Privame

ระบบควบคุมการเข้าถึงเวชระเบียนระหว่างโรงพยาบาลด้วยนโยบายความเป็นส่วนตัว

รหัสโครงการ : 23p15w0024

เสนอต่อ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์และเทคโนโลยี

ทีมพัฒนาโครงการ :

นางสาวชิดชนก	บรรจงเพียร	(หัวหน้าโครงการ)
นางสาวอริสา	ดลสุขเลิศ	(ผู้ร่วมพัฒนา)
นายจิรพัส	ธรรมสงเคราะห์	(ผู้ร่วมพัฒนา)

อาจารย์ที่ปรึกษาโครงการ :

ดร. อิทธิพล รัศมีโรจน์

หัวหน้าสถาบัน :

ดร. พัฒนศักดิ์ มงคลวัฒน์ (คณบดี)

คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

สารบัญ

สาระสำคัญของโครงการ (Keywords)

(ภาษาไทย) การรักษาความเป็นส่วนตัว, การกำหนดสิทธิ์การเข้าถึงข้อมูลด้านสุขภาพ

(ภาษาอังกฤษ) Privacy-preserving, Health Information Network

ข้อมูลและประวัติการรักษาของผู้ป่วยภายในโรงพยาบาลถือเป็นข้อมูลที่มีความสำคัญและละเอียดอ่อนสูง ซึ่งข้อมูลเหล่านี้มีความจำเป็นอย่างมากในการรักษาของแพทย์และถือเป็นข้อมูลสำคัญทางกฎหมายดังนั้น การยืนยันตัวตนบนระบบเครือข่าย การจำกัดสิทธิ์ในการเข้าถึงข้อมูลระหว่างโรงพยาบาล จึงเป็นสิ่งสำคัญที่ต้องใช้ความระมัดระวังเป็นอย่างสูงเพื่อรักษาความปลอดภัยของข้อมูลและเพื่อการรักษาความเป็นส่วนตัวของเจ้าของข้อมูล ในโครงการนี้ทางทีมพัฒนาจึงมุ่งเน้นถึงการรักษาความปลอดภัยของข้อมูลและการกำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ป่วยตามหลัก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

หลักการและเหตุผล

เนื่องด้วยเทคโนโลยีที่ก้าวหน้าขึ้น ช่องทางสื่อสารต่าง ๆ จึงมีหลากหลายขึ้น ซึ่งทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลทำได้ง่ายขึ้นและนำมาซึ่งความเดือดร้อนหรือสร้างความเสียหายให้แก่เจ้าของข้อมูล บันทึกเวชระเบียนคือบันทึกที่เก็บข้อมูลและประวัติการรักษา ประวัติโรคประจำตัวและโรคปัจจุบัน ไปจนถึงประวัติครอบครัว ถือเป็นข้อมูลที่สำคัญทางการแพทย์ในการรักษาพยาบาล รวมทั้งเป็นข้อมูลสำคัญทางกฎหมายเช่นเดียวกัน ในหลาย ๆ โรงพยาบาลในปัจจุบัน ผู้ป่วยไม่มีสิทธิ์ในการเข้าข้อมูลเหล่านี้ แต่บุคลากรทางการแพทย์สามารถเข้าถึงระบบและเรียกดูข้อมูลของเหล่านี้ได้เกือบทั้งหมด แม้ว่าจะไม่ได้รับความยินยอมจากผู้ป่วยก็ตาม นอกจากนี้ผู้ป่วยหนึ่งคนอาจไม่ได้เข้ารับการรักษาจากเพียงโรงพยาบาลเดียว ทำให้ข้อมูลการรักษานั้น กระจัดกระจาย เป็นเหตุให้ผู้ป่วยและบุคลากรต้องเก็บรวบรวมข้อมูลนั้นแยกกันในแต่ละโรงพยาบาล หรือต้องเดินทางด้วยตนเองเพื่อนำเอกสารข้อมูลจากโรงพยาบาลหนึ่งไปส่งยังโรงพยาบาลอีกแห่งหนึ่ง

จากปัญหาข้างต้น ทางทีมพัฒนาจึงมีความประสงค์ที่จะพัฒนาระบบยืนยันตัวตน (Authentication System) และกำหนดสิทธิ์การเข้าถึงเวชระเบียนของผู้ป่วย (Authorization) เพื่อความสะดวก ปลอดภัย และเรียบง่ายในการเข้าถึงข้อมูลของผู้ป่วยนั้น ๆ ตามหลัก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

โครงการระบบควบคุมการเข้าถึงเวชระเบียนระหว่างโรงพยาบาลด้วยนโยบายความเป็นส่วนตัวนี้ มีวัตถุประสงค์เพื่อเป็นเป้าหมายในการศึกษา พัฒนาและวิจัยโดยจะให้ความรู้ทางด้านเทคโนโลยีสารสนเทศ มาช่วยเหลือในด้านการแพทย์ และประยุกต์ใช้ในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการกำหนดสิทธิ์การเข้าถึง

ข้อมูลส่วนบุคคล (Authorization) ในการช่วยเหลือผู้ป่วยและอำนวยความสะดวกแก่บุคลากรทางการแพทย์ โดยที่ผู้ใช้ไม่จำเป็นต้องมีความรู้ ความชำนาญในด้านซอฟต์แวร์มากนัก

วัตถุประสงค์

1. เพื่อให้ผู้ป่วยสามารถเข้าถึงข้อมูลเวชระเบียนอิเล็กทรอนิกส์ของตนเองผ่านเครือข่ายอินเทอร์เน็ต
2. เพื่อให้ผู้ป่วยสามารถกำหนดสิทธิ์ในการเข้าถึงข้อมูลเวชระเบียนของตนเองให้กับบุคลากรทางการแพทย์ระหว่างโรงพยาบาลได้
3. เพื่อเพิ่มทางเลือกและสร้างความคุ้นเคย ในการตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล และพัฒนาเทคโนโลยีให้มีมาตรฐานที่สูงขึ้นในการกำกับดูแลคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการเก็บรวบรวม การใช้งาน และการเปิดเผยข้อมูลส่วนบุคคล

ปัญหาหรือประโยชน์ที่เป็นเหตุผลควรให้พัฒนาโปรแกรม

การจัดการข้อมูลด้านเวชระเบียนของผู้ป่วยภายในโรงพยาบาลให้สอดคล้องตามหลักกฎหมายการคุ้มครองข้อมูลส่วนบุคคล เช่น Genral Data Protection Regulation (GDPR) หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) นั้นทำได้ค่อนข้างยากเนื่องจากผู้ป่วยไม่สามารถเข้าถึงข้อมูลส่วนบุคคลในการรักษาพยาบาลของตนเอง และไม่สามารถกำหนดสิทธิ์ให้กับผู้ที่เข้าถึงข้อมูลได้ แต่บุคลากรในโรงพยาบาลสามารถเข้าถึงข้อมูลของผู้ป่วยได้ทุกคน นอกจากนี้หากผู้ป่วยต้องการเอกสารเกี่ยวกับการรักษา จะต้องขอเอกสารและประวัติการรักษาโดยตรงจากทางโรงพยาบาล และไม่มีทางรู้ได้เลยว่าบุคคลใดบ้างที่สามารถเข้าถึงข้อมูลของผู้ป่วยได้ การเก็บรักษาข้อมูลนั้นมีความเป็นส่วนตัวมากน้อยแค่ไหน

ขณะเดียวกันในหลาย ๆ โรงพยาบาลได้พัฒนาระบบจัดการบัญชีผู้ป่วย (Account Management) เพื่อให้ผู้ป่วยสามารถเข้าล็อกอินและเข้าถึงเวชระเบียนของตนเองได้ แต่ผู้ป่วยหนึ่งคนอาจจะรักษามากกว่าหนึ่งโรงพยาบาล แต่ละโรงพยาบาลมีระบบจัดการบัญชีผู้ป่วยและระบบยืนยันตัวตนเป็นของตัวเอง ดังนั้นผู้ป่วยอาจจะเกิดความยุ่งยากและซับซ้อนหากต้องมีความจำเป็นต้องใช้บริการและเข้าถึงเวชระเบียนของตนเองในหลาย ๆ โรงพยาบาล นอกจากนี้บุคลากรทางการแพทย์ต่างโรงพยาบาลก็สามารถเข้าถึงข้อมูลเวชระเบียนของโรงพยาบาลตนเองเท่านั้น

ด้วยเหตุนี้ ทางทีมพัฒนาจึงเล็งเห็นปัญหาดังกล่าว และคำนึงถึงแนวทางการแก้ไขปัญหาโดยใช้ระบบคอมพิวเตอร์เข้ามาช่วย ซึ่งจะนำระบบยืนยันตัวตน (Authentication System) เข้าร่วมกับซอฟต์แวร์ที่ทางโรงพยาบาลใช้อยู่ในปัจจุบัน เพื่อช่วยให้ผู้ป่วยสามารถดึงข้อมูลเวชระเบียนของผู้ป่วยจากโรงพยาบาลที่เคย

รักษาได้ โดยที่ผู้ป่วยไม่จำเป็นต้องเดินทางไปยังโรงพยาบาลที่เคยรักษาเพื่อนำข้อมูลไปส่งให้โรงพยาบาลที่ผู้ป่วยกำลังรักษาอยู่ ณ ปัจจุบัน เพื่อให้สอดคล้องตาม สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to Data Portability) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยส่งผลกระทบให้น้อยที่สุดต่อระบบดั้งเดิมของทางโรงพยาบาล (Existing Systems)

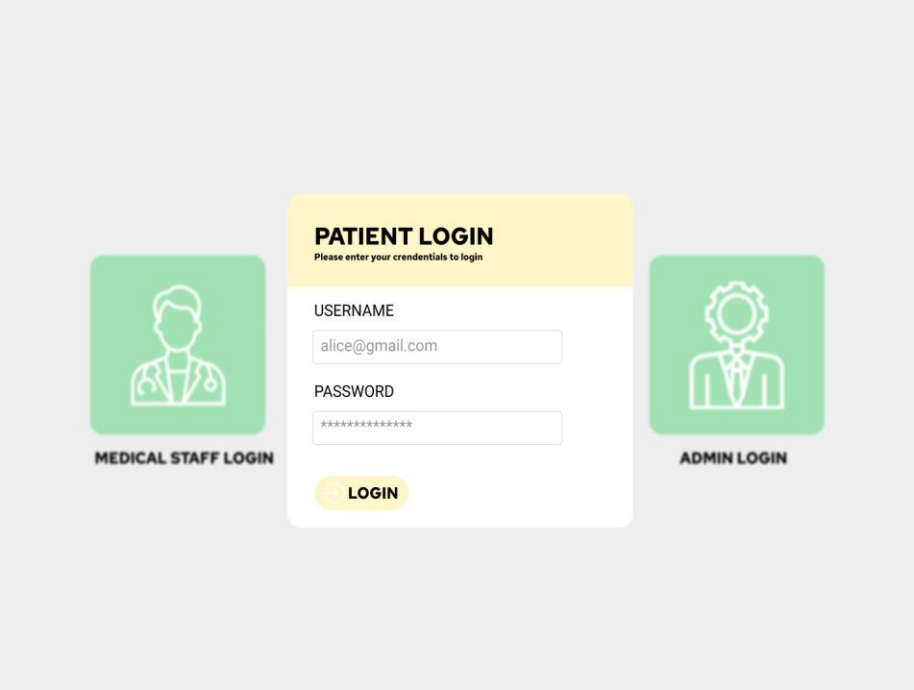
เป้าหมายและขอบเขตของโครงการ

1. มีระบบยืนยันตัวตน (Authentication System) และกำหนดสิทธิ์ (Authorization) ในการเข้าถึงข้อมูลของผู้ป่วย ตามหลัก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)
2. บุคลากรทางการแพทย์สามารถเข้าถึงข้อมูลของผู้ป่วยจากอีกโรงพยาบาลได้อย่างสะดวกและปลอดภัย ภายใต้การอนุญาตของผู้ป่วยเจ้าของข้อมูล (Right to Object)
3. ระบบของโรงพยาบาลจะต้องใช้ฐานข้อมูลประเภท SQL
4. โดยเบื้องต้นมีความประสงค์จะนำไปใช้กับโรงพยาบาลบ้านแพร้ว โรงพยาบาลนครปฐม และโรงพยาบาลสามพราน
5. การเปลี่ยนแปลงกับระบบของโรงพยาบาลจะต้องเกิดขึ้นเพียงเล็กน้อยหรือไม่มีการเปลี่ยนแปลงเลย

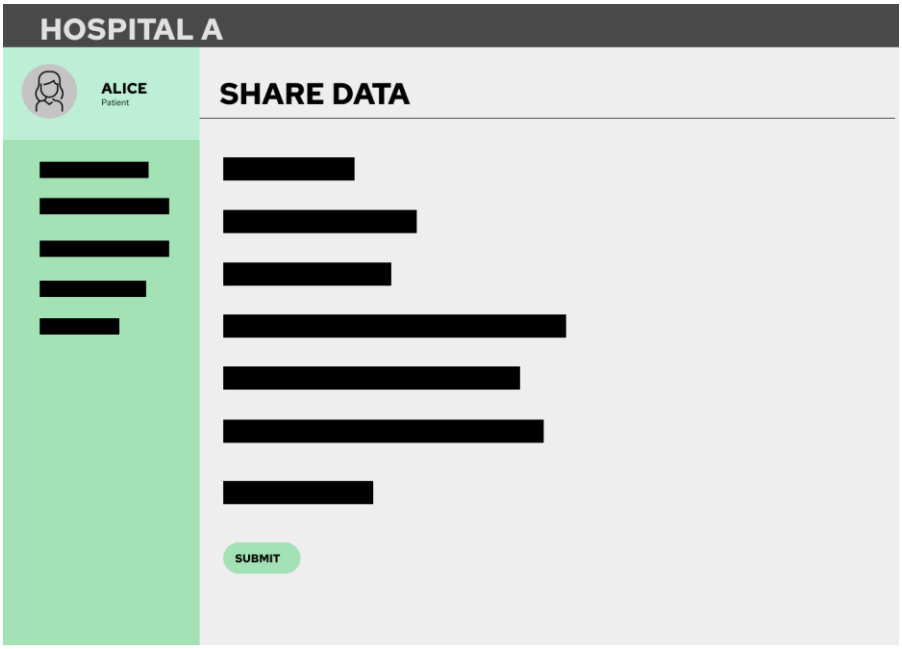
รายละเอียดการพัฒนา

1. **ภาพประกอบ แบบจำลอง และทฤษฎีที่เกี่ยวข้อง**
    - หน้าแรกของเว็บไซต์

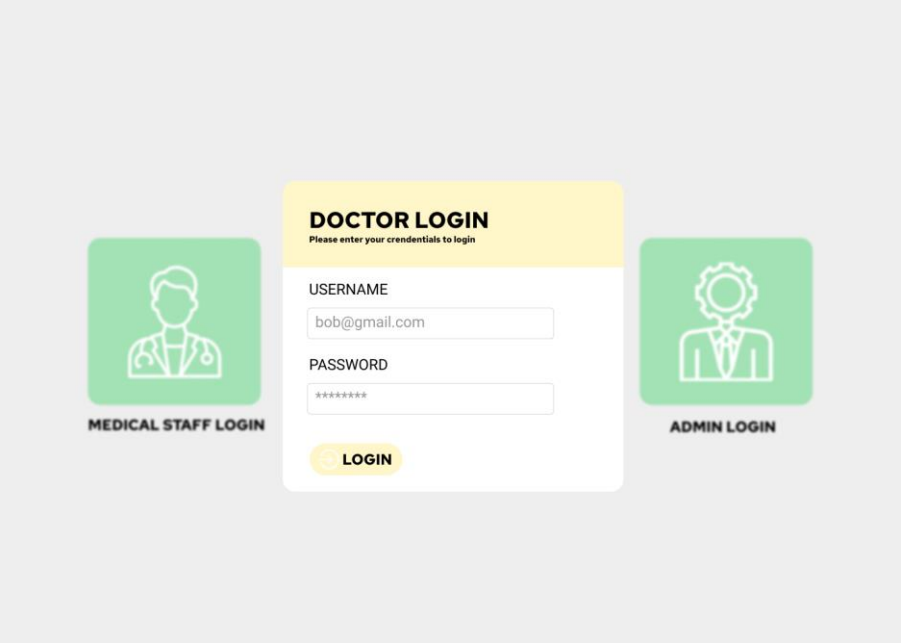
- หน้าเข้าใช้ระบบของผู้ป่วย



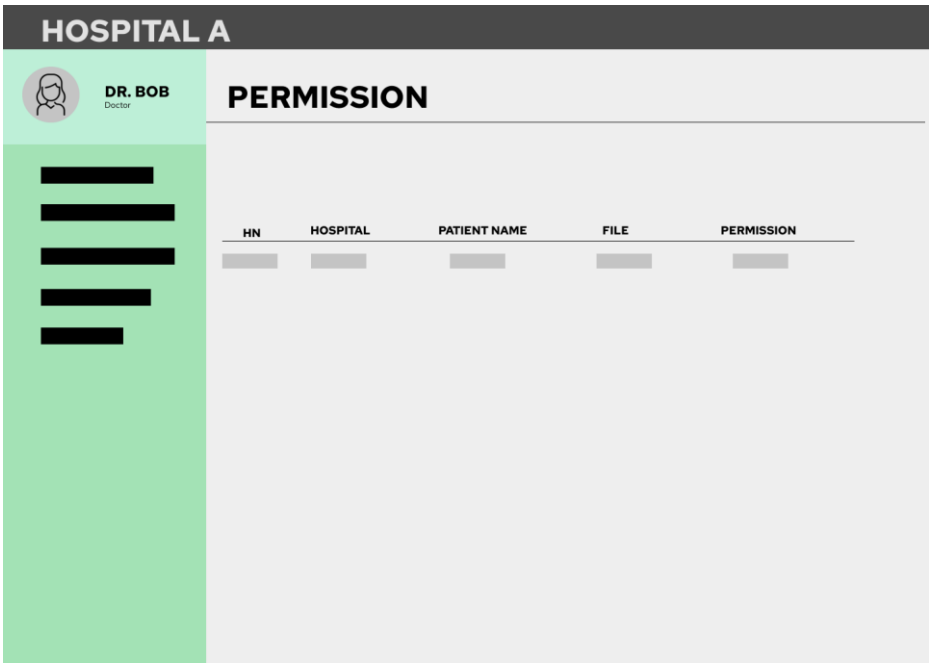
- หน้ามอบสิทธิ์ให้บุคลากรทางการแพทย์เข้าถึงข้อมูล



- หน้าเข้าใช้ระบบของบุคลากรทางการแพทย์



- หน้าดูสิทธิ์ที่บุคลากรทางการแพทย์มีสิทธิ์ดูประวัติการรักษาของผู้ป่วย



2. เทคนิคหรือเทคโนโลยีที่ใช้

a. การยืนยันตัวตนบนระบบเครือข่าย (Authentication System)

เป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่ใช้งานระบบเครือข่าย เพื่อพิสูจน์ตัวบุคคลว่าเป็นบุคคลผู้มีสิทธิ์เข้าใช้งาน

b. การจัดการข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data Managament)

การวางโครงสร้างและจัดการระบบเพื่อปกป้องข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

3. เครื่องมือที่ใช้ในการพัฒนา

a. ซอฟต์แวร์เพื่อการจัดการเวชระเบียน
   i. ซอฟต์แวร์ สำหรับโรงพยาบาล HOSxP บน Windows 7
   ii. ระบบจัดการฐานข้อมูลเชิงสัมพันธ์ MySQL
b. แอคทีฟไดเรคทอรี่ Active Directory [3]
c. โพรโทคอล Protocol
   i. ภาษามาร์กอัปการยืนยันความปลอดภัย Open source SAML software
   ii. ระบบยืนยันตัวบุคคลกลาง OpenID Connect [2]
   iii. OAuth 2.0 [2]
d. เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ PKI
e. โปรแกรมประยุกต์บนเว็บ Web Application [1]
   i. Node.js
   ii. React
   iii. HTML
   iv. ภาษา PHP
   v. JavaScript
   vi. jQuery
   vii. Cascading Style Sheets (CSS)
   viii. เว็บเซิร์ฟเวอร์ Apache/XAMPP

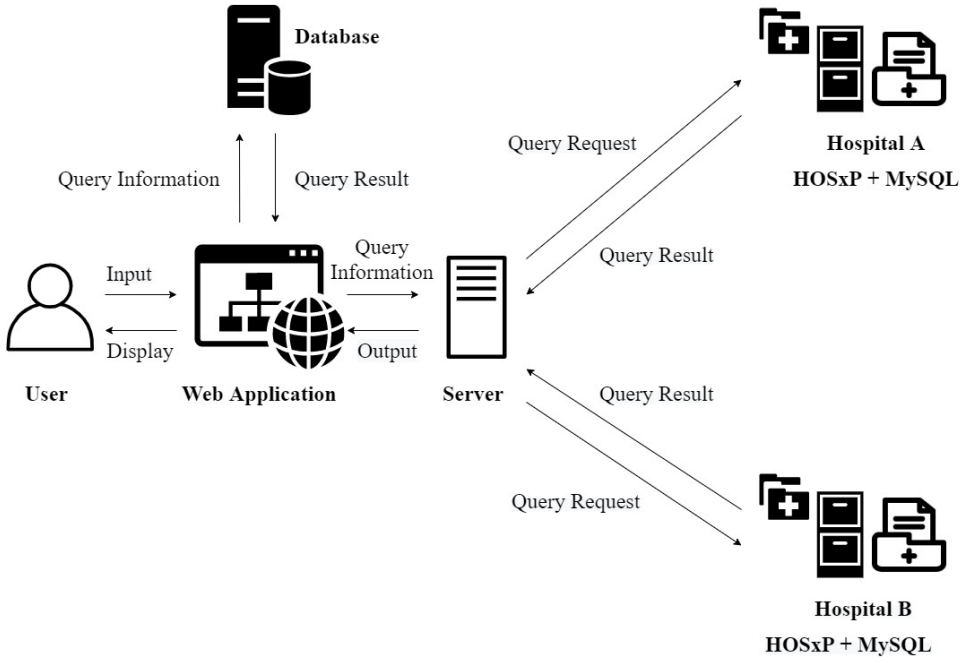
รายละเอียดโปรแกรมที่จะพัฒนา

1. Input/Output Specification
    a. Input
        i. การกรอกชื่อผู้ใช้และรหัสผ่าน
        ii. การให้สิทธิ์การเข้าถึงข้อมูลแก่บุคลากรทางการแพทย์
        iii. การกรอกข้อมูลการรักษาของผู้ป่วย
    b. Output
        i. การแสดงข้อมูลการรักษาของผู้ป่วย
        ii. การแสดงสิทธิ์ของบุคลากรทางการแพทย์
2. Functional Specification
    a. กำหนดสิทธิ์การเข้าถึงข้อมูลผ่านเว็บไซต์

        ผู้ป่วยจะสามารถกำหนดสิทธิ์การเข้าถึงข้อมูลได้ผ่านทางเว็บไซต์
    b. การเข้าถึงข้อมูล

        ผู้ป่วยและบุคลากรทางการแพทย์จะสามารถเข้าถึงข้อมูลผ่านทางเว็บไซต์ได้
    c. ความสะดวกในการใช้งานเว็บไซต์

        เว็บไซต์มีความสะดวกสบายในการใช้ และง่ายต่อการใช้งาน
3. โครงสร้างของซอฟต์แวร์ (Software Design)



ขอบเขตและข้อจำกัดของโปรแกรมที่จะพัฒนา

- ระบบการยืนยันตัวบุคคลของโรงพยาบาลจะต้องเป็นระบบใกล้เคียงกัน
- โรงพยาบาลที่ต้องการจะใช้โปรแกรมนี้ต้องสามารถเชื่อมต่อผ่านเครือข่ายสื่อสารได้ หรือได้มีการตกลงความร่วมมือแล้วเท่านั้น
- ประเภทของข้อมูลที่จะนำมาใช้ในโครงงานนี้จะเป็นข้อมูลเวชระเบียนเบื้องต้นของผู้ป่วยเท่านั้น
- ผู้ป่วยจะต้องมีบัญชีกับโรงพยาบาลในเครือแล้วอย่างน้อย 1 แห่ง
- โปรแกรมนี้รองรับเฉพาะโรงพยาบาลที่เก็บข้อมูลเวชระเบียนบนคอมพิวเตอร์เท่านั้น

กลุ่มผู้ใช้

- ผู้ป่วยหรือเจ้าของข้อมูลการรักษาของโรงพยาบาลบ้านแพ้ว โรงพยาบาลนครปฐม และโรงพยาบาลสามพราน
- บุคลากรทางการแพทย์ในเครือของโรงพยาบาลบ้านแพ้ว โรงพยาบาลนครปฐม และโรงพยาบาลสามพราน

บรรณานุกรม

1. Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, Jahangir MM, Chowdhry K, Lachhani R, Idnani N, Schumacher M, Aberer K, Stoller SD, Ryu S, Wang F ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care J Med Internet Res 2020;22(8):e13598
2. Yvonne Wilson, Abhishek Hingnikar. Solving Identity Management in Modern Applications. Apress, 2019
3. Brian Desmond, Joe Richards, Robbie Allen, and Alistair G. Lowe-Norris. Active Directory. O'REILLY, 2013

ประวัติของผู้พัฒนาโครงการ

<u>หัวหน้าโครงการ</u>

ชื่อ-นามสกุล นางสาวชิดชนก บรรจงเพียร

การศึกษา	มัธยมศึกษาตอนปลาย	ชื่อสถาบัน	มัธยมวัดนายโรง
		สายการเรียน	วิทยาศาสตร์-คณิตศาสตร์
		ปีที่จบการศึกษา	2559
	ปริญญาตรี	ชื่อสถาบัน	มหาวิทยาลัยมหิดล
		คณะ	เทคโนโลยีสารสนเทศและการสื่อสาร

<u>ผู้ร่วมโครงการ คนที่ 1</u>

ชื่อ-นามสกุล นางสาวอริสา ดลสุขเลิศ

การศึกษา	มัธยมศึกษาตอนปลาย	ชื่อสถาบัน	โรงเรียนโพธิสารพิทยากร
		สายการเรียน	วิทยาศาสตร์-คณิตศาสตร์
		ปีที่จบการศึกษา	2559
	ปริญญาตรี	ชื่อสถาบัน	มหาวิทยาลัยมหิดล
		คณะ	เทคโนโลยีสารสนเทศและการสื่อสาร

<u>ผู้ร่วมโครงการ คนที่ 2</u>

ชื่อ-นามสกุล นายจิรพัส ธรรมสงเคราะห์

การศึกษา	มัธยมศึกษาตอนปลาย	ชื่อสถาบัน	โรงเรียนสวนกุหลาบวิทยาลัย นนทบุรี
		สายการเรียน	วิทยาศาสตร์-คณิตศาสตร์
		ปีที่จบการศึกษา	2559
	ปริญญาตรี	ชื่อสถาบัน	มหาวิทยาลัยมหิดล
		คณะ	เทคโนโลยีสารสนเทศและการสื่อสาร