็นส่วนตัวของผู้ใช้เว็บ
ดำเนินการ	26.เผยแพร่นโยบายการรักษาความเป็นส่วนตัว
ดำเนินการ	27. ป้องกันเข้าถึงข้อมูลของบุคคลโดยไม่ต้องระบุผู้ใช้งานและต้องได้รับอนุญาตจากผู้ใช้ ในการเก็บรวบรวมข้อมูลที่จำเป็น
ดำเนินการ	28. ไม่อนุญาตให้ใช้คุกกี้ถาวร
ดำเนินการ	29.ใช้เซสชันคุกกี้เท่านั้นหากมีการระบุไว้อย่างชัดเจนในนโยบายความเป็นส่วนตัว ลดการโจมตีทางอ้อมกับเนื้อหาของเว็บ
ดำเนินการ	30.มั่นใจว่าผู้ใช้ของเว็บไซต์ที่มีความตระหนักถึงอันตรายของการการโจมตีแบบฟิชชิ่งฟาร์มมิ่งและและรู้วิธีการหลีกเลี่ยงวิธีดังกล่าว
ดำเนินการ	31.ตรวจสอบการสื่อสารอย่างเป็นทางการโดยการปรับแต่งอีเมล์และการให้บริการที่ไม่ซ้ำกันระบุ (แต่ไม่เป็นความลับ) ให้เป็นข้อมูลภายในองค์กรเท่านั้นและผู้ใช้ต้องรู้
ไม่จำเป็น	32.ใช้ลายเซ็นดิจิตอลใน e-mail ตามความเหมาะสม
ดำเนินการ	33.ดำเนินการตรวจสอบเนื้อหาภายในโปรแกรมประยุกต์บนเว็บเพื่อป้องกันโจมตีแบบฟิชชิ่งที่มีความซับซ้อน (เช่น cross-site scripting based)ไม่ให้เพิ่มขึ้น
ดำเนินการ	34.ปรับปรุงเนื้อหาของเว็บที่จะช่วยให้ผู้ใช้ทราบถึงระบุเว็บไซต์หลอกลวงต่างๆ

ตารางที่ 4.26 (ต่อ)

ผลการประเมิน	กิจกรรม
ดำเนินการ	35.ใช้ Tocken ในการการเชื่อมต่อระบบ ถ้ามี
ดำเนินการ	36.แนะนำการใช้งานเว็บเบราเซอร์หรือแถบเครื่องมือในเบราว์เซอร์ที่มีการฟิชชิ่ง / การป้องกันฟาร์มมิ่ง
ดำเนินการ	37.ใช้ซอฟแวร์ DNS รุ่นปัจจุบันของ ร่วมกับซอฟต์แวร์ปรับปรุงล่าสุดเพื่อการรักษาความปลอดภัย
ดำเนินการ	38.ติดตั้งกลไกการป้องกันในเซิร์ฟเวอร์ DNS
ดำเนินการ	39.ตรวจสอบโดเมนขององค์กรและโดเมนที่คล้ายกัน
ดำเนินการ	40.ลดความซับซ้อนชื่อโดเมนขององค์กร
ดำเนินการ	41.ใช้การเชื่อมต่อที่ปลอดภัยสำหรับการเข้าสู่ระบบ
ดำเนินการ	42.หากจำเป็นต้องมีการจ้างผู้พัฒนา เพื่อให้ที่จะให้สามารถป้องกันฟิชชิ่ง / และการ
	ป้องกันการ pharming อย่างปลอดภัย
	การพิจารณาความปลอดภัยของเนื้อหาที่ใช้งานในไคลเอ็นต์
ดำเนินการ	43.ชั่งน้ำหนักความเสี่ยงและประโยชน์ของเนื้อหาที่ใช้งานของไคลเอ็นต์
ดำเนินการ	44.ไม่ดำเนินการใดๆโดยไม่ได้รับอนุญาตจากผู้ใช้
ดำเนินการ	45.ใช้ JavaScript,รูปแบบไฟล์ PDF และ Flash ในการเผยแพร่เนื้อหาเว็บ
ดำเนินการ	46.ให้ใช้วิธีการเลือกรูปแบบ (เช่น HTML ให้พร้อมกับรูปแบบไฟล์ PDF)
	การรักษาความปลอดภัยเนื้อหาที่ใช้งานรักษาฝั่งเซิร์ฟเวอร์
ดำเนินการ	47.ควรจะใช้ภาษาโปรแกรมที่เรียบง่ายและง่ายต่อการเข้าใจ
ดำเนินการ	48.จำกัด หรือไม่อนุญาตการอ่านหรือเขียนไฟล์ที่ควรจะได้รับอนุญาต
ดำเนินการ	49.จำกัดการเชื่อมต่อกับโปรแกรมอื่น ๆ (เช่น sendmail) เฉพาะได้รับอนุญาต
ดำเนินการ	50.ไม่ควรมีความต้องการที่ใช้สิทธิ์ SUID บน Unix หรือ Linux
ดำเนินการ	51.ควรใช้ชื่อ path ที่ชัดเจน (ไม่ใช้ตัวแปร path)
ดำเนินการ	52.ไม่มีไดเรกทอรีที่มีสิทธิ์ทั้งเขียนและ Execute
ดำเนินการ	53.แฟ้ม Execute ทั้งหมดจัดเก็บไว้ในโฟลเดอร์เฉพาะ
ดำเนินการ	54. ปิดใช้งาน SSIs และฟังก์ชั่น Execute

ตารางที่ 4.26 (ต่อ)

ผลการประเมิน	กิจกรรม
ดำเนินการ	55.ตรวจสอบผู้ใช้งานทั้งหมด
ดำเนินการ	56.ควรจะสแกนหรือตรวจสอบภาษาโปรแกรมที่สร้างเนื้อหาเว็บ
ดำเนินการ	57.เนื้อหาแบบ Dynamic ไม่ควรสร้าง Meta characters อันตราย
ดำเนินการ	58. Character Set ควรจะกำหนดอย่างชัดเจนในแต่ละหน้า
ดำเนินการ	59.ข้อมูลของผู้ใช้ควรจะสแกนเพื่อให้แน่ใจว่ามีการป้อนข้อมูลที่กำหนดเท่านั้น (เช่น a-z, A-Z, 0-9) ไม่ควรใช้อักษรพิเศษหรือ Tag
ดำเนินการ	60.ควรจะตรวจสอบคุกกี้ที่ใช้ตัวอักษรพิเศษ
ดำเนินการ	61.ใช้กลไกการเข้ารหัสในการเข้ารหัสรหัสผ่านที่ป้อนผ่านสคริปต์ ผ่านสคริปต์ฟอร์ม
ดำเนินการ	62.สำหรับการใช้งานเว็บที่ถูกจำกัดการเข้าถึง โดยชื่อผู้ใช้และรหัสผ่าน ไม่ควรมีหน้าเว็บที่สามารถเข้าถึงได้โดยไม่ต้องป้อนชื่อผู้ใช้และรหัสผ่าน
ดำเนินการ	63.ลบสคริปต์ตัวอย่างทั้งหมดออกไป
ดำเนินการ	64.ไม่มีสคริปต์ของบุคคลที่สามหรือคำสั่งประมวลผลที่ใช้งานโดยไม่ผ่านการตรวจสอบ

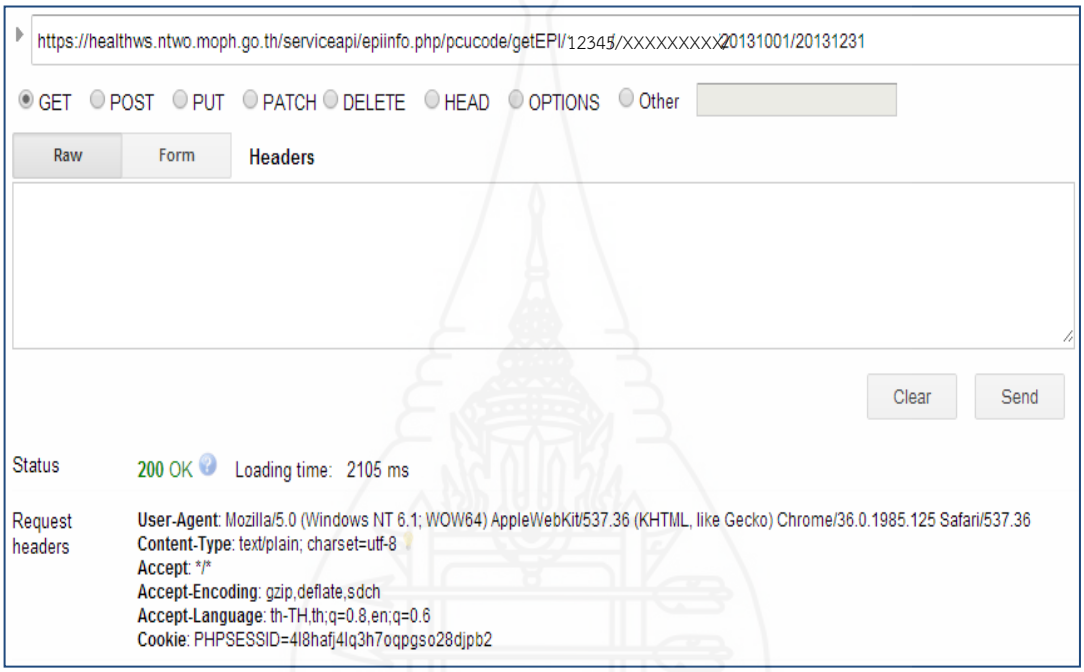
3.3 ผลการทดสอบความพร้อมใช้งาน (Availability) โดยบุคลากรสาธารณสุข (ภาคผนวก ฉ) จำนวน 10 คน คนละ 3 ครั้ง เพื่อทดสอบว่าระบบ Healthws-Client สามารถให้เรียกใช้บริการเว็บเซอร์วิสได้อย่างราบรื่น ไม่ติดขัด โดยผู้ใช้ระบบเฉพาะที่ได้รับอนุญาตเท่านั้น

3.3.1 ทดสอบระบบ Healthws-Client ทดสอบการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล (PIS) ด้วยผู้ใช้งานตามสถานะสถานบริการที่แตกต่างกัน ผลการทดสอบสามารถเข้าถึงข้อมูลของผู้รับบริการตามสถานะของการแลกเปลี่ยนข้อมูลและการเรียกใช้ข้อมูลได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

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

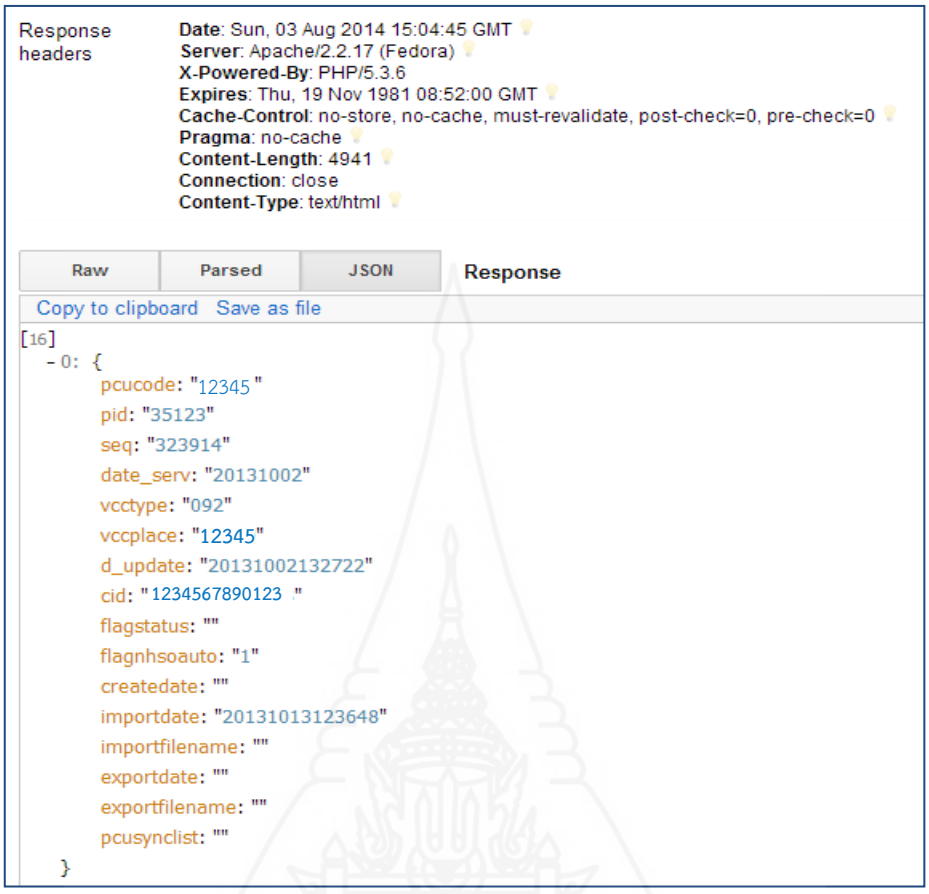
สามารถเข้าถึงข้อมูลของผู้รับบริการตามสถานะของการแลกเปลี่ยนข้อมูลและการเรียกใช้ข้อมูลได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

3.3.3 ส่วนการร้องขอข้อมูล (https request) ข้อมูลที่ถูกส่งการร้องขอไปยังเว็บเซอร์วิส จะถูกส่งไปค้นหาข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรคในฐานข้อมูลระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยใช้ http โปรโตคอล ดังภาพที่ 4.23



ภาพที่ 4.23 ตัวอย่างการร้องขอข้อมูล (http request) ไปยังเว็บเซอร์วิส

ข้อมูลการรับบริการสร้างเสริมภูมิคุ้มกันโรค จะถูกส่งกลับมาในรูปแบบ JSON เพื่อส่งไปแสดงที่หน้าจอเว็บแอปพลิเคชัน หรือ เว็บเซอร์วิสไคลเอนต์ เพื่อนำเข้าไปยังฐานข้อมูล JHCISDB ของโรงพยาบาลส่งเสริมสุขภาพตำบล ดังภาพที่ 4.24



ภาพที่ 4.24 ตัวอย่างการตอบกลับข้อมูล (http response)

จากผลการทดสอบมาตรฐานความปลอดภัยหัวข้อที่ 3.1 ด้านการรักษาความลับ (Confidentiality) หัวข้อที่ 3.2 ด้านการคงสภาพของข้อมูล (Integrity) และหัวข้อที่ 3.3 ผลการทดสอบความพร้อมใช้งาน (Availability) โดยผู้พัฒนาระบบ พบว่าสารสนเทศที่ได้จากระบบ Healthws System ที่ผู้วิจัยพัฒนาขึ้นมีความปลอดภัยตามมาตรฐานความปลอดภัยตามแนวคิด C.I.A Triangle ข้อมูลสารสนเทศครบทั้ง 3 ด้าน มีความปลอดภัยตามมาตรฐานความปลอดภัยที่ได้ออกแบบไว้

บทที่ 5
สรุปการวิจัย และข้อเสนอแนะ

การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาสนี้ ตั้งแต่การศึกษาโครงสร้างระบบข้อมูลสารสนเทศสุขภาพที่จัดเก็บอยู่ในปัจจุบัน การวิเคราะห์ระบบและออกแบบระบบการทำงาน การพัฒนาระบบ Healthws System ด้วย Restful web service และออกแบบมาตรฐานความปลอดภัยด้วยวิธีการ Securing RESTful Web Services ร่วมกับ มาตรฐาน SSL/TLS มีการประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ตามข้อกำหนดของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา และทดสอบระบบ สามารถสรุปเป็นข้อได้ดังนี้

1. สรุปการวิจัย
2. ปัญหาและแนวทางแก้ไข
3. ข้อเสนอแนะ

1. สรุปการวิจัย

1.1 ผู้วิจัยได้ทำการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส เพื่อให้ข้อมูลสารสนเทศมีมาตรฐานความปลอดภัยอ้างอิงแบบจำลองโอเอสไอ (OSI Model) และ องค์ประกอบความปลอดภัยของสารสนเทศ (C.I.A Triangle) ที่สมบูรณ์ คือ ด้านการรักษาความลับ (Confidentiality) ในลำดับชั้นขนส่ง (Transport Layer) ใช้มาตรฐาน SSL 3.0 / TLS 1.0 ลำดับชั้นส่วนงาน (Session Layer) มีการจัดการ Session ของผู้ใช้งาน ในลำดับชั้นการประยุกต์ (Application Layer) ใช้วิธีการ Authentication ตรวจสอบค่าเลขบัตรประจำตัวประชาชนจากฐานข้อมูลระบบบริหารงานบุคคลของสำนักงานสาธารณสุขจังหวัดนราธิวาสและตรวจสอบค่า Client Key ของผู้ใช้งาน ด้านการคงสภาพของข้อมูล (Integrity) มีการกำหนดสถานะของหน่วยบริการสาธารณสุขและสิทธิ (Authorization) ในการแลกเปลี่ยนข้อมูล การเรียกใช้ข้อมูล ร่วมกับการใช้ภาษา PHP Slim Framework และด้านความพร้อมในการใช้งาน (Availability) มีการพิสูจน์ตัวตน (Identification) การให้สิทธิ์ (Authorization)

การเรียกใช้ข้อมูลมีขั้นตอนเริ่มขึ้นเมื่อผู้รับบริการที่อยู่ในพื้นที่รับผิดชอบไปรับบริการสร้างเสริมภูมิคุ้มกันโรคจากหน่วยบริการสาธารณสุขอื่น และมีการบันทึกข้อมูลเข้าไปในระบบและส่งข้อมูลอัตโนมัติไปยังศูนย์ข้อมูลจังหวัด (Data Center) โรงพยาบาลส่งเสริมสุขภาพตำบลสามารถเรียกใช้และแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสไปยังศูนย์ข้อมูลจังหวัด (Data Center) เพื่อนำข้อมูลกลับเข้ามาเพิ่มในระบบฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบลได้ทันทีโดยไม่ต้องมีการบันทึกข้อมูลใหม่อีกครั้งหนึ่ง ซึ่งผลจากการทำงานสามารถร้องขอข้อมูลและส่งกลับข้อมูลได้ตามเงื่อนไขที่ร้องขอได้อย่างถูกต้อง และข้อมูลมีความปลอดภัยตามมาตรฐานความปลอดภัยที่ออกแบบไว้

1.2 ผลการทดสอบมาตรฐานความปลอดภัยตามองค์ประกอบความปลอดภัยของสารสนเทศ

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

1.2.1 ด้านการรักษาความลับ (Confidentiality) ทดสอบการเข้าถึงข้อมูล โดยผู้พัฒนาระบบทดสอบการเข้าสู่ระบบและเข้าถึงข้อมูล 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 และเมื่อทดสอบการเข้าถึงข้อมูลด้วย Client Key ที่ถูกต้อง ผลการทดสอบสามารถเข้าถึงข้อมูลสุขภาพส่วนบุคคล ได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

1.2.2 ด้านการคงสภาพของข้อมูล (Integrity) โดยผู้พัฒนาระบบทำการทดสอบด้วยวิธีการทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ Rest ตรวจสอบความถูกต้องในการเรียกใช้ในแต่ละฟังก์ชัน จำนวน 9 ฟังก์ชัน คือ getEPI , addEPI, updateEPI, deleteEPI, searchEPI. getSERVICEINFO, getDIAGINFO, getDRUGINFO และ getMCHINFO โดยใช้วิธีการตามแนวทางทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ REST ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น สถาบันศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพ และฝ่ายวิจัยและพัฒนาเทคโนโลยีเพื่อคำนวณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์

และคอมพิวเตอร์แห่งชาติ จังหวัดปทุมธานี ด้วยเครื่องมือ Google Chrome Advanced Rest Client ผลการทดสอบพบว่า ผ่านทุกฟังก์ชัน

1.2.3 ด้านความพร้อมในการใช้งาน (Availability) เมื่อทดสอบการเข้าไปเรียกใช้ข้อมูลโดยการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่มีในฐานข้อมูลระบบบริหารงานบุคคล สามารถเรียกใช้และแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล ผ่านระบบแลกเปลี่ยนข้อมูลสุขภาพส่วนบุคคล Healthws System ได้

ผลการทดสอบระบบ Healthws-Client ด้วยผู้ใช้งานตามสถานะสถานบริการที่แตกต่างกัน ผลการทดสอบสามารถเข้าถึงข้อมูลของผู้รับบริการตามสถานะของการเรียกใช้และการแลกเปลี่ยนข้อมูลได้ตามมาตรฐานความปลอดภัยที่ออกแบบไว้

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

1.3 การประเมินมาตรฐานความปลอดภัยตามแนวทางในการรักษาความปลอดภัยของเว็บเซิร์ฟเวอร์ โดยการประเมินตามข้อกำหนด NIST SP 800-44 Guidelines on Securing Public Web Servers ของสถาบันกำหนดมาตรฐานของเทคโนโลยีของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทำการประเมิน 3 ส่วนคือ

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

1.3.2 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

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

1.3.4 ผลการทดสอบมาตรฐานการรักษาความปลอดภัยที่นำมาใช้เป็นมาตรฐานที่เกิดขึ้นจากการใช้งาน (De facto) ในองค์กร ทั้งการบริหารจัดการโดยใช้นโยบายด้านความมั่นคงและด้านเทคนิค ทำให้ข้อมูลสุขภาพส่วนบุคคลได้รับการคุ้มครองจากผู้ที่ไม่เกี่ยวข้องกับข้อมูล ตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7, 8, 9 และ 10 และมีการรักษาความปลอดภัยของข้อมูลที่เป็นความลับตาม พระราชบัญญัติข้อมูลข่าวสาร พ.ศ.2540 มาตรา 23, 24 และ 25

1.3.5 งานวิจัยนี้ได้ดำเนินการตามแนวทางการวิจัยของ Omar Slomic เรื่อง A message-level security approach for RESTful services. เนื่องจากเทคโนโลยี RESTful Web Services ซึ่งใช้พื้นฐานของ HTTP มีความเรียบง่ายในการพัฒนาและใช้วิธีการรักษาความปลอดภัยในระดับของข้อความสำหรับ REST based services ปัจจุบันมีการนำมาใช้งานอย่างแพร่หลายกว่าสถาปัตยกรรมแบบ Service Oriented Architecture (SOA) ซึ่งสถาปัตยกรรม SOA มีลักษณะและข้อกำหนดทางสถาปัตยกรรมที่เฉพาะตัว ที่มีความซับซ้อน จะต้องรวมเอากระบวนการและกลวิธีต่างๆ เพื่อที่จะสามารถพัฒนาความปลอดภัยของ application และระบบข้อมูล

2. ปัญหาและแนวทางแก้ไข

ในการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส พบปัญหาในด้านความพร้อมในการใช้งาน (Availability) ในบางพื้นที่ เนื่องจากระบบโครงข่ายอินเตอร์เน็ตในพื้นที่ที่ห่างไกลและเป็นภูเขาสูงไม่มีการให้บริการเครือข่ายอินเตอร์เน็ตทำให้ หน่วยบริการสาธารณสุขในจังหวัดนราธิวาส โดยเฉพาะโรงพยาบาลส่งเสริมสุขภาพตำบลบางแห่งไม่สามารถส่งข้อมูลการให้บริการเข้าสู่ศูนย์ข้อมูลจังหวัด (Data Center) และไม่สามารถทำการแลกเปลี่ยนข้อมูลสารสนเทศสุขภาพผ่านเว็บเซอร์วิสระบบแลกเปลี่ยนข้อมูล Healthws System ได้ รวมทั้งปัญหาการเชื่อมต่อเครือข่ายอินเทอร์เน็ตไม่มีเสถียรภาพ ทำให้ข้อมูลการให้บริการสาธารณสุขในศูนย์ข้อมูลจังหวัด (Data Center) ของหน่วยบริการสาธารณสุขแห่งนั้นไม่เป็นปัจจุบัน ซึ่งส่งผลให้ข้อมูลที่ร้องขอได้รับการส่งกลับไม่ครบถ้วน ต้องมีการขอความร่วมมือให้ผู้ดูแลระบบของหน่วยบริการสาธารณสุขต่างๆ ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตให้สามารถใช้งานได้ตลอดเวลา รวมทั้งการสำรองข้อมูลและนำข้อมูลเข้าเพื่อการเรียกใช้และแลกเปลี่ยนข้อมูลในจุดพื้นที่ที่เครือข่ายอินเทอร์เน็ตเข้าถึง เพื่อให้การส่งข้อมูลการให้บริการเข้าสู่ศูนย์ข้อมูลจังหวัด (Data Center) สามารถเรียกใช้และแลกเปลี่ยนข้อมูลได้อย่างครบถ้วนและเป็นปัจจุบัน

3. ข้อเสนอแนะ

3.1 ในการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสารสนเทศสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส เว็บเซอร์วิสพัฒนาด้วยภาษา PHP ร่วมกับ PHP Slim Framework และเว็บเซอร์วิสไคลเอนต์ พัฒนาด้วยภาษา JAVA โดยใช้เครื่องมือ Netbean 8.0 เนื่องจากมี Library สนับสนุนครบถ้วนและสามารถทำงานได้หลาย platform และควรทำการอัพเดตช่องโหว่ในส่วน Openssl ของเซิร์ฟเวอร์ให้เป็นปัจจุบันอย่างสม่ำเสมอเพื่อความปลอดภัยในการแลกเปลี่ยนข้อมูล

3.2 ในการเตรียมข้อมูลสำหรับการวิจัยครั้งนี้ ระบบจัดการฐานข้อมูล คือ MySQL พบว่าหากมีการร้องขอข้อมูลจากการสร้างความสัมพันธ์จากตารางข้อมูลมากกว่า 2 ตาราง จะทำให้การทำงานของระบบในการค้นหาข้อมูลและปรับปรุงข้อมูลมีความล่าช้าเล็กน้อย เนื่องจากการสร้างความสัมพันธ์ระหว่างตาราง ผู้วิจัยได้ใช้วิธีการสร้างฟังก์ชันเฉพาะขึ้นมาทำงานแทนกรณีดังกล่าวโดยเก็บค่าข้อมูลที่มีความสัมพันธ์มาเก็บไว้ในตัวแปรและส่งค่าข้อมูลนั้นคืนกลับเมื่อมีการร้องขอข้อมูลนั้น ปรากฏว่าการค้นหาข้อมูลและปรับปรุงข้อมูลทำได้รวดเร็วขึ้น และได้เพิ่มตัวเลือกให้มีการเลือกตั้งค่าการร้องขอข้อมูลได้ตามช่วงเวลาที่ต้องการ โดยค่าเริ่มต้นของระบบจะกำหนดช่วงเวลาในการแลกเปลี่ยนข้อมูล เริ่มตั้งแต่วันแรกของปีงบประมาณ คือ วันที่ 1 ตุลาคม จนถึงวันที่ปัจจุบัน หรือช่วงเวลาอื่นๆ ซึ่งผู้ใช้งานสามารถกำหนดช่วงเวลาได้ตามต้องการ ดังนั้นไม่ควรกำหนดช่วงข้อมูลในการแลกเปลี่ยนข้อมูลสำหรับเว็บเซอร์วิสไคลเอนต์มากกว่า 1 ปี

3.3 เพื่อให้การให้บริการเรียกใช้และแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสมีความปลอดภัยเพิ่มขึ้น ต้องมีการรักษาความปลอดภัยของข้อมูลสารสนเทศสุขภาพแบบอื่นๆ เช่น การออกแบบ policy ของ Firewall หรือ การรักษาความปลอดภัยทางกายภาพร่วมด้วย

ภาคผนวก

ภาคผนวก ก

หนังสือขอความอนุเคราะห์ให้นักศึกษาเก็บข้อมูลเพื่อการวิจัย

กลุ่มงานพัฒนาคุณภาพและระบบบริการ
รับเลขที่ 463
วันที่ 4 มิ.ย. 2557 เวลา 10.34 น.
ที่ ศธ 0522.25/606

มหาวิทยาลัยสุโขทัยธรรมาธิราช
ตำบลบางพูด อำเภอปากเกร็ด
จังหวัดนนทบุรี 11120

28 พฤษภาคม 2557

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาเก็บข้อมูลเพื่อการวิจัย

เรียน นายแพทย์สาธารณสุขจังหวัดนราธิวาส

สิ่งที่ส่งมาด้วย โครงการวิทยานิพนธ์ จำนวน 1 แผ่น

ด้วยนายจรูญศักดิ์ เวทมาหะ นักศึกษาระดับบัณฑิตศึกษา แขนงวิชาสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช กำลังทำวิทยานิพนธ์ เรื่อง การออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเลคทรอนิคส์ผ่านเว็บเซอร์วิสของจังหวัดนราธิวาส โดยมี รองศาสตราจารย์ณัฐพร เห็นเจริญเลิศ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และอาจารย์ ดร.สุภาวดี อิงศรีสว่าง เป็นอาจารย์ที่ปรึกษาร่วม

ในการนี้ นักศึกษาจำเป็นจะต้องเก็บข้อมูลเพื่อการวิจัย การวิเคราะห์ข้อมูลการออกแบบมาตรฐานความปลอดภัยในการเรียกใช้ข้อมูลสุขภาพส่วนบุคคลอิเลคทรอนิคส์ผ่านเว็บเซอร์วิส ของจังหวัดนราธิวาส ตั้งแต่วันที่ 1 มิถุนายน - 31 ธันวาคม 2557 จึงขอความอนุเคราะห์จากท่านในการอนุญาตให้นายจรูญศักดิ์ เวทมาหะ ได้ดำเนินการเก็บข้อมูลเพื่อการวิจัย ตามวัน เวลา และรายละเอียดที่นักศึกษาเสนอมาพร้อมนี้ หวังเป็นอย่างยิ่งจะได้รับความกรุณาจากท่าน และขอขอบคุณมา ณ โอกาสนี้

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

(รองศาสตราจารย์สุณี ภู่สีม่วง)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ถึง นายแพทย์สาธารณสุขจังหวัดนราธิวาส
- เพื่อโปรดทราบ
- เพื่อโปรดพิจารณาอนุมัติให้ นายจรูญศักดิ์ เวทมาหะ ได้ดำเนินการเก็บข้อมูลวิจัยต่อไป

บัณฑิตศึกษา สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
โทร. 02-5048192

(นางสาวอารีย์ อ่องสว่าง)
นักวิชาการสาธารณสุขชำนาญการพิเศษ ปฏิบัติราชการแทน
นายแพทย์สาธารณสุขจังหวัดนราธิวาส

4 มิ.ย. 57
4 มิ.ย. 57

105

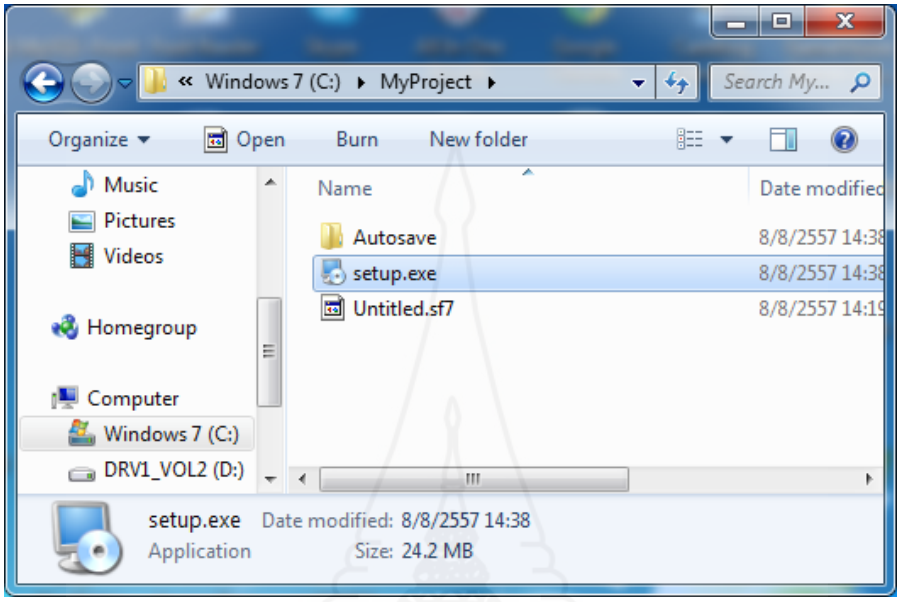
5 มิ.ย. 2557

ภาคผนวก ข

การติดตั้งระบบแลกเปลี่ยนข้อมูล Healthws-Client

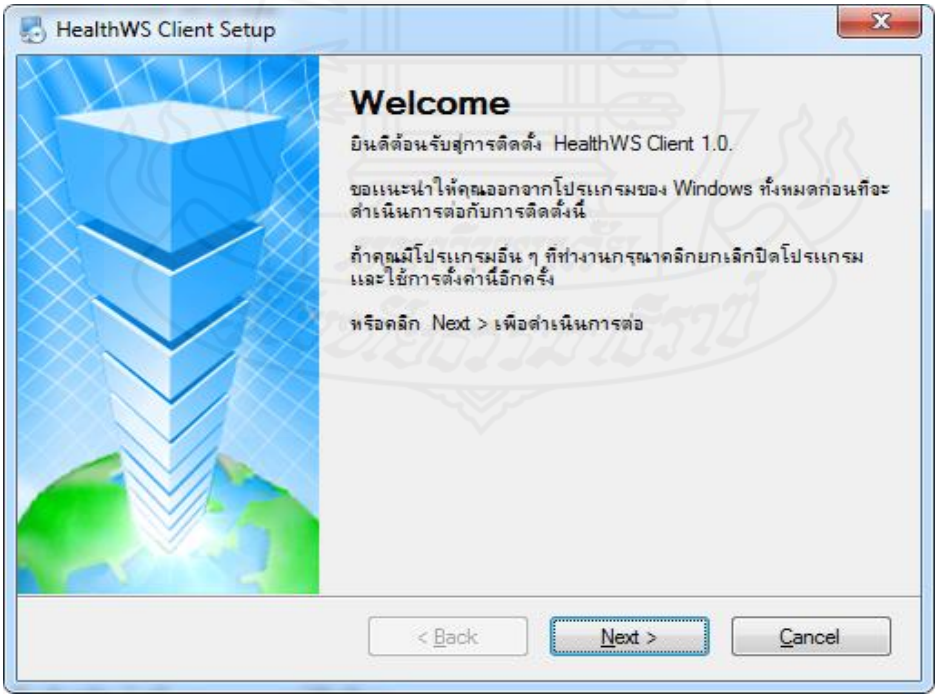
การติดตั้งระบบแลกเปลี่ยนข้อมูล Healthws-Client

1.การติดตั้งจากไฟล์ setup.exe



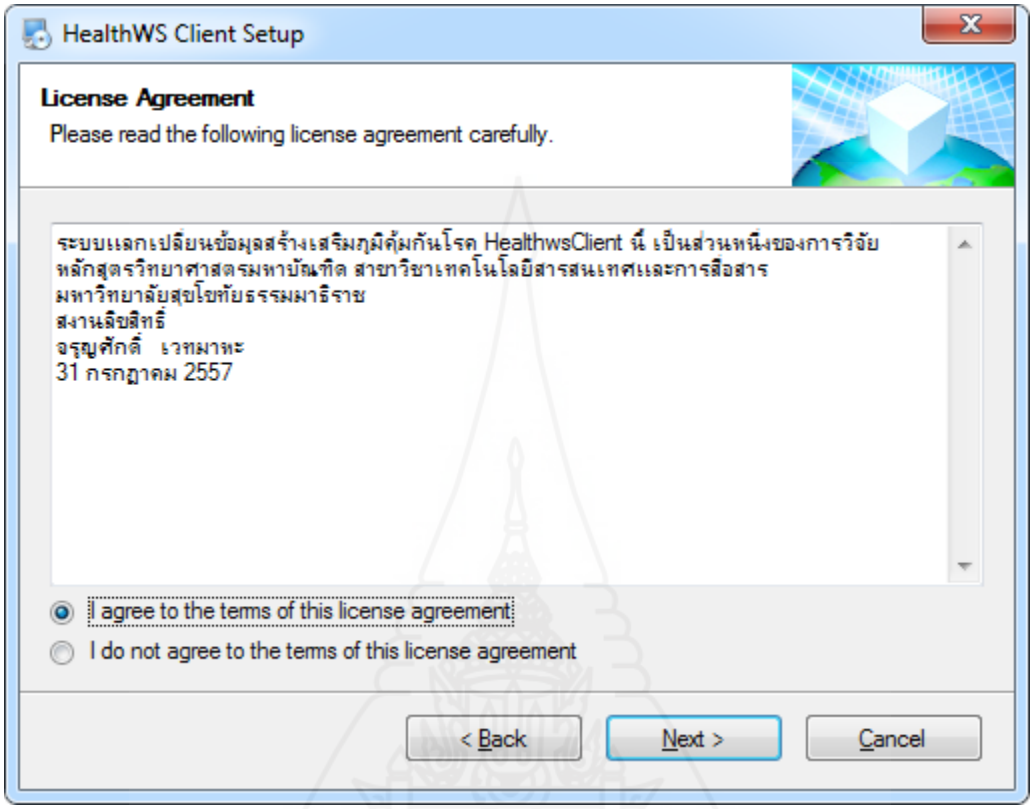
ภาพที่ ข-1 การติดตั้งจากไฟล์ setup.exe

2.ดับเบิลคลิก ไฟล์ setup.exe จะได้หน้าจอ Welcome กดปุ่ม Next >



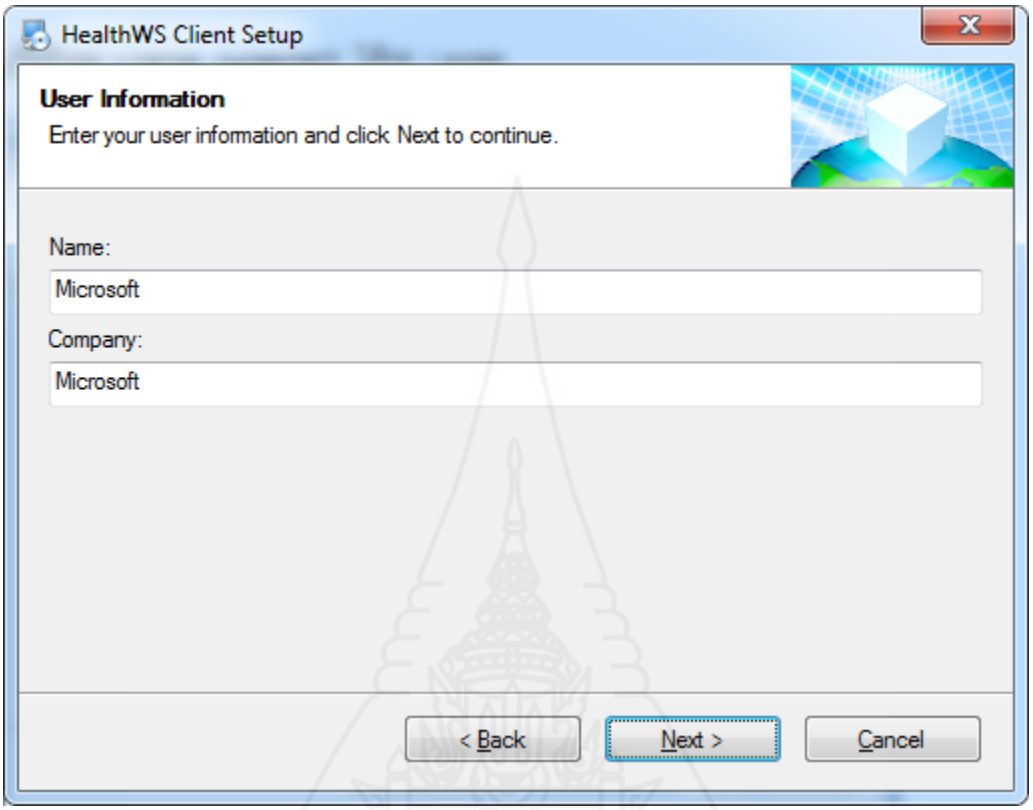
ภาพที่ ข-2 หน้าจอการติดตั้งจากไฟล์ setup.exe

3.ที่หน้าจอ License Agreement ให้กด I agree



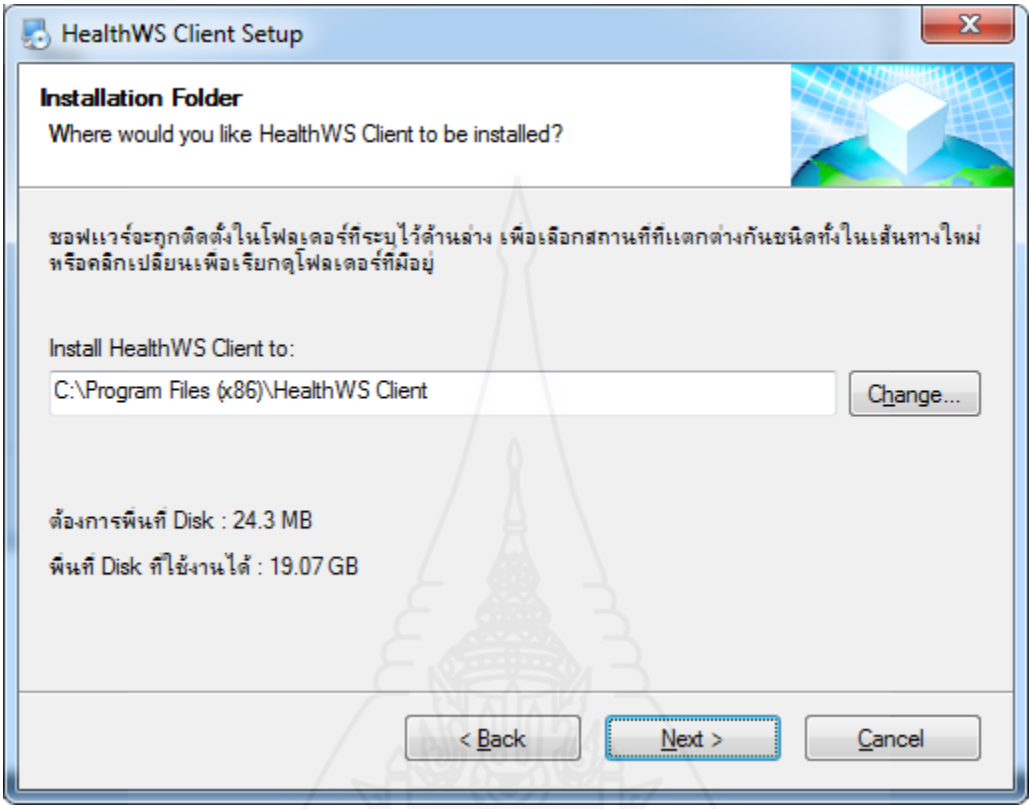
ภาพที่ ข-3 การติดตั้งหน้าจอ License Agreement

4. หน้าจอ User information ให้กดปุ่ม Next>



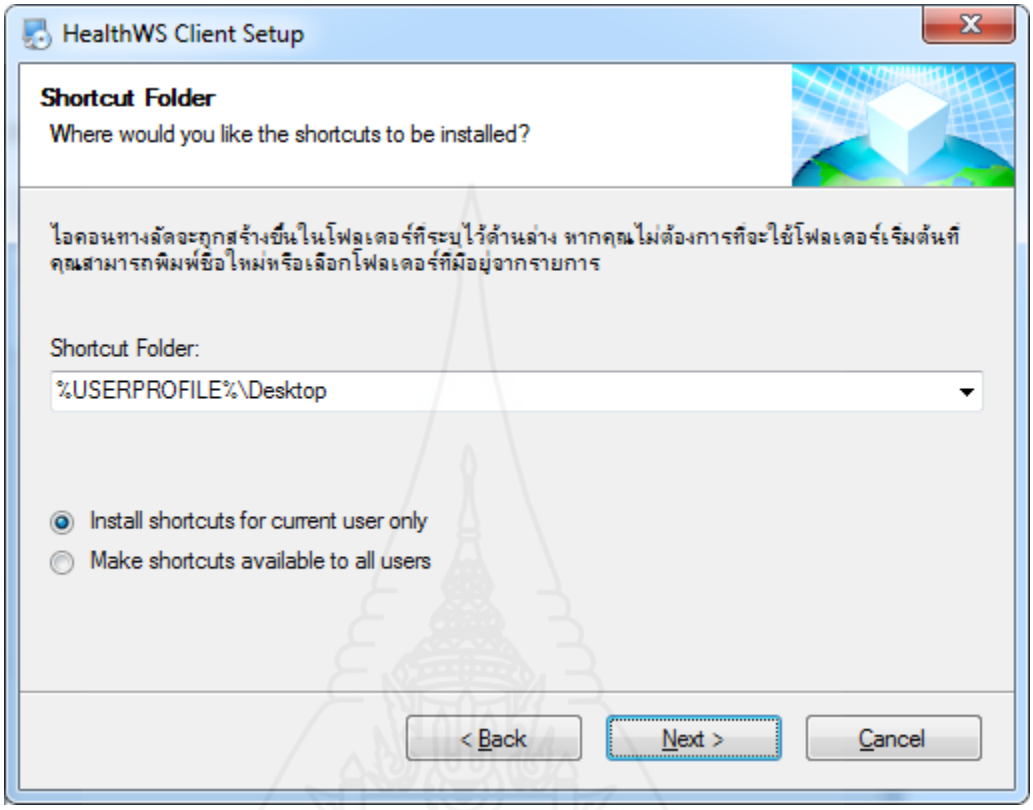
ภาพที่ ข-4 การติดตั้ง หน้าจอ User information

5.หน้าจอ Installation Folder ให้กดปุ่ม Next>



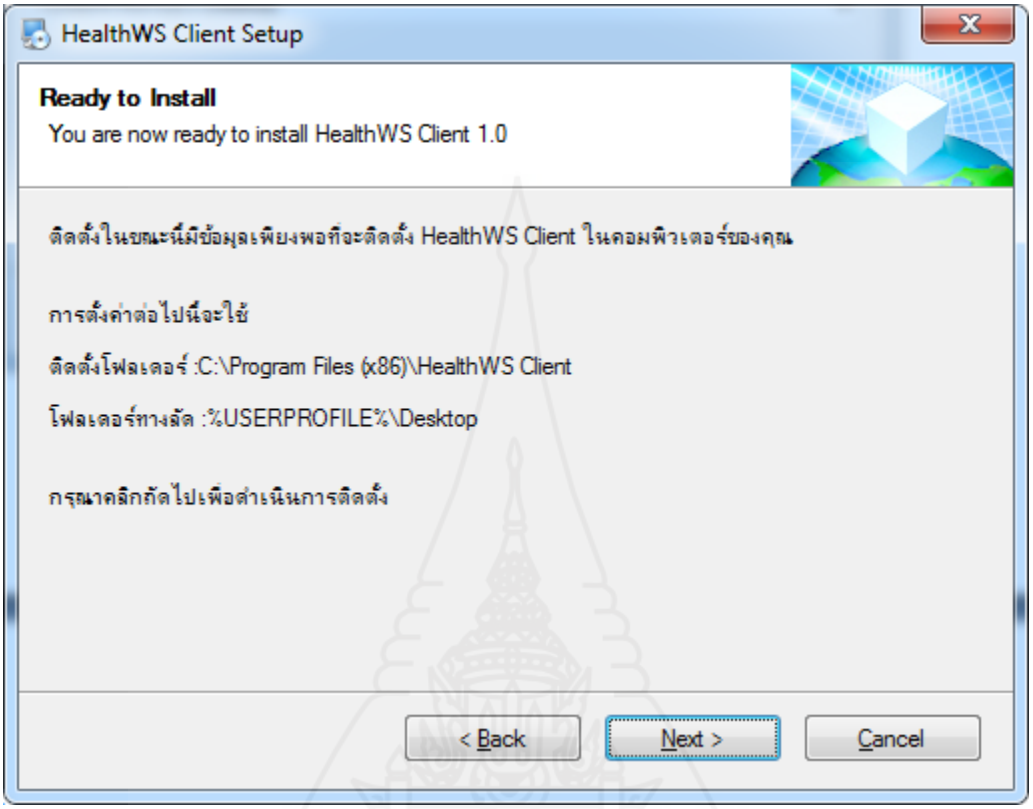
ภาพที่ ข-5 การติดตั้ง หน้าจอ Installation Folder

6.หน้าจอ Shortcut Folder ให้เลือกตามต้องการ และ กดปุ่ม Next>



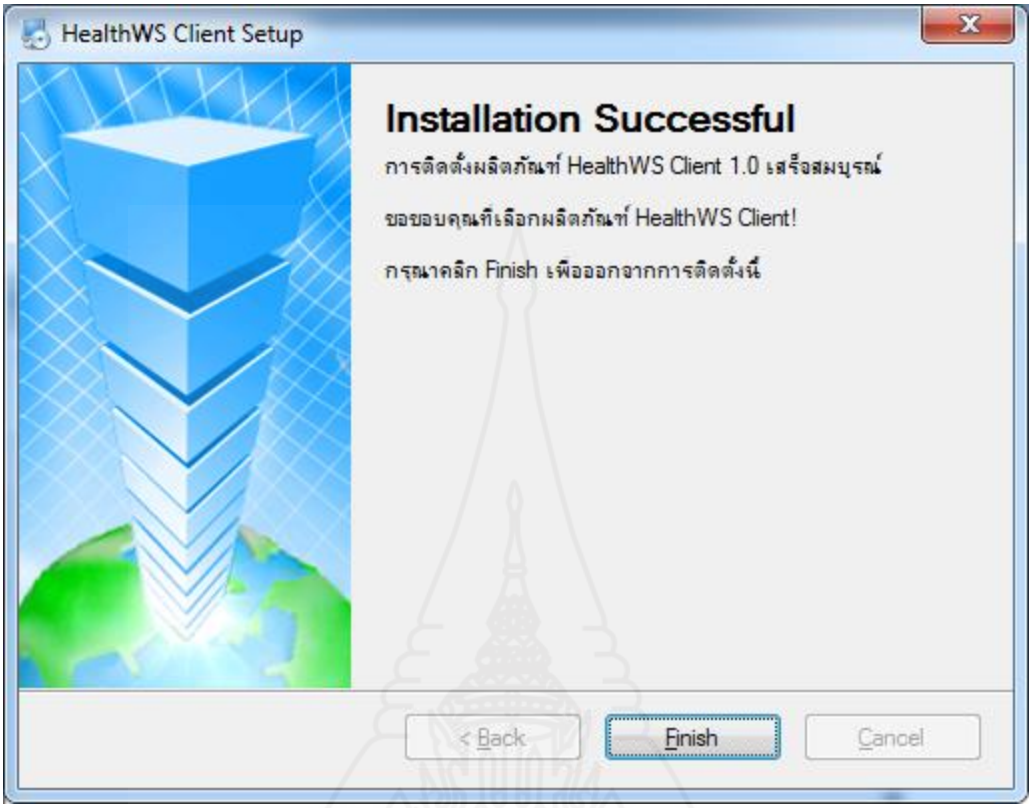
ภาพที่ ข-6 การติดตั้ง หน้าจอ Shortcut Folder

7. หน้าจอ Ready to Install ให้กดปุ่ม Next>



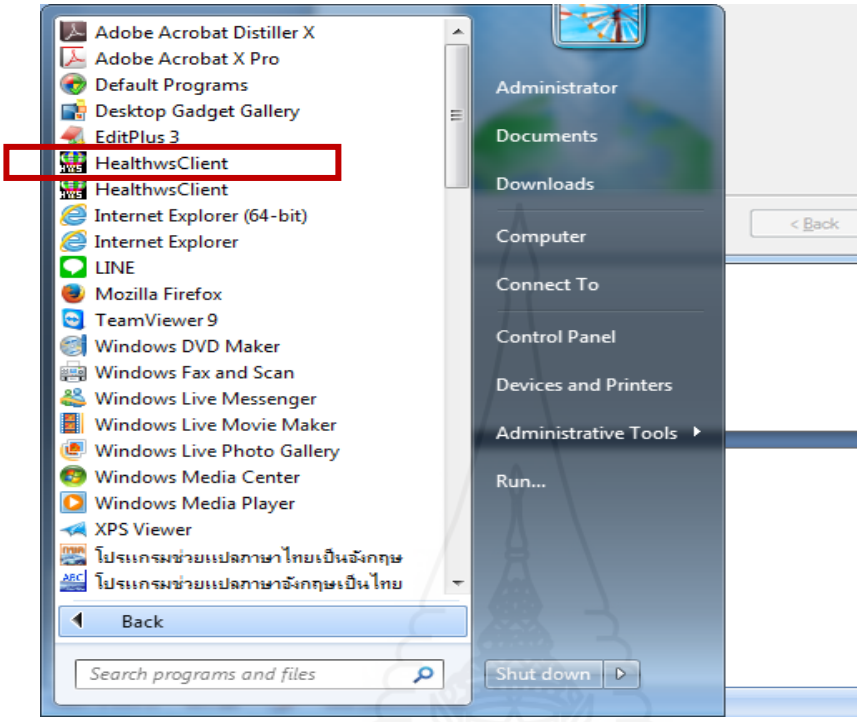
ภาพที่ ข-7 การติดตั้ง หน้าจอ Ready to Install

8.โปรแกรมจะทำการติดตั้ง จนเสร็จและกดปุ่ม finish เพื่อออกจากการติดตั้ง



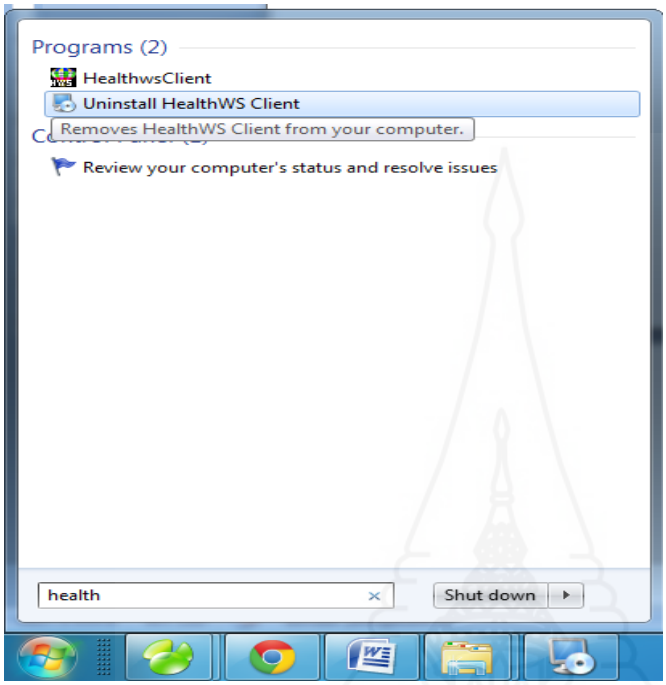
ภาพที่ ข-8 การติดตั้ง การติดตั้งเสร็จ

9.การเข้าใช้งานให้คลิกเมนู start และ เลือก Healthws-Client



ภาพที่ ข-9 การติดตั้ง หน้าจอการเข้าใช้งาน

10.การยกเลิกการติดตั้งโปรแกรม Healthws-Client ให้ให้คลิกเมนู start และ เลือก Uninstall Healthws Client



ภาพที่ ข-10 การยกเลิกการติดตั้งโปรแกรม

ภาคผนวก ค

คู่มือการใช้งานระบบ Healthws-Client

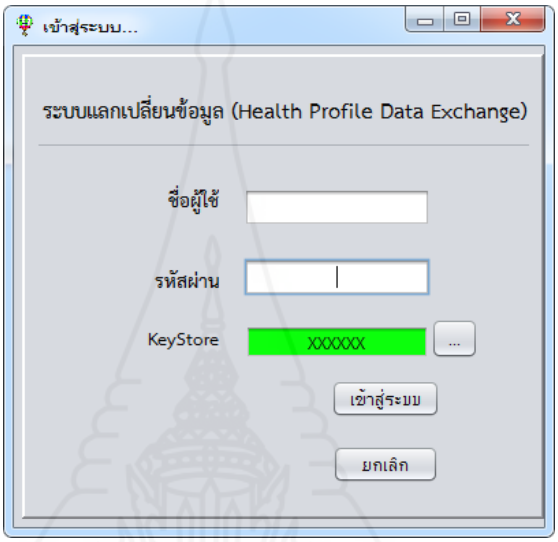
- Java Application
- Web Application

คู่มือการใช้งานระบบ Healthws-Client

JAVA Applicaton

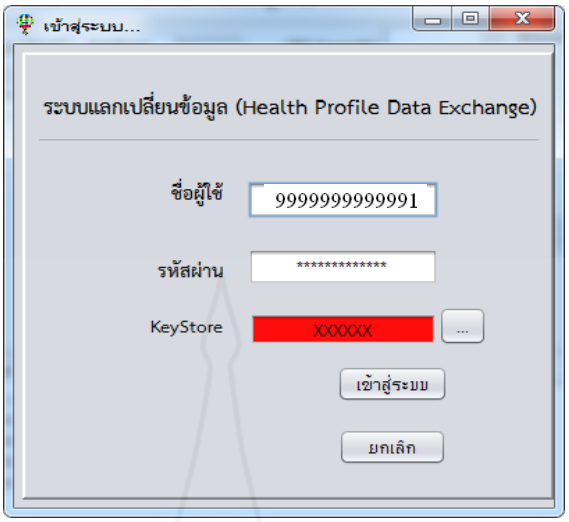
- **ระบบ Healthws-Client**

1. การเข้าสู่ระบบ ให้ระบุรหัสชื่อผู้ใช้งานและรหัสผ่านให้ถูกต้อง หลังจากนั้นกด เข้าสู่ระบบเพื่อเข้าใช้งานดังภาพที่ ค-1

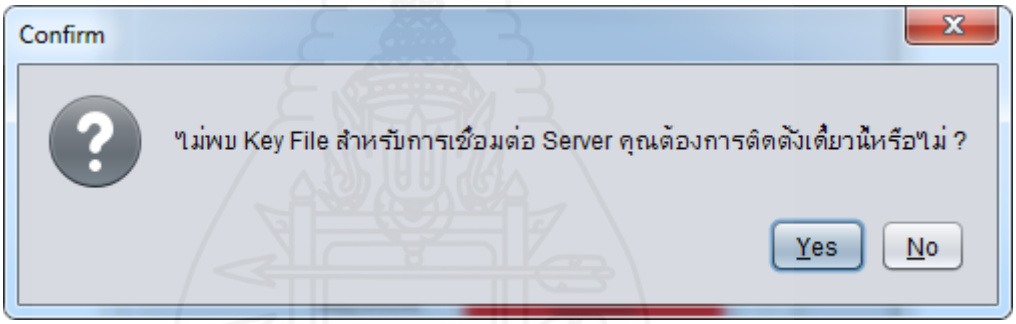


ภาพที่ ค-1 หน้าจอเข้าสู่ระบบ Healthws Client

2. หากไม่พบไฟล์ healthws.keystore ซึ่งใช้ในการติดต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ ระบบจะแจ้งเตือน ตาภาพที่ ค-2 และภาพที่ ค-3 และเปิดหน้าจอการค้นหาไฟล์ healthws.keystore ดังภาพที่ ค-4 สามารถติดตั้งไฟล์ healthws.keystore ได้จากผู้ดูแลระบบเว็บเซอร์วิสเซิร์ฟเวอร์ ให้ถูกต้องและทำการเข้าสู่ระบบ กรณีที่มีการระบุข้อมูลใดไม่ถูกต้องจะมีหน้าต่างข้อความแจ้งเตือนดังภาพที่ ค-2 หากไม่สามารถเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ได้ จะมีหน้าจอแจ้งเตือนความผิดพลาดดังภาพที่ ค-5

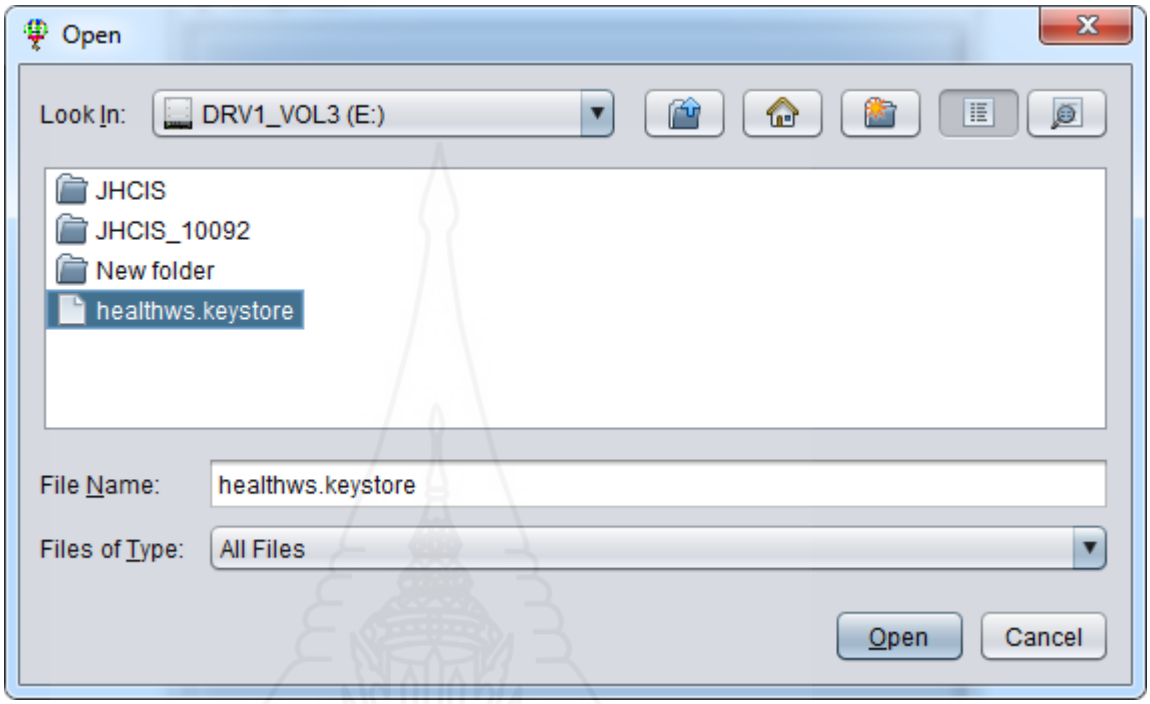


ภาพที่ ค-2 หน้าจอเข้าสู่ระบบ ไม่พบไฟล์ healthws.keystore



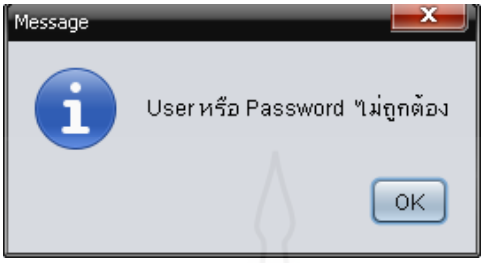
ภาพที่ ค-3 หน้าจอแจ้งเตือนไม่พบไฟล์ healthws.keystore

3. หน้าจอการค้นหาไฟล์ healthws.keystore ที่ใช้ในการเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ ตามภาพที่ ค-4



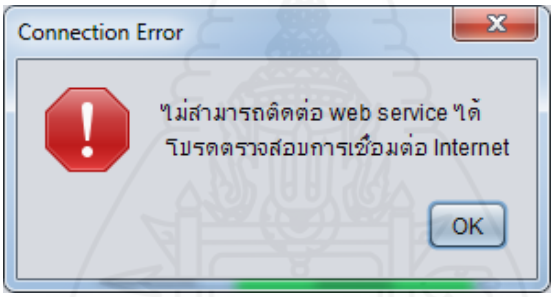
ภาพที่ ค-4 หน้าจอการค้นหาไฟล์ healthws.keystore

4. กรณีที่มีการระบุข้อมูลในการเข้าสู่ระบบไม่ถูกต้องจะมีหน้าต่างข้อความแจ้งเตือน ดังภาพที่ ค-5



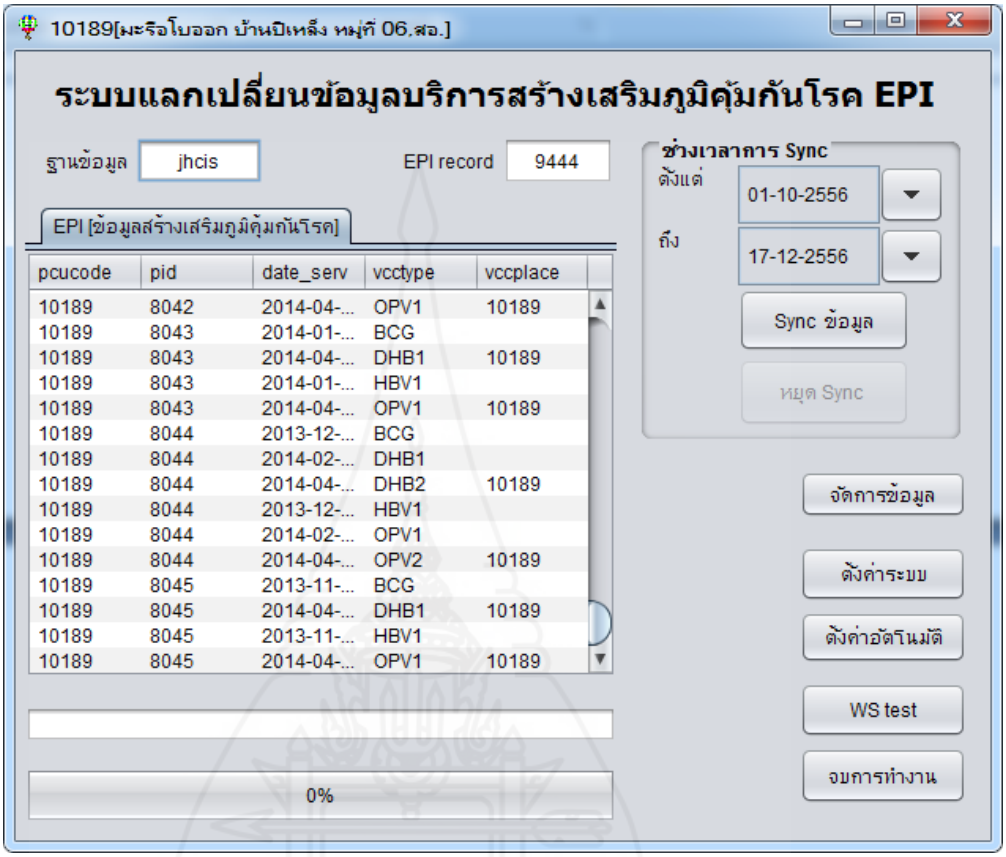
ภาพที่ ค-5 หน้าจอแจ้งเตือนเมื่อผู้ใช้งานกรอกข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน

5.หากไม่สามารถเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ได้ จะมีหน้าจอแจ้งเตือนความผิดพลาดดังภาพที่ ค-6



ภาพที่ ค-6 หน้าจอแจ้งเตือนเมื่อไม่สามารถเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์ได้

6. หากเข้าสู่ระบบได้สำเร็จจะเข้าสู่หน้าจอหลักระบบแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรค EPI



ภาพที่ ค-7 หน้าจอหลักระบบแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรค EPI

7. รายละเอียดหน้าจอหลักระบบแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรค EPI ตามภาพที่ ค-8 มีดังนี้

1) คือ ชื่อฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล

2) คือ จำนวนข้อมูลในตาราง visitepi ในฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล

3) คือ รายละเอียดข้อมูลจากตาราง visitepi

4) คือ กล่องข้อความแสดงสถานะการทำงานของ โปรแกรม Healthws-Client

5) คือ progressbar แสดงความก้าวหน้าในขณะทำงานดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์

6) คือ ช่วงเวลาของข้อมูลที่ต้องการแลกเปลี่ยน บันทึกอยู่ในไฟล์ database. properties ของโปรแกรม Healthws-Client สามารถตั้งค่าได้จากปุ่มตั้งค่าระบบ หรือ หรือแก้ไขไฟล์ database. properties

7) คือ ปุ่มเริ่มต้น ดึงข้อมูล และปุ่มหยุดการดึงข้อมูล

8) คือ ปุ่มจัดการข้อมูล การบริการสร้างเสริมภูมิคุ้มกันโรค EPI จากข้อมูลในฐานฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบล

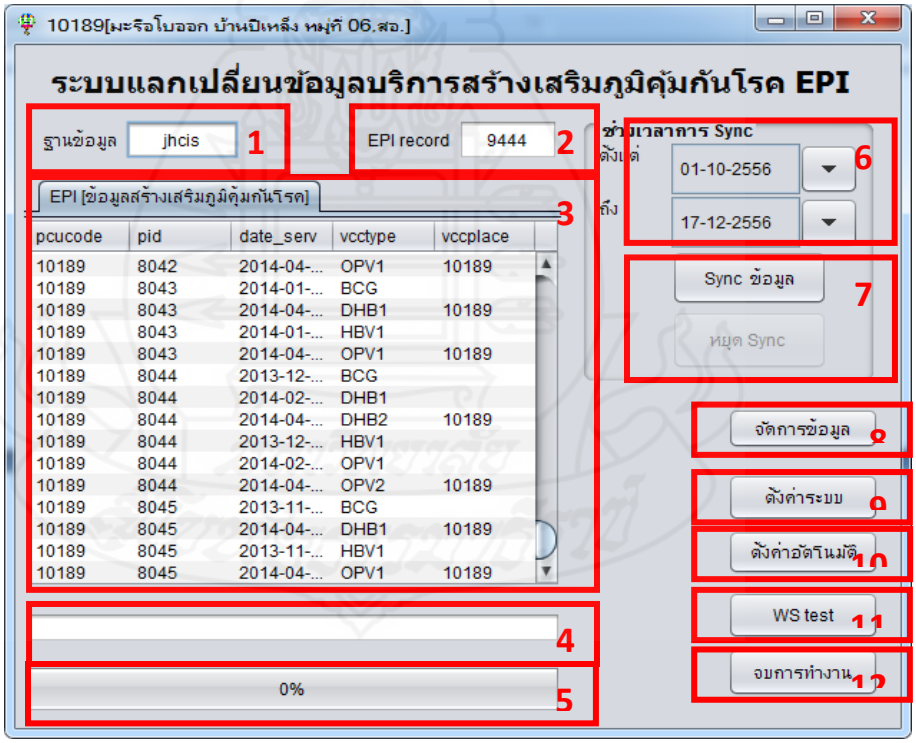
9) คือ ปุ่มการตั้งค่าที่ใช้ในการทำงานของโปรแกรม Healthws-Client

10) คือ ปุ่มการตั้งเวลาการดึงข้อมูลอัตโนมัติจากเว็บเซอร์วิสเซิร์ฟเวอร์

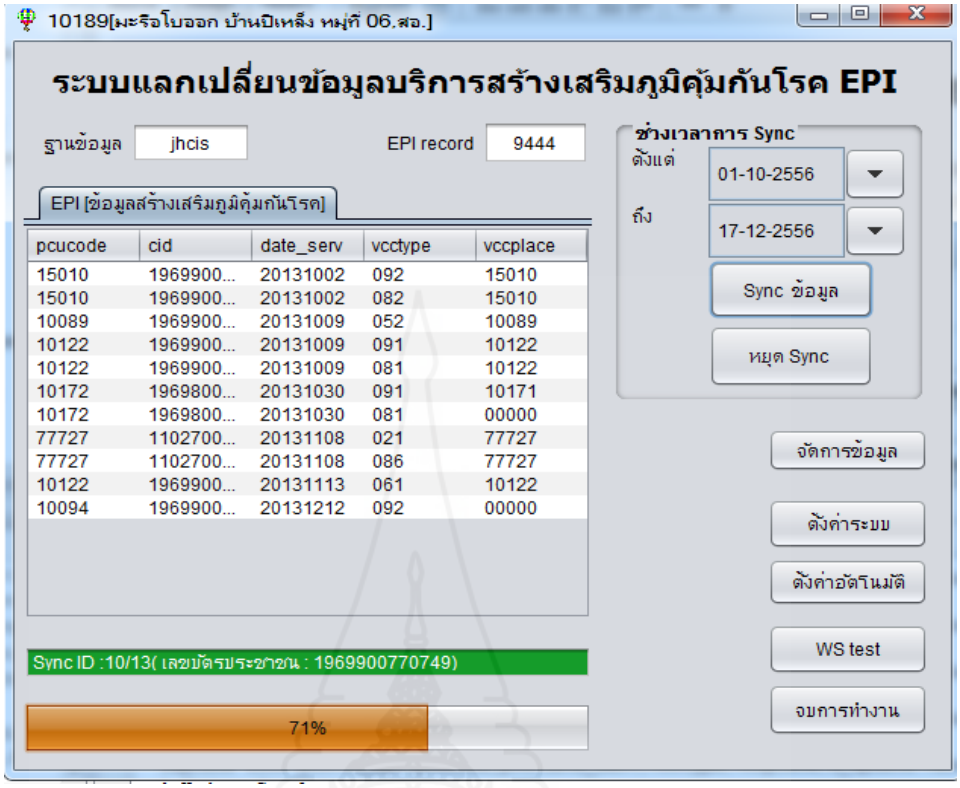
11) คือ ปุ่มทดสอบการเชื่อมต่อกับเว็บเซอร์วิสเซิร์ฟเวอร์

12 คือ ปุ่มจบการทำงาน

8. ระบบกำลังทำงานดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์ ตามภาพที่ ค-9

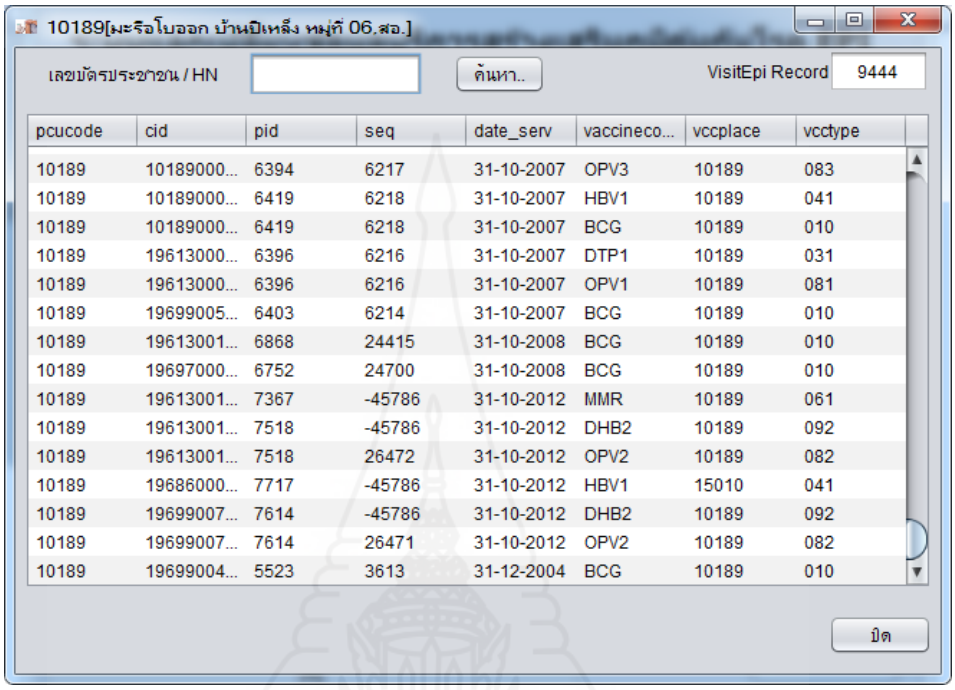


ภาพที่ ค-8 รายละเอียดหน้าจอหลักระบบแลกเปลี่ยนข้อมูลบริการสร้างเสริมภูมิคุ้มกันโรค EPI



ภาพที่ ค-9 หน้าจอระบบกำลังทำงานดึงข้อมูลจากเว็บเซอร์วิสเซิร์ฟเวอร์

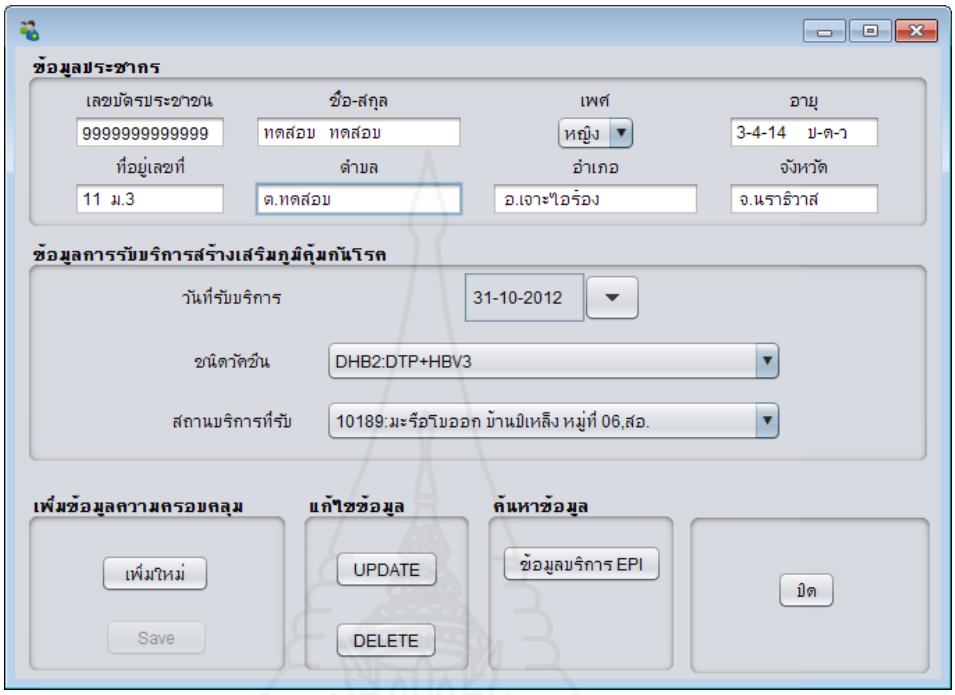
9. การจัดการข้อมูลในตาราง visitepi คลิกปุ่ม จัดการข้อมูล จะปรากฏหน้าจอ ตามภาพที่ ค-10



pcucode	cid	pid	seq	date_serv	vaccineco...	vccplace	vcctype
10189	10189000...	6394	6217	31-10-2007	OPV3	10189	083
10189	10189000...	6419	6218	31-10-2007	HBV1	10189	041
10189	10189000...	6419	6218	31-10-2007	BCG	10189	010
10189	19613000...	6396	6216	31-10-2007	DTP1	10189	031
10189	19613000...	6396	6216	31-10-2007	OPV1	10189	081
10189	19699005...	6403	6214	31-10-2007	BCG	10189	010
10189	19613001...	6868	24415	31-10-2008	BCG	10189	010
10189	19697000...	6752	24700	31-10-2008	BCG	10189	010
10189	19613001...	7367	-45786	31-10-2012	MMR	10189	061
10189	19613001...	7518	-45786	31-10-2012	DHB2	10189	092
10189	19613001...	7518	26472	31-10-2012	OPV2	10189	082
10189	19686000...	7717	-45786	31-10-2012	HBV1	15010	041
10189	19699007...	7614	-45786	31-10-2012	DHB2	10189	092
10189	19699007...	7614	26471	31-10-2012	OPV2	10189	082
10189	19699004...	5523	3613	31-12-2004	BCG	10189	010

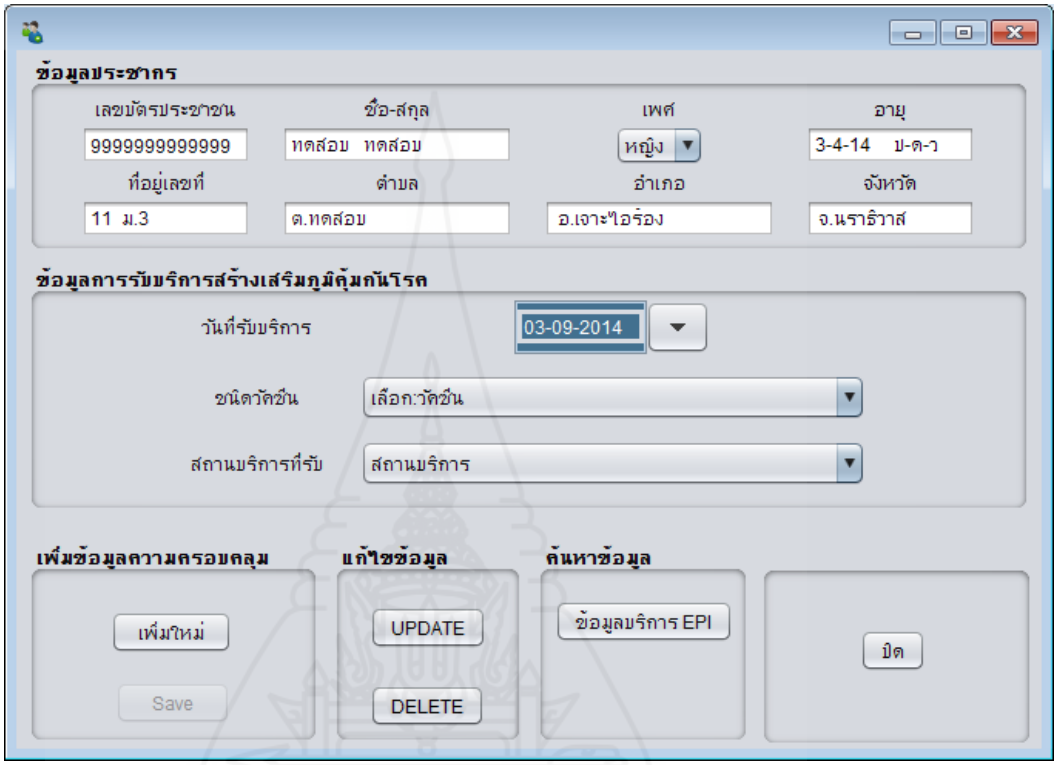
ภาพที่ ค-10 หน้าจอหลักระบบจัดการข้อมูลผู้รับบริการ

10. สามารถค้นหาผู้รับบริการโดยกรอกเลขบัตรประชาชน หรือ เลขประจำตัวผู้รับบริการ และดับเบิลคลิกเมาส์ เพื่อเปิดหน้าจอข้อมูลของผู้รับบริการขึ้นมา ตามภาพที่ ค-11



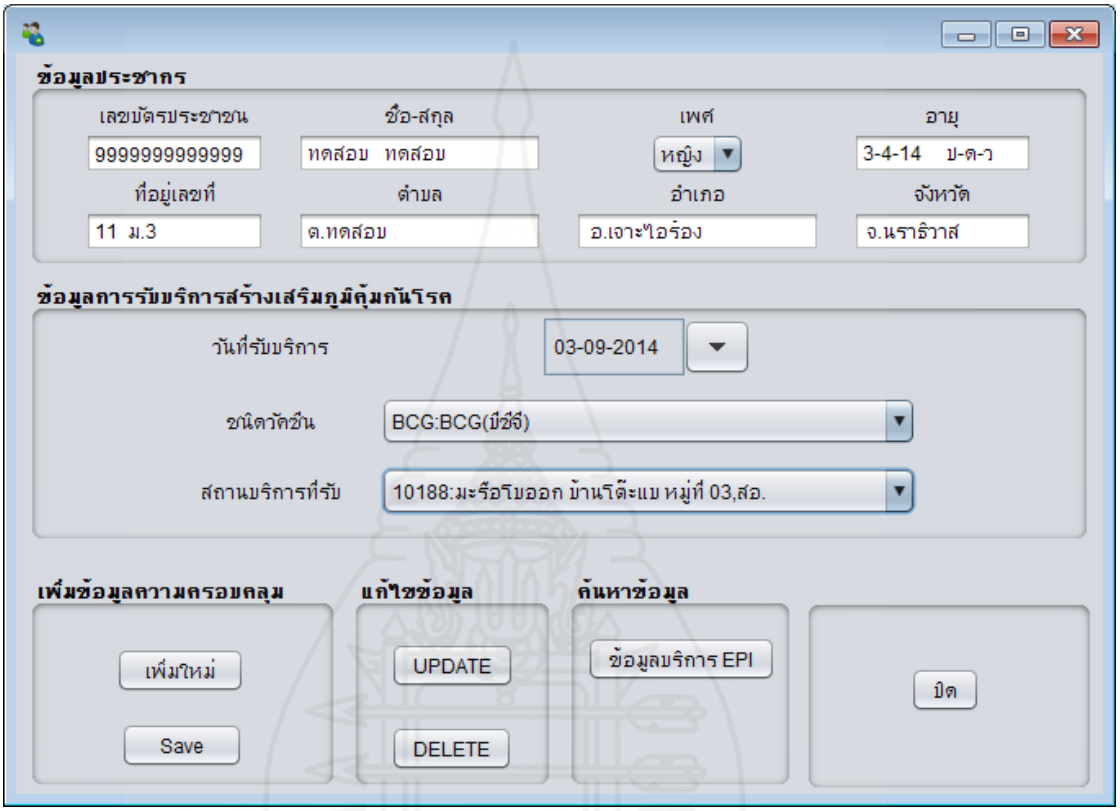
ภาพที่ ค-11 หน้าจอหลักจัดการข้อมูลผู้รับบริการ รายบุคคล

11. การเพิ่มข้อมูลความครอบคลุมการบริการสร้างเสริมภูมิคุ้มกันโรค EPI สามารถกดปุ่มเพิ่มใหม่ และเลือก วัน เดือน ปีที่รับบริการ ชนิดวัคซีน และหน่วยบริการที่รับบริการ ตามภาพที่ ค-12

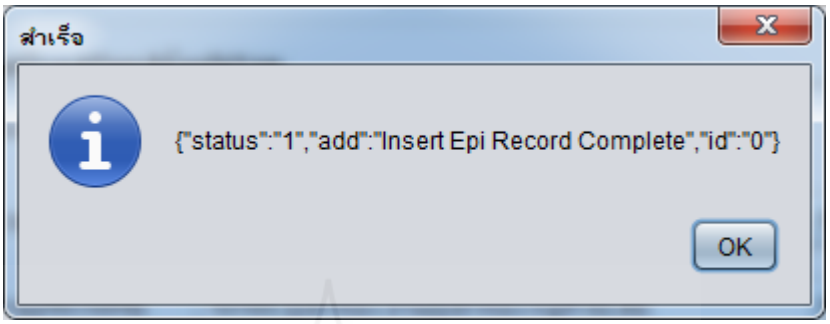


ภาพที่ ค-12 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล เพิ่มข้อมูลความครอบคลุมรายใหม่

12. หากบันทึกข้อมูลครบ จะสามารถเพิ่มข้อมูลเข้าไปในตาราง visitepi ในฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบลและในตาราง epi ของฐานข้อมูล provisdb ของระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยเว็บเซอร์วิสเซิร์ฟเวอร์ ตามภาพที่ ค-13 และภาพที่ ค-14

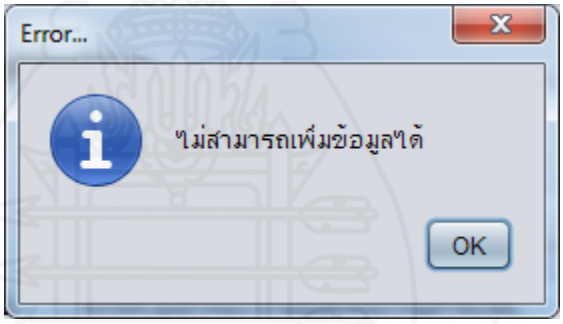


ภาพที่ ค-13 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล กดปุ่ม Save เพื่อเพิ่มข้อมูลความครอบคลุมรายใหม่



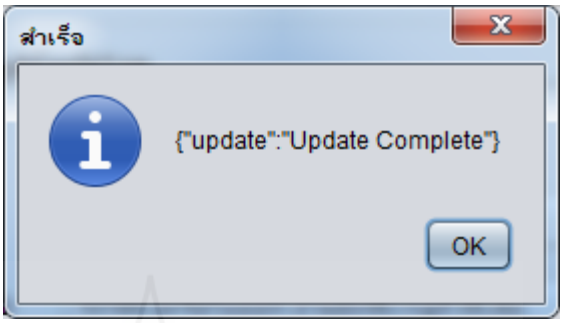
ภาพที่ ค-14 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล เพิ่มข้อมูลความครอบคลุมรายใหม่สำเร็จ

13. หากข้อมูลที่ต้องการเพิ่มมีอยู่ในตาราง epi ของฐานข้อมูล provisdb ของระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) และ หน้าจอจะแจ้งเตือน ตามภาพที่ ค-15



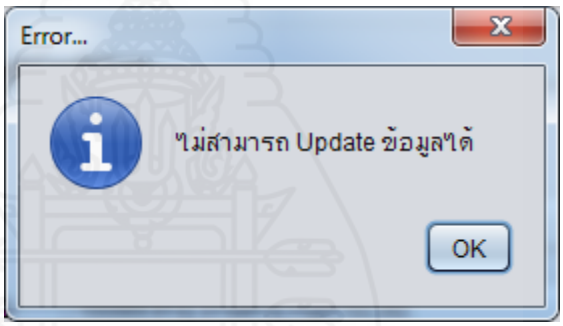
ภาพที่ ค-15 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล เพิ่มข้อมูลความครอบคลุมรายใหม่ไม่สำเร็จ

14. การปรับปรุงข้อมูลการบริการสร้างเสริมภูมิคุ้มกันโรค โดยการแก้ไขข้อมูล ชนิดวัคซีน และหน่วยบริการที่รับบริการ และกดปุ่ม UPDATE หากการปรับปรุงข้อมูลในตาราง visitepi ในฐานข้อมูลของโรงพยาบาลส่งเสริมสุขภาพตำบลและในตาราง epi ของฐานข้อมูล provisdb ของระบบสารสนเทศเพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยเว็บเซอร์วิสเซิร์ฟเวอร์สำเร็จ ตามภาพที่ ค-16



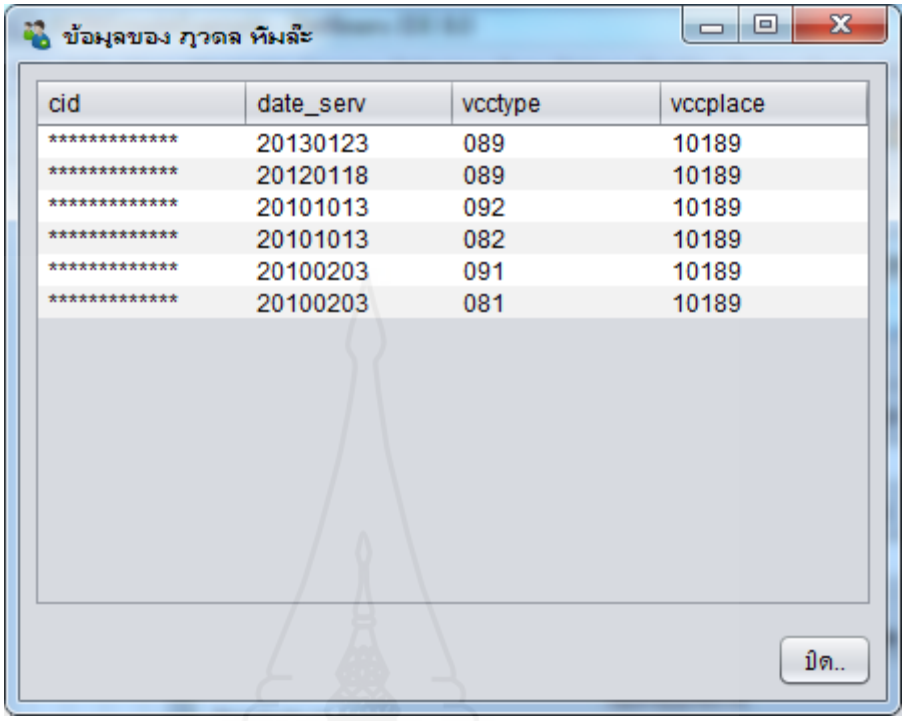
ภาพที่ ค-16 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล ปรับปรุงข้อมูลการรับบริการสำเร็จ

15. หากการปรับปรุงข้อมูลไม่สำเร็จ เนื่องจากมีข้อมูลซ้ำและปรากฏหน้าจอตามภาพที่ ค-17



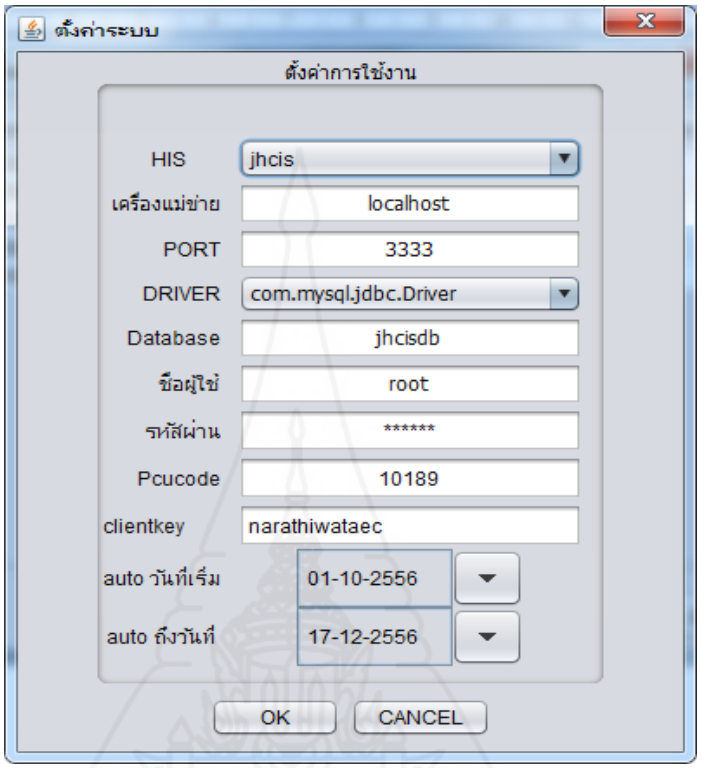
ภาพที่ ค-17 หน้าจอจัดการข้อมูลผู้รับบริการ รายบุคคล ปรับปรุงข้อมูลการรับบริการไม่สำเร็จ

16. การแสดงประวัติการรับบริการสร้างเสริมภูมิคุ้มกันโรค จากฐานข้อมูล provisdb ของระบบสารสนเทศ เพื่อการบริหารจัดการข้อมูลด้านสาธารณสุข (PROVIS) โดยเว็บเซอร์วิสเซิร์ฟเวอร์ ตามภาพที่ ค-18



ภาพที่ ค-18 หน้าจอจัดการข้อมูลผู้รับบริการ ประวัติการรับบริการรายบุคคล จากเว็บเซอร์วิสเซิร์ฟเวอร์

17. การตั้งค่าเพื่อการใช้งานระบบโปรแกรม Healthws-Client โดยกดปุ่ม ตั้งค่าระบบ จากหน้าจอหลัก ตามภาพที่ ค-19



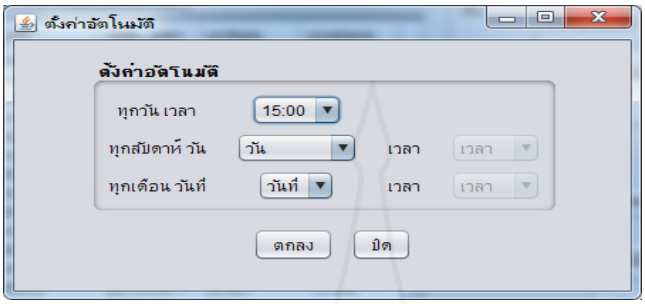
ภาพที่ ค-19 หน้าจอตั้งค่าในการแลกเปลี่ยนข้อมูลการรับบริการรายบุคคล จากเว็บเซอร์วิสเซิร์ฟเวอร์

18. การหากต้องการดึงข้อมูลอัตโนมัติ เพื่อดึงข้อมูลผู้รับบริการสร้างเสริมภูมิคุ้มกันโรคของผู้รับบริการในเขตรับผิดชอบที่ไปรับบริการที่หน่วยบริการสาธารณสุขอื่นๆ ในจังหวัดนราธิวาสเข้ามาในฐานข้อมูล JHCISDB ของโรงพยาบาลส่งเสริมสุขภาพตำบลทันที โดยใช้ค่า Configuration ที่บันทึกไว้ จากการตั้งค่าจาก ปุ่ม ตั้งค่าอัตโนมัติ ตามภาพที่ ค-20 ซึ่งสามารถตั้งค่าได้ตาม 3 รูปแบบ คือ

1) ดึงข้อมูลอัตโนมัติทุกวัน ต้องระบุเวลา

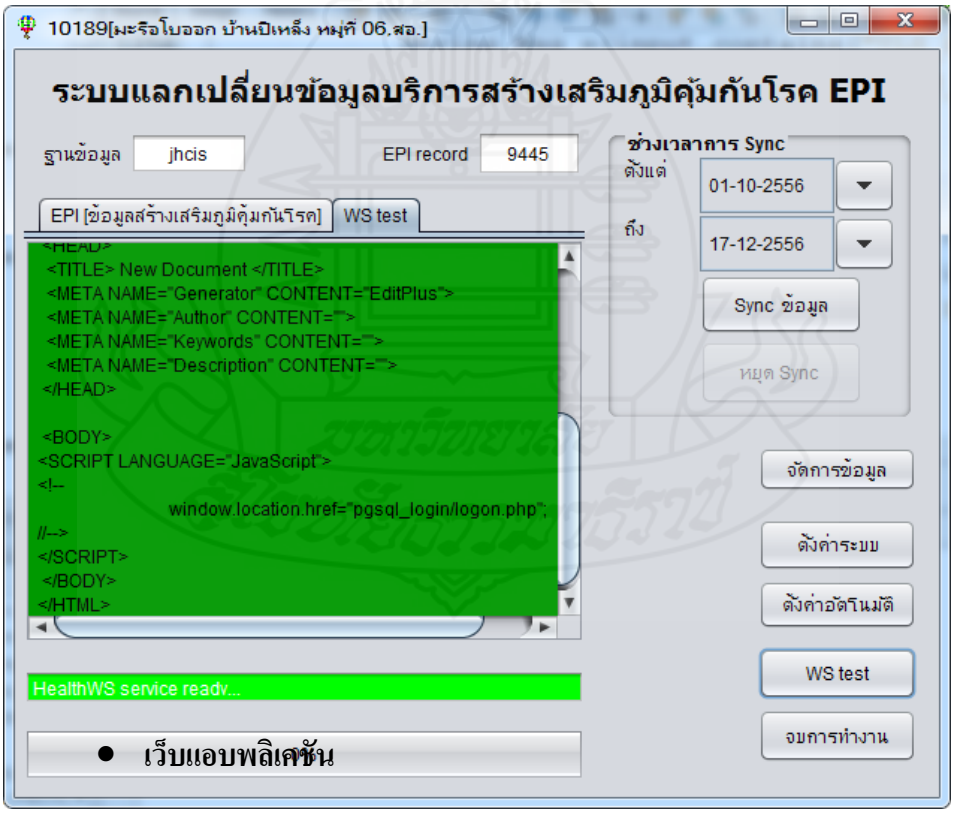
2) ดึงข้อมูลอัตโนมัติทุกสัปดาห์ ต้องระบุวันและระบุเวลา

3) ดึงข้อมูลอัตโนมัติทุกเดือน ต้องระบุวันที่และระบุเวลา



ภาพที่ ค-20 หน้าจอตั้งค่าการดึงข้อมูลอัตโนมัติ จากเว็บเซอร์วิสเซิร์ฟเวอร์

19. การทดสอบการเชื่อมต่อ เว็บเซอร์วิสเซิร์ฟเวอร์ สามารถกดปุ่ม WS test ตามภาพที่ ค-21



ภาพที่ ค-21 หน้าจอทดสอบการเชื่อมต่อ เว็บเซอร์วิสเซิร์ฟเวอร์

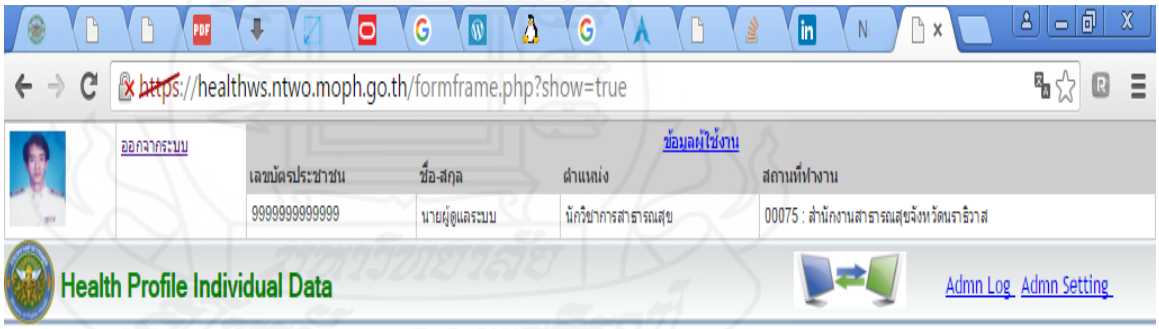
1. การเข้าสู่ระบบ เป็นหน้าจอเพื่อให้ผู้ใช้งานกรอกชื่อผู้ใช้งาน และรหัสผ่าน เพื่อทำการยืนยันเข้าใช้งานระบบ โดยสิทธิ์ในการใช้งานระบบ มี 2 กลุ่ม คือ ผู้ดูแลระบบ และกลุ่มผู้ใช้งานทั่วไป แต่ละกลุ่มจะมีเมนูในการใช้งานแตกต่างกัน ภาพที่ ค-22 แสดงหน้าจอการใช้งาน โดยต้องระบุชื่อผู้ใช้ รหัสผ่าน และรหัสสุ่มโดยระบบ (CAPCHA) ให้ถูกต้องและทำการเข้าสู่ระบบ กรณีที่มีการระบุข้อมูลใดไม่ถูกต้องจะมีหน้าต่างข้อความแจ้งเตือนกังภาพที่ ค-23

ภาพที่ ค-22 หน้าจอการเข้าสู่ระบบ Web Application

ภาพที่ ค-23 หน้าจอแจ้งเตือนเมื่อผู้ใช้งานกรอกข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน

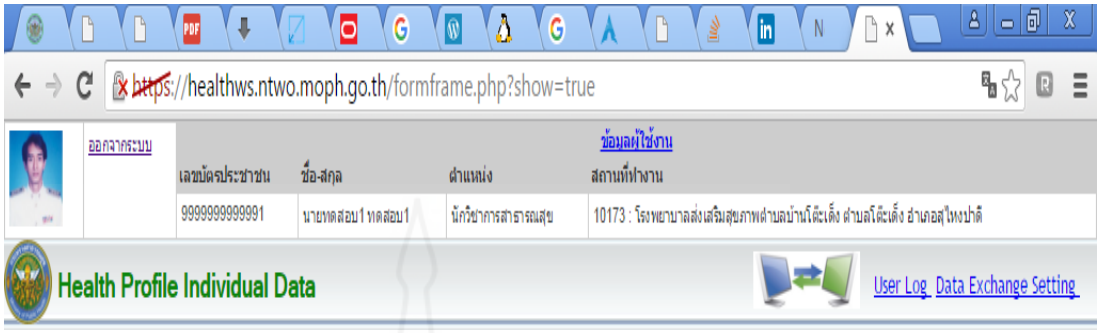
2. หน้าหลักของระบบ โดยระบบจะแสดงเมนูตามสิทธิ์ของผู้ใช้งาน 2 กลุ่ม คือ

ก) ผู้ดูแลระบบ มีเมนูหลัก คือ Admin Setting และ Admin Log ดังภาพที่ ค-24



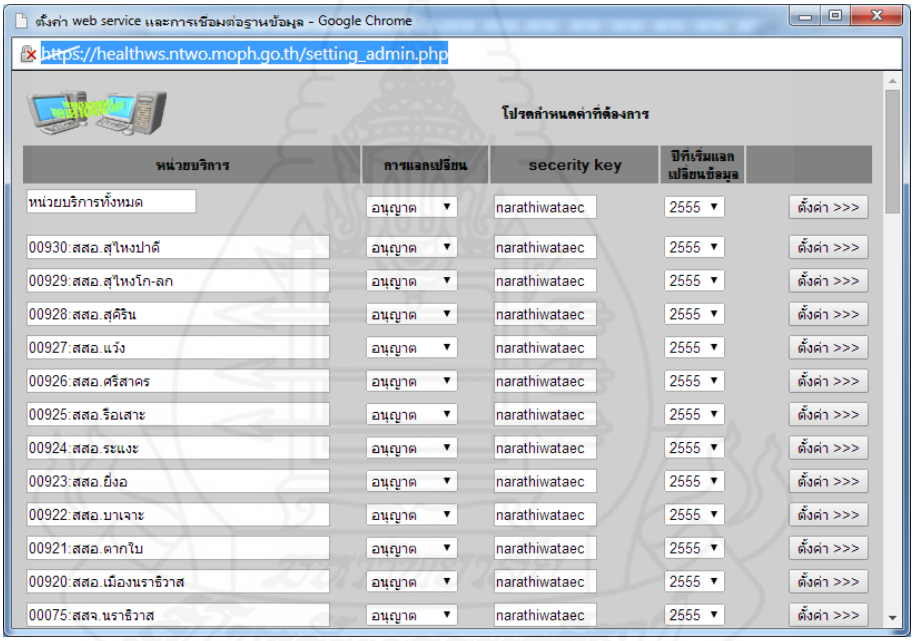
ภาพที่ ค-24 หน้าจอ เมนูหลักผู้ดูแลระบบ

ข) ผู้ใช้งาน มีเมนูหลัก คือ Data Exchange Setting และ User Log ดังภาพที่ ค-25



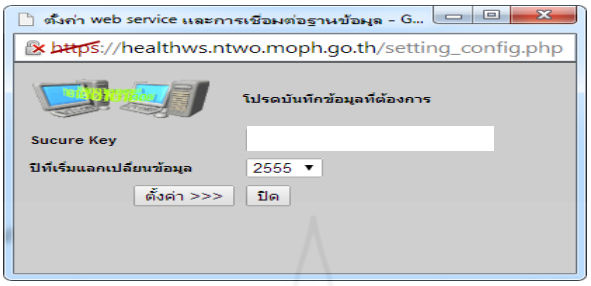
ภาพที่ ค-25 หน้าจอ เมนูหลักผู้ใช้งาน

ค) หน้าจอ เมนู Admin Setting ของผู้ดูแลระบบ ดังภาพ ค-26



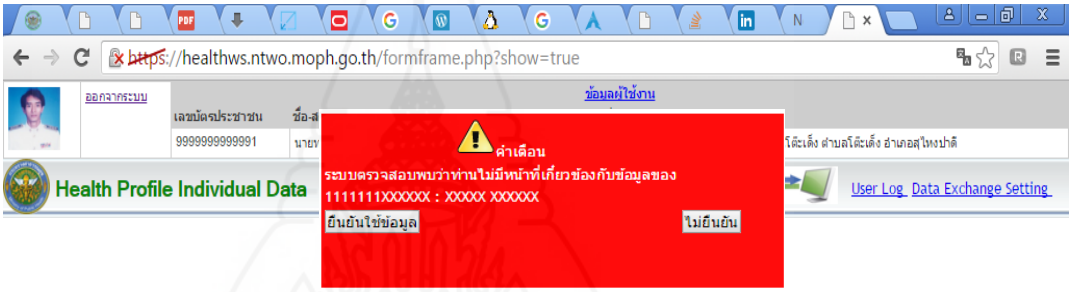
ภาพที่ ค-26 หน้าจอหลักในสิทธิ์ผู้ดูแลระบบ เมนู Admin Setting

ง) หน้าจอ เมนู Data Exchange Setting ของผู้ใช้งาน ดังภาพที่ ค-27



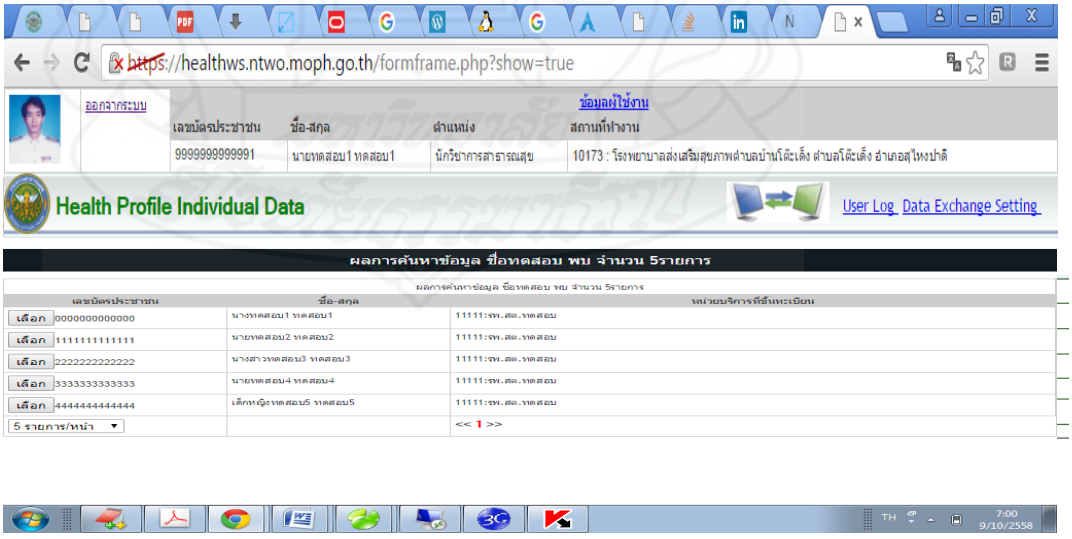
ภาพที่ ค-27 หน้าจอหลักในสิทธิ์ผู้ใช้งาน เมนู Data Exchange Setting

จ) จากภาพที่ ค-28 แสดงการค้นหาข้อมูลโดยใช้เลขบัตรประชาชน



ภาพที่ ค-28 ตัวอย่างการค้นหาข้อมูลโดยใช้เลขบัตรประชาชน

ฉ) จากภาพที่ ค-29 แสดงการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ



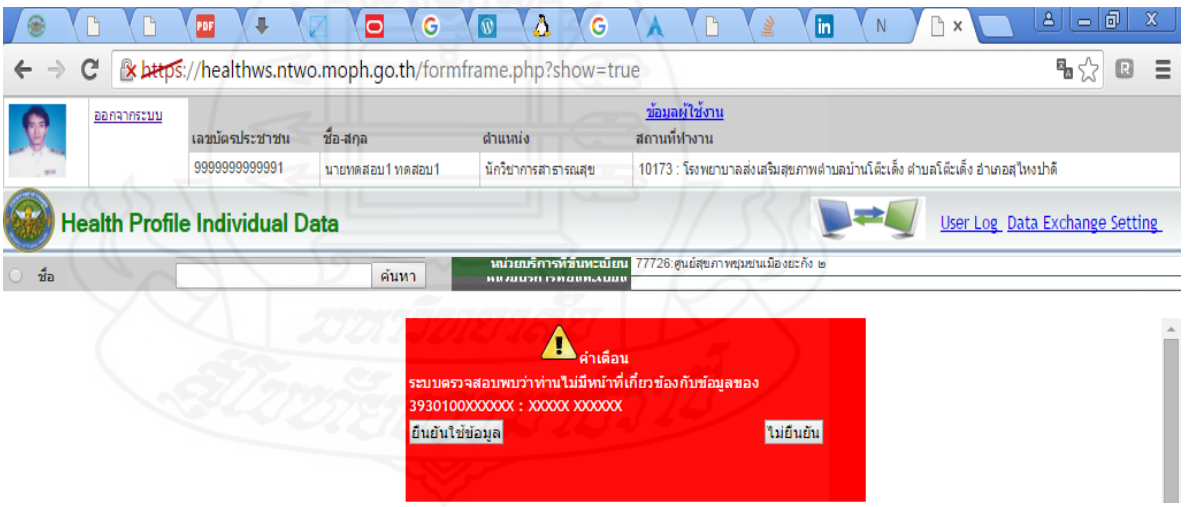
ภาพที่ ค-29 ตัวอย่างการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ

3. การเรียกใช้ข้อมูลทุกครั้งจะมีการบันทึกข้อมูลเลขบัตรประชาชนผู้ใช้งาน วัน เดือน ปีที่เรียกใช้ เลขบัตรประชาชนผู้ที่ถูกเรียกดูข้อมูล หมายเลขแมค แอดเดรสที่อยู่ของเครื่องคอมพิวเตอร์ หรือ อุปกรณ์ที่เรียกดูข้อมูล หมายเลขไอพี แอดเดรส ที่อยู่ของเครื่องคอมพิวเตอร์ หรือ อุปกรณ์ที่เรียกดู ไว้ทุกครั้งสำหรับผู้ใช้งาน หรือ ผู้ดูแลระบบจะตรวจสอบประวัติการเรียกดูข้อมูลได้ภายหลัง ตลอดเวลา

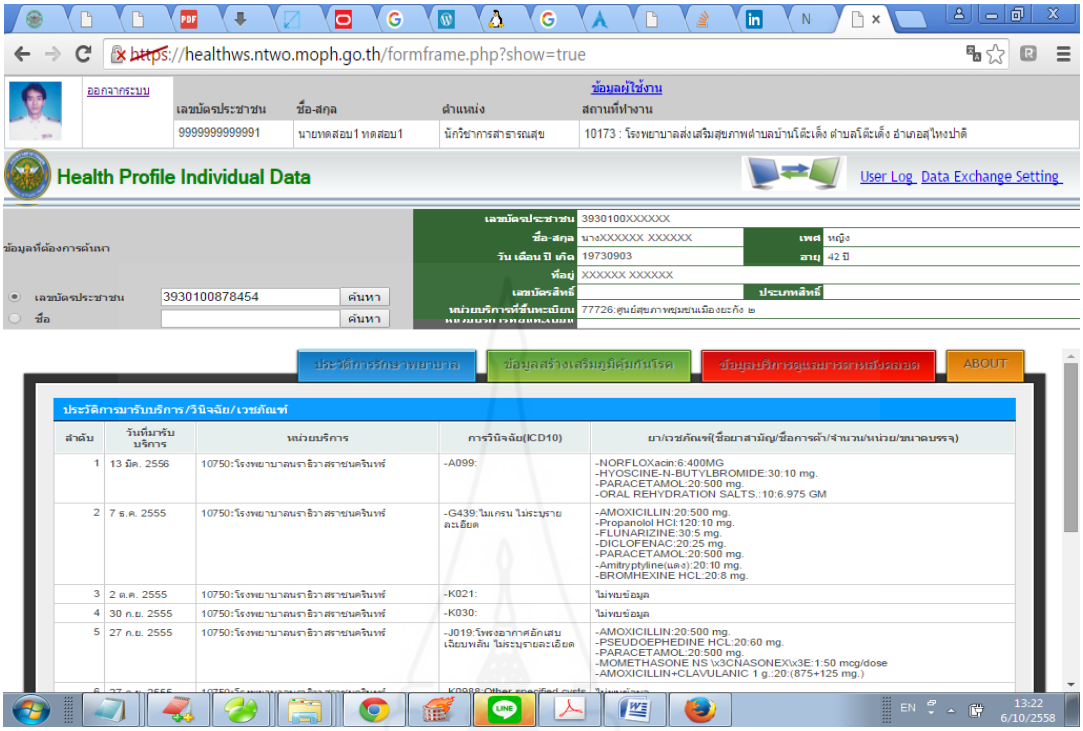
จากภาพที่ ค-30 แสดงข้อมูลผู้รับบริการ คือ เลขบัตรประจำตัวปะชาชน ชื่อ-สกุล เพศ วันเดือนปีเกิด อายุ ที่อยู่ เลขที่บัตรสิทธิ์ประกันสุขภาพ ประเภทสิทธิ์ประกันสุขภาพ และหน่วยบริการที่ขึ้นทะเบียน รับผิดชอบไว้ ตามสิทธิ 2 แบบ คือ

1) ผู้ใช้งานเป็นผู้มีสิทธิในการเข้าถึงข้อมูลแบบ All ระบบจะแสดงข้อมูลผู้รับบริการ คือ เลขบัตรประจำตัวปะชาชน ชื่อ-สกุล เพศ วันเดือนปีเกิด อายุ ที่อยู่ เลขที่บัตรสิทธิ์ประกันสุขภาพ ประเภทสิทธิ์ประกันสุขภาพ และหน่วยบริการที่ขึ้นทะเบียนรับผิดชอบไว้

2) ผู้ใช้งานเป็นผู้มีสิทธิในการเข้าถึงข้อมูลแบบ Any เนื่องจากผู้ที่ใช้งานระบบและข้อมูลที่ค้นหาไม่ใช่บุคคลเดียวกัน ระบบจะมีหน้าจอเตือนผู้ที่เข้าใช้งานก่อนเข้าเรียกดูและไม่แสดงข้อมูลเลขบัตรประชาชน ชื่อ สกุลและที่อยู่ และให้ยืนยัน หรือไม่ยืนยันการเรียกดูข้อมูลและเก็บข้อมูลของผู้เข้าใช้งานระบบไว้ทั้ง 2 กรณี



ภาพที่ ค-30 ตัวอย่างการค้นหาข้อมูลโดยใช้ชื่อของผู้รับบริการ



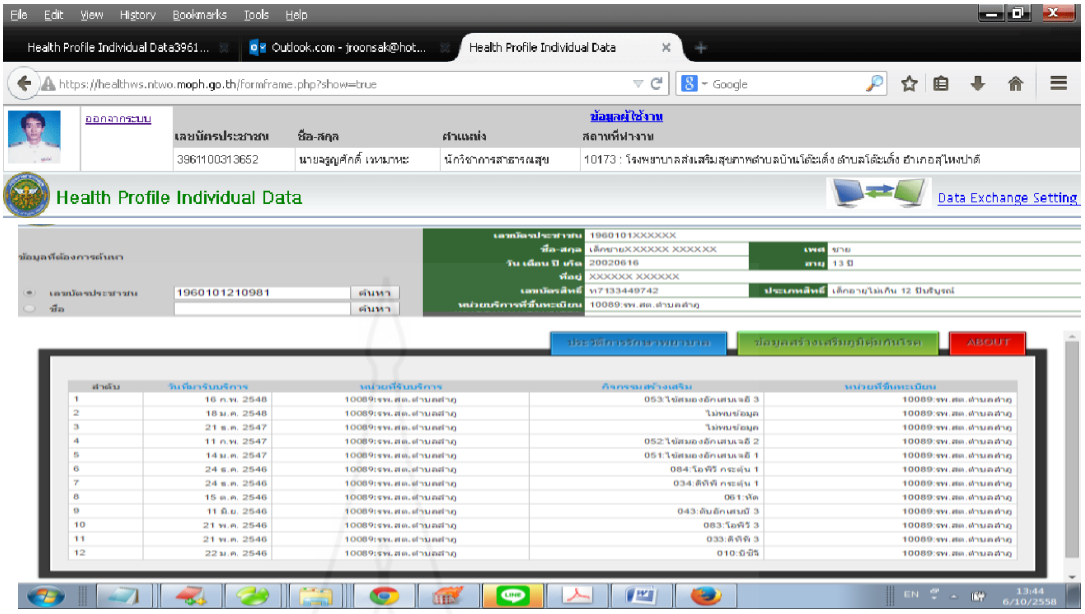
ภาพที่ ค-31 ข้อมูลประวัติการรับบริการรักษาพยาบาล

จากภาพที่ ค-31, ภาพที่ ค-32 และภาพที่ ค-33 หากผู้เข้าใช้ระบบยืนยันการเรียกดูข้อมูล ระบบจะแสดงข้อมูลผู้รับบริการ 3 ส่วน คือ

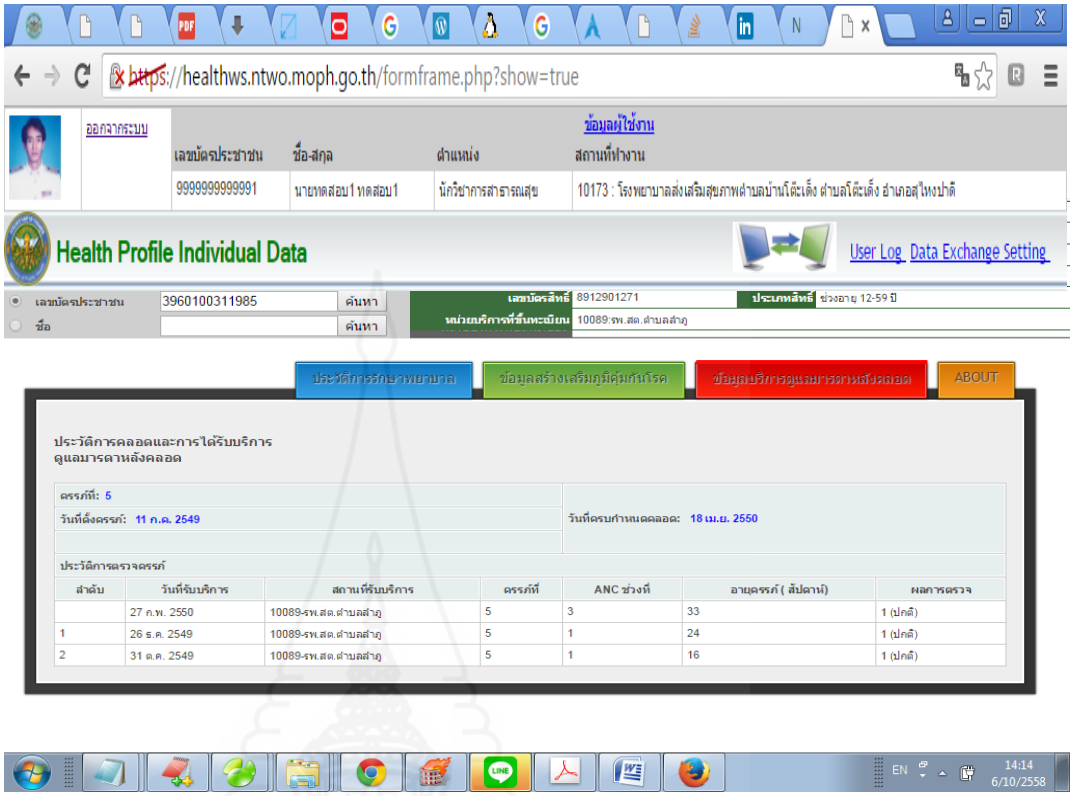
ส่วนที่ 1 ประวัติการรับบริการรักษาพยาบาล ย้อนหลัง 10 ครั้งที่มารับบริการ

ส่วนที่ 2 ประวัติการรับบริการสร้างเสริมภูมิคุ้มกันโรค ย้อนหลัง 10 ครั้งที่มารับบริการ

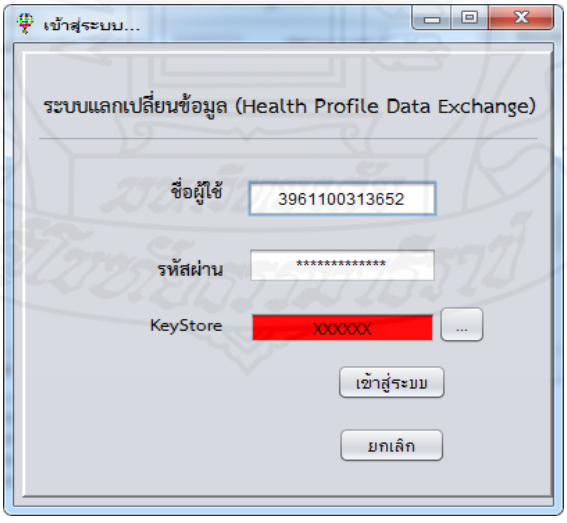
ส่วนที่ 3 ประวัติการรับบริการดูแลมารดาหลังคลอด ย้อนหลัง 10 ครั้งที่มารับบริการ



ภาพที่ ค-32 ข้อมูลประวัติการรับบริการสร้างเสริมภูมิคุ้มกันโรค



ภาพที่ ค-33 ข้อมูลประวัติการรับบริการดูแลมารดาหลังคลอด



ภาคผนวก ง

โครงสร้างตารางข้อมูลเจ้าหน้าที่สาธารณสุขจังหวัดนราธิวาส
ในระบบบริหารงานบุคคล (PIS)

โครงสร้างตารางข้อมูลเจ้าหน้าที่สาธารณสุขจังหวัดนราธิวาสจากระบบบริหารงานบุคคล (PIS)

รูปแบบ POSTGRES Database ฐานข้อมูล PIS ตาราง (relation) pispersonel มี ATTRIBUTE ตามตารางที่ ง-1

ตารางที่ ง-1 โครงสร้างคารางข้อมูลเจ้าหน้าที่สาธารณสุข (pispersonel) ในระบบ PIS

Attribute Name	**Column Name**	**Column Datatype**	**PK**
เลขที่ประจำตัว	id	CHAR(15)	(PK)
รหัสคำนำหน้า	pcode	TINYINT	
ชื่อ	fname	CHAR(50)	
นามสกุล	lname	CHAR(50)	
เพศ	sex	CHAR(1)	
เชื้อชาติ	race	CHAR(30)	
สัญชาติ	nationality	CHAR(30)	
รหัสสถานภาพสมรส	mrcode	TINYINT	
รหัสศาสนา	recode	TINYINT	
วันเกิด	birthdate	DATETIME	
วันที่บรรจุ	appointdate	DATETIME	
วันที่เข้าสู่หน่วยงาน	deptdate	DATETIME	
Attribute Name	Column Name	Column Datatype	PK
วันที่เข้าสู่ระดับปัจจุบัน	cdate	DATETIME	
วันที่เกษียณ	retiredate	DATETIME	
รหัสกอง	dcode	SMALLINT	
รหัสกรม	deptcode	SMALLINT	
รหัสหน่วยงาน	sdcode	NUMERIC(5)	
รหัสฝ่าย/กลุ่มงาน	seccode	SMALLINT	
รหัสงาน	jobcode	SMALLINT	
รหัสหมวด	hmcode	TINYINT	
รหัสตำแหน่งสายงาน	poscode	NUMERIC(5)	

Attribute Name	**Column Name**	**Column Datatype**	**PK**
รหัสตำแหน่งบริหาร	excode	NUMERIC(5)	
รหัสตำแหน่งวิชาการ	epcode	NUMERIC(5)	
รหัสจังหวัด	provcode	TINYINT	
ที่อยู่1 เลขที่-ถนน	address1	CHAR(100)	
ที่อยู่1 ตำบล-จังหวัด	address2	CHAR(100)	
โทรศัพท์	tel	CHAR(30)	
รหัสไปรษณีย์	zip	NUMERIC(5)	
รหัสวิชาเอก	macode	SMALLINT	
Attribute Name	Column Name	Column Datatype	PK
รหัสวุฒิการศึกษา	qcode	SMALLINT	
รหัสระดับการศึกษา	ecode	TINYINT	
รหัสประเทศ	cocode	SMALLINT	
เลขที่ตำแหน่ง	posid	CHAR(10)	
ระดับ	c	TINYINT	
เงินเดือน	salary	NUMERIC(8,2)	
ชื่อเดิม	oldfname	CHAR(50)	
สกุลเดิม	oldlname	CHAR(50)	
ชื่อบิดา	father	CHAR(50)	
ชื่อมารดา	mother	CHAR(50)	
ชื่อคู่สมรส	spouse	CHAR(50)	
จำนวนบุตร	childs	TINYINT	
วันลาพักผ่อนคงเหลือ	totalabsent	NUMERIC(5,1)	
salcode	salcode	TINYINT	
รหัสการปฏิบัติงาน	j18code	TINYINT	
ชื่อรูปภาพ	picname	CHAR(50)	
oldid	oldid	NUMERIC(6)	
Attribute Name	Column Name	Column Datatype	PK
วันที่ออกจากหน่วยงาน	exitdate	DATETIME	

Attribute Name	Column Name	Column Datatype	PK
รหัสเงินพิเศษ	spcode	SMALLINT	
จำนวนเงินพิเศษ	spmny	NUMERIC(8,2)	
รักษาการ(รหัส ตน.บริหาร)	spexpos	INTEGER	
ใบประกอบวิชาชีพ	codetrade	SMALLINT	
วันที่เปลี่ยนชื่อ	renamedate	DATETIME	
วันที่รับโอน	getindate	DATETIME	
กสจ/กบข (1/0)	kbk	CHAR(1)	
สถานะบุคคล	pstatus	CHAR(1)	
ว/ว/ชช	ptcode	TINYINT	
วันลาพักผ่อน 1 ตค	vac1oct	NUMERIC (4,1)	
เลขประจำตัวประชาชน	pid	CHAR(13)	
รหัสผ่าน	pwd	VARCHAR(15)	

ภาคผนวก จ

ตัวอย่าง Source code ของเว็บเซอร์วิส

ตัวอย่าง Source code ของเว็บเซอร์วิสเป็นการเรียกใช้ Library Slim PHP Framework

ทำการตรวจสอบ clientkey ว่าถูกต้องตรงกันหรือไม่ ถ้าถูกต้อง จะนำข้อมูลส่งเข้าไปในตัวแปร JSON เพื่อตอบกลับให้กับไคลเอนต์ผู้ร้องขอข้อมูล

```
<?php
ini_set("display_errors",1);
//เรียกใช้ Slim Framework
require '../Slim/Slim.php';
//เรียกใช้ค่าตัวแปรการเชื่อมต่อ ฐานข้อมูล
require '../Connections/conn.php';
Slim\Slim::registerAutoloader();
use Slim\Slim;
use Slim\View\Twig as TwigView;
$app = new Slim();
//ลงทะเบียน getEPIs   Service
$app->get('/pcucode/getEPIs', 'getEPIs');

//ลงทะเบียน getEPI Service
$app->get('/pcucode/getEPI/:pcucode/:securekey/:startdate/:enddate', 'getEPI');

//ลงทะเบียน addepi  Service
$app->post('/addepi', 'addepi');

//ลงทะเบียน updateepi  Service
$app->post('/updateepi', 'updateepi');

//ลงทะเบียน deleteepi  Service
$app->delete('/deleteepi/:clientkey/:pcucode/:pid/:date_serv/:vcctype', 'deleteepi');
//ลงทะเบียน searchepi  Service
$app->get('/searchepi/:clientkey/:pcucode/:pid', 'searchBypid');
//เริ่มต้นการทำงาน Rest Service ที่ลงทะเบียนไว้
$app->run();
```

ภาพที่ จ-1 ตัวอย่าง Source code ของเว็บเซอร์วิส

ฟังก์ชันเชื่อมต่อฐานข้อมูล

```
//ฟังก์ชันเชื่อมต่อฐานข้อมูล
function conn() {
   $db_conn = new PDO(
              'mysql:host=$hostname_conn;dbname=$database_conn',
              $username_conn,
              $password_conn);
   return $db_conn;  }
```

ภาพที่ จ-2 ตัวอย่าง Source code ฟังก์ชันเชื่อมต่อฐานข้อมูลของเว็บเซอร์วิส

ฟังก์ชัน Rest ดึงข้อมูล โดยรับค่า http request จาก client

```
//ฟังก์ชัน Rest ดึงข้อมูล  โดยรับค่า request จาก client
function getEPI($pcucode,$securekey,$startdate,$enddate){
if($securekey=="********************************")      {
$strSQL = "select *  from epi where
            cid IN (select cid from person where pcucode= :pcucode ) and pcucode != :pcucode
            and date_serv between :startdate and :enddate  ";
            and pcucode in(select off_id from webservice_config where syncAllow='1' )
             $db_conn = conn();
            $sql = 'SELECT * FROM epi  WHERE pcucode= :pcucode and date_serv between :startdate
and :enddate ORDER BY pcucode';
            $record = $db_conn->prepare($strSQL );
            $pp = array(':pcucode' => $pcucode,':startdate' => $startdate,':enddate' => $enddate);
            $row = $record->execute($pp);
            $rs = $record->fetchAll(PDO::FETCH_ASSOC);        }
else
{
            $rs[]= array("statusid" => "0","status" => "Invalid Clientkey", "pcucode" => $pcucode );
}
echo   json_encode($rs);
}
```

ภาพที่ จ-3 ตัวอย่าง Source code ฟังก์ชัน Rest ดึงข้อมูล ของเว็บเซอร์วิส

ฟังก์ชัน Rest เพิ่มข้อมูล โดยรับค่า http request จาก client

```
//ฟังก์ชัน Rest เพิ่มข้อมูล  โดยรับค่า request จาก client
function addepi() {
   $db_conn = conn();
   $return_a = array();
   $app_r = Slim::getInstance()->request();
 $securekey= $app_r->post('clientkey');
if($securekey=="**********")
  {
   $pcucode = $app_r->post('pcucode');
   $pid = $app_r->post('pid');
   $date_serv = $app_r->post('date_serv');
   $vcctype = $app_r->post('vcctype');
   $vccplace = $app_r->post('vccplace');
   $d_update = date('Ymdhis');
   $sql_st = "INSERT INTO epi(pcucode,pid,date_serv,vcctype,vccplace,d_update)
VALUES(?,?,?,?,?,?)";
   $sql = $db_conn->prepare($sql_st);
   if ($sql->execute(array($pcucode,$pid,$date_serv,$vcctype,$vccplace,$d_update))) {
      $return_a = array('status'=>'1','add'=>'Insert Epi Record Complete','id' => $db_conn-
>lastInsertId());
   } else {
      $return_a = array('status'=>'0','add' => 'failed');
   }
}
else
{
      $return_a = array('status'=>'0','add' => 'failed','error' => 'Invalid Clientkey');
}
   echo json_encode($return_a);
}
```

ภาพที่ จ-4 ตัวอย่าง Source code ฟังก์ชัน Rest เพิ่มข้อมูล ของเว็บเซอร์วิส

ฟังก์ชัน Rest ปรับปรุงข้อมูล โดยรับค่า http request จาก client

```
//ฟังก์ชัน Rest ปรับปรุงข้อมูล  โดยรับค่า request จาก client
function updateepi() {
        $db_conn = conn();
        $app_r = Slim::getInstance()->request();
         $securekey= $app_r->post('clientkey');
if($securekey=="**********")
  {
  $pcucode = $app_r->post('pcucode');
  $pid = $app_r->post('pid');
  $seq = $app_r->post('seq');
  $vcctype = $app_r->post('vcctype');
  $vccplace = $app_r->post('vccplace');
  $d_update = date('Ymdhis');
  $date_serv_n = $app_r->post('date_serv_n');
  $vcctype_n = $app_r->post('vcctype_n');
  $vccplace_n = $app_r->post('vccplace_n');
 $sql_st = 'Update epi
        set d_update=:d_update,
        date_serv=:date_serv_n,
        vcctype=:vcctype_n,
        vccplace=:vccplace_n
        WHERE        pcucode=:pcucode and
                pid=:pid and
                seq=:seq ';
  $update_array = array(
                        'date_serv_n' => $date_serv_n,
                        'vcctype_n' => $vcctype_n,
                        'vccplace_n' => $vccplace_n,
                        'd_update' => $d_update,
```

```
                    'pcucode' => $pcucode,
                    'pid' => $pid,
                    'seq' => $seq,
                    );

  $sql = $db_conn->prepare($sql_st);
  if ($sql->execute($update_array)) {
        $update_array = array('update' => 'Update Complete') ;//,'sql'=>$sql_st
,'array'=>$update_array );
        }
        }
else
        {
        $update_array = array('update' => $sql_st,'error' => 'Invalid Clientkey');
        }
  echo json_encode($update_array);
}
```

ภาพที่ จ-5 ตัวอย่าง Source code ฟังก์ชัน Rest ปรับปรุงข้อมูล ของเว็บเซอร์วิส

ฟังก์ชัน Rest ลบข้อมูล โดยรับค่า http request จาก client

```
//ฟังก์ชัน Rest ลบข้อมูล  โดยรับค่า request จาก client
function deleteepi($clientkey,$pcucode,$pid,$date_serv,$vcctype) {
if($securekey=="********************************")
  {          $db_conn = conn();
             $sql_st = 'DELETE FROM epi WHERE pcucode=?
                    and pid=? and date_serv=? and vcctype=?';
   $sql = $db_conn->prepare($sql_st);
   if ($sql->execute(array($pcucode,$pid,$date_serv,$vcctype))) {
$aa = array('delete' => 'Complete && success');}}
else{       $aa = array('delete' => 'Error Invalid Clientkey');}
      echo json_encode($aa); }
```

ภาพที่ จ-6 ตัวอย่าง Source code ฟังก์ชัน Rest ลบข้อมูล ของเว็บเซอร์วิส

ฟังก์ชัน Rest ค้นหาข้อมูล โดยรับค่า http request จาก client

```
//ฟังก์ชัน Rest ค้นหาข้อมูล  โดยรับค่า request จาก client
function searchBypid($clientkey,$pcucode,$pid)
{
if($securekey=="********************************")
  {
  $db_conn = conn();
   $sql = 'SELECT pcucode,pid,seq,date_serv,vcctype,vccplace FROM epi WHERE pcucode
=:pcucode and pid =:pid  ORDER BY date_serv desc';
   $record = $db_conn->prepare($sql);
   $aa_search = array(':pcucode' => $pcucode,':pid' => $pid);
   $row = $record->execute($aa_search);
   if (!$row) {
      $rs = array('error' => 'connection');
   } else {
```

```
        $rs = $record->fetchAll(PDO::FETCH_ASSOC);
    }
}
else
{
        $rs = array('search' => 'Error Invalid Clientkey');
}
  echo json_encode($rs);
}
?>
```

ภาพที่ จ-7 ตัวอย่าง Source code ฟังก์ชัน Rest ค้นหาข้อมูล ของเว็บเซอร์วิส

โปรแกรม getEPI รับข้อมูลจาก Operation getEPI ของเว็บเซอร์วิสเซิร์ฟเวอร์

```
public  void getData()  throws ClassNotFoundException, MalformedURLException, IOException,
JSONException, SQLException
 {
              URL u;
        InputStream is = null;
        DataInputStream dis;
try {
    String StrUrl =
"https://healthws.ntwo.moph.go.th/serviceapi/epiinfo.php/pcucode/getEPI/"+jhcisconfig.offid+"/"+jhci
sconfig.clientkey+"/"+Sdate+"/"+Edate;
              SocketFactory factory = SSLSocketFactory.getDefault();    u = new URL(StrUrl);
              is = u.openStream();
              forme.startDate.getDate().getDateFormat().format(dateFormat).toString();
               StringBuilder   str = new StringBuilder();
            String line = null;
```

โปรแกรม getEPI รับข้อมูลจาก Operation getEPI ของเว็บเซอร์วิสเซิร์ฟเวอร์ (ต่อ)

```
            dis = new DataInputStream(new BufferedInputStream(is));
        BufferedReader reader = new BufferedReader(new InputStreamReader(dis));
        while ((line = reader.readLine()) != null)
            str.append(line);
            reader.close();
          JSONArray dataJson = new JSONArray(str.toString());
          ArrayList<HashMap<String, String>> myArrList = new ArrayList<HashMap<String,
       String>>();
          HashMap<String, String> map;
           for(int i = 0; i < dataJson.length(); i++){
            JSONObject c = dataJson.getJSONObject(i);
            map = new HashMap<String, String>();
            map.put("pcucode", c.getString("pcucode"));
            map.put("pid", c.getString("pid"));
            map.put("date_serv", c.getString("date_serv"));
            map.put("vcctype", c.getString("vcctype"));
            map.put("vccplace", c.getString("vccplace"));
            myArrList.add(map);
          }
          for (int i = 0; i < myArrList.size(); i++) {
            int num_rows = myArrList.size();
             setAllrec(num_rows);
       String provispcucode = myArrList.get(i).get("pcucode");
            String provispid = myArrList.get(i).get("pid");
            String proviscid = myArrList.get(i).get("cid");
            String provisdate_serv = myArrList.get(i).get("date_serv");
            String provisvcctype = myArrList.get(i).get("vcctype");
            String provisvccplace = myArrList.get(i).get("vccplace");
        setOffid(provispcucode);
```

โปรแกรม getEPI รับข้อมูลจาก Operation getEPI ของเว็บเซอร์วิสเซิร์ฟเวอร์ (ต่อ)

```
            if("is".equals(status))
                {
                System.out.println("Error Securekey");
                System.exit(0);
            }rs=st.executeQuery(str);
Vector <String> d=new Vector<String>();
        d.add(myArrList.get(i).get("pcucode"));
        d.add(myArrList.get(i).get("pid"));
        d.add(myArrList.get(i).get("date_serv"));
        d.add(myArrList.get(i).get("vcctype"));
        d.add(myArrList.get(i).get("vccplace"));
        d.add("\n\n\n\n\n\n\n");
        data.add(d);
if(provispcucode=="99x99")
{
forme.TxtStatus.setText("pcucode :"+jhcisconfig.offid+"ไม่ได้รับอนุญาตแลกเปลี่ยน
ข้อมูล");
for (Thread t : Thread.getAllStackTraces().keySet())
if (t.getState()==Thread.State.RUNNABLE)
    t.stop();
}
int Pr = (100*(i/Allrec));
forme.Bar2.setMaximum(Allrec);
addEpi(provispcucode,
proviscid ,
provisdate_serv,
provisvcctype,
provisvccplace);
forme.TxtStatus.setText("");
```

โปรแกรม getEPI รับข้อมูลจาก Operation getEPI ของเว็บเซอร์วิสเซิร์ฟเวอร์ (ต่อ)

```
forme.TxtStatus.setText("Sync ID :"+i+"/"+(Allrec) + "( เลขบัตรประชาชน : "+proviscid
+")");
forme.TxtStatus.repaint();
Object[][] rowData = {{provispcucode, proviscid,
provisdate_serv,provisvcctype,provisvccplace}};
model.addRow(new Object[]{provispcucode, proviscid,
provisdate_serv,provisvcctype,provisvccplace});
forme.jTable1.scrollRectToVisible(forme.jTable1.getCellRect(forme.jTable1.getRowCou
nt()-1, 0, true));
 forme.Bar2.setValue(i);
   }
}
catch (IOException | JSONException e)
{   forme.TxtStatus.setForeground(Color.red);
   forme.TxtStatus.setText("ไม่สามารถติดต่อ web service ได้ โปรดตรวจสอบการ
เชื่อมต่อ Internet");
JOptionPane.showMessageDialog(null, "ไม่สามารถติดต่อ web service ได้ \n โปรด
ตรวจสอบการเชื่อมต่อ Internet", "Connection Error",
                        JOptionPane.ERROR_MESSAGE);
   System.out.println("ไม่สามารถติดต่อ web service ได้");
   System.exit(-1);
 e.printStackTrace();
}
}
```

ภาพที่ จ-8 โปรแกรมรับข้อมูลจาก getEPI Operation ของเว็บเซอร์วิสไคลเอนต์

ภาคผนวก ฉ

รายชื่อบุคลากรสาธารณสุขที่ทำการทดสอบระบบ Healthws System

รายชื่อบุคลากรสาธารณสุขที่ทำการทดสอบระบบ Healthws System

1. การทดสอบด้านการรักษาความลับ

1.1 ทดสอบระบบ Healthws-Client

1. นางสาวจิลาวรรณ เพ็ชรรัตน์ โรงพยาบาลส่งเสริมสุขภาพตำบลสอวอนอก
2. นางจันทร์ยา จันทร์คง โรงพยาบาลส่งเสริมสุขภาพตำบลพร่อน
3. นายเชาวลิต ภู่ทับทิม โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
4. นายซำสุดิน หามะ โรงพยาบาลส่งเสริมสุขภาพตำบลโคกสะตอ
5. นางผจงพร ทองเชื้อ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลมะรือโบออก
6. นายมะรอซา กูโน โรงพยาบาลส่งเสริมสุขภาพตำบลลาไม
7. นางสาวสาลินี จงเจตดี โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลปาเสมัส
8. นายอยุทธ มือเสาะ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลตะปอเยาะ
9. นายสุสนัน เจ๊ะอารง โรงพยาบาลส่งเสริมสุขภาพตำบลสากอ

1.2 ทดสอบเว็บเซอร์วิสเซิร์ฟเวอร์

1. นางสาวจิลาวรรณ เพ็ชรรัตน์ โรงพยาบาลส่งเสริมสุขภาพตำบลสอวอนอก
2. นางจันทร์ยา จันทร์คง โรงพยาบาลส่งเสริมสุขภาพตำบลพร่อน
3. นายเชาวลิต ภู่ทับทิม โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
4. นายซำสุดิน หามะ โรงพยาบาลส่งเสริมสุขภาพตำบลโคกสะตอ
5. นางประจิกศักดิ์ เพชรช่วย โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลลุโบะสาวอ

2. การทดสอบด้านการคงสภาพของข้อมูล

2.1 การทดสอบด้านความถูกต้อง

1. นางสาวจิลาวรรณ เพ็ชรรัตน์ โรงพยาบาลส่งเสริมสุขภาพตำบลสอวอนอก
2. นางจันทร์ยา จันทร์คง โรงพยาบาลส่งเสริมสุขภาพตำบลพร่อน
3. นายเชาวลิต ภู่ทับทิม โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
4. นายซำสุดิน หามะ โรงพยาบาลส่งเสริมสุขภาพตำบลโคกสะตอ
5. นางผจงพร ทองเชื้อ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลมะรือโบออก
6. นายมะรอซา กูโน โรงพยาบาลส่งเสริมสุขภาพตำบลลาไม
7. นางสาวสาลินี จงเจตดี โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลปาเสมัส
8. นายอยุทธ มือเสาะ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลตะปอเยาะ
9. นายเชาวลิต ภู่ทับทิม โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
10. นายฮุสนัน เจ๊ะอารง โรงพยาบาลส่งเสริมสุขภาพตำบลสากอ

2.2 การทดสอบความครบถ้วนของข้อมูล

1. นางสาวจิลาวรรณ เพ็ชรรัตน์ โรงพยาบาลส่งเสริมสุขภาพตำบลสอวอนอก
2. นางจันทร์ยา จันทร์คง โรงพยาบาลส่งเสริมสุขภาพตำบลพร่อน
3. นายเชาวลิต ภู่ทับทิม โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
4. นายซำสุดิน หามะ โรงพยาบาลส่งเสริมสุขภาพตำบลโคกสะตอ
5. นางประจิกศักดิ์ เพชรช่วย โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลลุโบะสาวอ
6. นางผจงพร ทองเชื้อ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลมะรือโบออก
7. นายมะรอซา กูโน โรงพยาบาลส่งเสริมสุขภาพตำบลลาไม
8. นายมูฮัมมัดตารมีซี สาแม โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลริโก๋
9. นางสาวสาลินี จงเจตดี โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลปาเสมัส
10. นายสุวัฒน์ ทองเล็ก โรงพยาบาลส่งเสริมสุขภาพตำบลไม้ฝาด
11. นางอุไร พจน์เพริศ โรงพยาบาลส่งเสริมสุขภาพตำบลยี่งอ
12. นายแอมะ มะเซ็ง โรงพยาบาลส่งเสริมสุขภาพตำบลตะโละแน็ง
13. นายฮุสนัน เจ๊ะอารง โรงพยาบาลส่งเสริมสุขภาพตำบลสากอ
14. นายอยุทธ มือเสาะ โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลตะปอเยาะ

3. การทดสอบด้านความพร้อมใช้งาน

1.	นางสาวจิลาวรรณ เพ็ชรรัตน์	โรงพยาบาลส่งเสริมสุขภาพตำบลสอวอนอก
2.	นางจันทร์ยา จันทร์คง	โรงพยาบาลส่งเสริมสุขภาพตำบลพร่อน
3.	นายเชาวลิต ภู่ทับทิม	โรงพยาบาลส่งเสริมสุขภาพตำบลกูมุง
4.	นายซำสุดิน หามะ	โรงพยาบาลส่งเสริมสุขภาพตำบลโคกสะตอ
5.	นางประจิกศักดิ์ เพชรช่วย	โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลลุโบะสาวอ
6.	นางผจงพร ทองเชื้อ	โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลมะรือโบออก
7.	นายมะรอซา กูโน	โรงพยาบาลส่งเสริมสุขภาพตำบลลาไม
8.	นายมูฮัมมัดตัรมีซี สาแม	โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลริโก๋
9.	นางสาวสาลินี จงเจตดี	โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลปาเสมัส
10.	นายอยุทธ มือเสาะ	โรงพยาบาลส่งเสริมสุขภาพตำบลตำบลตะปอเยาะ

4. การประเมินตามข้อกำหนด NIST SP 800-44

1.	นายมะนาเซ อาแวเตะ	สำนักงานสาธารณสุขจังหวัดนราธิวาส

บรรณานุกรม

บรรณานุกรม

กานดา รุณนะพงศา และคณะ. (2557). “แนวทางในการทดสอบฟังก์ชั่นการทำงานของเว็บเซอร์วิสแบบ 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.* กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.

ชฎาวัลย์ สิงห์อินทร์. (2550). “การพิสูจน์ตัวตน หนทางสู่ความปลอดภัยของข้อมูล” ออนไลน์. สืบค้นจาก :http://www.ictc.ago.go.th/it53/safety_data.pdf [20 กรกฎาคม 2557].

ชาลี ธรรมรัตน์. (2554). “ความมั่นคงปลอดภัยการรับส่งแฟ้มข้อมูลและการจัดการการเข้ารหัสลับภายในองค์กร” สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร.

เดชาวัต นิชาญานันท์. (2555). *การจัดทำนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร กรณีศึกษาสำหรับบริษัท สินแพทย์ จำกัด (โรงพยาบาลสินแพทย์)* (สารนิพนธ์ปริญญาวิทยาศาสตรหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร. กรุงเทพฯ.

บุญฤทธิ์ คิดหงัน. (2554). “ความมั่นคงปลอดภัยของสารสนเทศ” ออนไลน์. สืบค้นจาก : http://sci.feu.ac.th/boonrit/security/ch1%20information%20security%20and%20management.ppt [28 มิถุนายน 2557].

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

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

“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.

มหาวิทยาลัยกรุงเทพ. (2554). “ความมั่นคงในระบบสารสนเทศและการควบคุม” ออนไลน์. สืบค้นจาก : https://docs.google.com/presentation/d/1JHNVI2RIWBKgVHZ8hanMNPn01gxxjV2NwrkkHuMlPo0/embed?hl=en&size=m&slide=id.p [30 มิถุนายน 2557].

วิจิตรา โกมาสถตย์. (2556). “OSI โมเดล” ออนไลน์. สืบค้นจาก : http://vijitrahvan.blogspot.com/2013/09/4- osi.html [30 มิถุนายน 2557].

ศราวุฒิ จันทะคัด. (2554). *การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา : บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด* (สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2555). “Cyber Security Articles 2012” ออนไลน์. สืบค้นจาก : https://www.thaicert.or.th/downloads/files/Cyber_Security_Articles_2012.pdf [1 กรกฎาคม 2557].

สิทธิศักดิ์ สายเงิน. (2556). “การรักษาความปลอดภัยในการให้บริการผ่านเว็บ” ใน*เอกสารการสอนชุดวิชา เทคโนโลยีการให้บริการผ่านเว็บและการประยุกต์* หน่วยที่ 11 หน้า 11-21, 11-24 นนทบุรี มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชาวิทยาศาสตร์และเทคโนโลยี.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2557). “เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI)” ออนไลน์. สืบค้นจาก : http://www.nrca.go.th/ [30 มิถุนายน 2557].

สำนักนโยบายและยุทธศาสตร์. (2556). “โครงสร้างฐานข้อมูลการให้บริการผู้ป่วยนอก การสร้างเสริมสุขภาพ และป้องกันโรคในรูปแบบ 21 แฟ้มมาตรฐาน ปีงบประมาณ 2556” ออนไลน์. สืบค้นจาก : http://healthcaredata.moph.go.th/main/wp-content/uploads/2012/04/structur-21-%E0%B9%81%E0%B8%9F%E0%B9%89%E0%B8%A1-%E0%B8%9B%E0%B8%B5-56.zip [30 มิถุนายน 2557].

สำนักนโยบายและยุทธศาสตร์. (2556)ใ “2 โครงสร้างมาตรฐานข้อมูลด้านการแพทย์และสุขภาพและการส่งต่อผู้ป่วย version 1.0 วันที่ 16 มี.ค. 2555” ออนไลน์. สืบค้นจาก : http://healthcaredata.moph.go.th/main/wp-ontent/uploads/2012/04/final_43_file_27122555.zip [30 มิถุนายน 2557].

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.

ประวัติผู้วิจัย

ชื่อ	นายจรูญศักดิ์ เวทมาหะ
วัน เดือน ปีเกิด	23 พฤษภาคม 2509
สถานที่เกิด	อำเภอสุไหงปาดี จังหวัดนราธิวาส
ประวัติการศึกษา	ปริญญาตรีเทคโนโลยีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศธุรกิจ มหาวิทยาลัยสุโขทัยธรรมาธิราช ปีการศึกษา 2551
สถานที่ทำงาน	กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข สำนักงานสาธารณสุขจังหวัดนราธิวาส อำเภอเมือง จังหวัดนราธิวาส
ตำแหน่ง	นักวิชาการสาธารณสุข ระดับชำนาญการ