บัตรสุขภาพอิเล็กทรอนิกส์ : ก้าวใหม่ของการพัฒนาการบริการสาธารณสุข อย่างมีคุณภาพและมาตรฐานสูง

นายรณชัย โตสมภาค
วิทยากรชำนาญการ
กลุ่มงานบริการวิชาการ 3 สำนักวิชาการ

การจัดทำบัตรรักษาพยาบาลข้าราชการของกรมบัญชีกลาง เป็นการนำหลักการทำงานของบัตรเครดิตมาประยุกต์ใช้ เพื่อตรวจสอบและพิสูจน์ตัวบุคคล ซึ่งผู้มีสิทธิและบุคคลในครอบครัวสามารถใช้บัตรดังกล่าวในการเบิกจ่ายตรง โดยไม่ต้องรอเวลาการประมวลผลข้อมูลตามระบบเดิม เพราะสามารถตรวจสอบการทำธุรกรรมได้ทันที ทำให้กรมบัญชีกลางสามารถรับรู้ข้อมูลและค่าใช้จ่ายในการเข้ารับบริการทางการแพทย์ของผู้ป่วย และเพิ่มประสิทธิภาพในการตรวจสอบการเบิกค่ารักษาพยาบาล เพื่อป้องกันไม่ให้เกิดการทุจริตขึ้น (กรมบัญชีกลางชี้แจงโครงการจัดทำบัตรสมาร์ทการ์ดรักษาพยาบาลข้าราชการ, 2560) ทั้งนี้ ปัญหาการบานปลายของค่าใช้จ่ายในระบบสวัสดิการรักษาพยาบาลของข้าราชการ จากการเบิกจ่ายยาโดยมิชอบ ด้วยการตระเวนใช้สิทธิตามโรงพยาบาลต่าง ๆ ในเวลาใกล้เคียงกัน เพื่อขอรับยาเกินความจำเป็นของผู้ป่วย และนำยาที่ได้มาไปจำหน่ายต่อในอัตราที่ได้กำไรมากขึ้น (ป.ช.ช.แฉ พบ ขรก. เอื้อประโยชน์บริษัทยาอื้อ! ชง รบ.คุมเข้มป้องกันเบิกจ่ายยาภาครัฐ, 2560) เป็นหนึ่งในสาเหตุที่ทำให้รายจ่ายของกองทุนต้องใช้งบประมาณถึง 7.1 หมื่นล้านบาทต่อจำนวนผู้มีสิทธิ์ 4.3 ล้านคนต่อปี หรือ 1.42 หมื่นบาทต่อคน ซึ่งจัดว่ามากที่สุด เมื่อนำมาเปรียบเทียบกับกองทุนหลักประกันสุขภาพ และกองทุนประกันสังคม ที่ใช้งบประมาณเพียง 3 พันกว่าบาทต่อคนต่อปีเท่านั้น โดยจัดเป็นค่ายาถึงร้อยละ 50 ของค่าใช้จ่ายในการรักษาพยาบาลทั้งหมด หรือ 30,000 ล้านบาทต่อปี (ปิดช่อง ‘งบ’ รั่วไหล ‘บัตรรักษา ขรก.’ แก้ทุจริตได้?, 2560) ถึงอย่างไรก็ตาม นายแพทย์มงคล ณ สงขลา ประธานเครือข่ายปฏิรูประบบสวัสดิการรักษาพยาบาลข้าราชการ เห็นว่าบัตรรักษาพยาบาลข้าราชการนั้น ไม่สามารถแก้ปัญหาเรื่องทุจริตเบิกจ่ายยา มีความซ้ำซ้อน สร้างภาระให้โรงพยาบาลมากขึ้น และสิ้นเปลืองงบประมาณของประเทศ เนื่องจากโครงการใช้งบประมาณในวงเงิน 124 ล้านบาท ซึ่งเพิ่มจากเดิมกว่า 70 ล้านบาท จึงทำให้เกิดข้อสงสัยว่า บัตรนี้จะเพิ่มความสะดวกในการรับบริการจากที่มีอยู่เดิม และไม่ทำให้ค่าใช้จ่ายบานปลายยิ่งขึ้นได้หรือไม่ (“หมอมงคล” ถามกรมบัญชีกลาง ปมบัตรรักษา ขรก. ชี้ไร้ประโยชน์ แก้ทุจริตไม่ได้ สิ้นเปลืองงบ, 2560)

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้บัญญัติหน้าที่ของรัฐในการจัดบริการด้านสาธารณสุขไว้อย่างชัดเจน ในมาตรา 55 **โดยสรุปคือ รัฐต้องดำเนินการให้ประชาชนได้รับบริการสาธารณสุขที่มีประสิทธิภาพอย่างทั่วถึง เสริมสร้างให้ประชาชนมีความรู้พื้นฐานเกี่ยวกับการส่งเสริมสุขภาพและการป้องกันโรค และส่งเสริมและสนับสนุนให้มีการพัฒนาภูมิปัญญาด้านแพทย์แผนไทยให้เกิดประโยชน์สูงสุด และรัฐต้องพัฒนาการบริการสาธารณสุขให้มีคุณภาพและมีมาตรฐานสูงขึ้นอย่างต่อเนื่อง** นอกจากนี้ ในข้อที่ 5 ของหกเสาหลักของระบบสุขภาพ (The Six Building Blocks of a Health System) ขององค์การอนามัยโลก ยังระบุด้วยว่าการนำระบบข้อมูลสารสนเทศ (Health Information System) มาใช้ในการ

บริหารกำลังคน บริหารกลไกการคลังด้านสุขภาพ การติดตามและประเมินผล การจัดการเวชระเบียน การให้บริการรักษาพยาบาล และการสื่อสารข่าวสารด้านสุขภาพไปยังประชาชนกลุ่มเป้าหมายต่าง ๆ จะช่วยส่งเสริมการพัฒนาระบบบริการสุขภาพให้มีประสิทธิภาพมากขึ้น (กฤษณ์ ขุนลึก, 2560, น. 46–49) ดังนั้น รัฐบาลควรเพิ่มขีดความสามารถของบัตรสุขภาพอิเล็กทรอนิกส์ โดยเพิ่มบทบาทการทำงานให้ครอบคลุมทุกบริการที่เกี่ยวข้องกับการรักษาพยาบาล เพื่อมิให้ขอรับยาซ้ำซ้อนเกินความจำเป็น

การศึกษาเกี่ยวกับบัตรสุขภาพอิเล็กทรอนิกส์ในต่างประเทศ

Marcel Winandy ศึกษาเกี่ยวกับ **"การบริหารจัดการระบบความปลอดภัยของบัตรสุขภาพอิเล็กทรอนิกส์ในประเทศเยอรมนี (A Note on the Security in the Card Management System of the German E-Health Card)"** พบว่า สิทธิส่วนบุคคลมีความสำคัญอย่างมากต่อผู้ใช้บริการด้านสาธารณสุข ซึ่งในประเทศเยอรมนี ได้นำระบบบัตรสุขภาพอิเล็กทรอนิกส์แบบสมาร์ทการ์ดมาใช้ (Smart card) โดยมีการฝังแผงไมโครโปรเซสเซอร์ (Microprocessor chip) ที่บรรจุชุดคำสั่งที่จำเป็นต่าง ๆ เอาไว้ พร้อมพื้นที่ความจุสำหรับบันทึกข้อมูลทั่วไปของผู้ป่วย อาทิ ชื่อ นามสกุล อายุ น้ำหนัก ส่วนสูง ฯลฯ รวมถึงพื้นที่การจัดเก็บข้อมูลภายนอก (Server storage) สำหรับการบริหารจัดการเวชระเบียนอิเล็กทรอนิกส์ของผู้ป่วย (Electronic Health Records–EHRs) การออกใบสั่งยาอิเล็กทรอนิกส์ (E-prescriptions) และการชำระค่าบริการรักษาพยาบาล (Medical Billing) โดยนำระบบเข้ารหัสมาใช้ (Cryptography) เพื่อเก็บรักษาข้อมูลส่วนตัวของผู้ป่วย ด้วยการซ่อนความหมายของข้อความ และการถอดรหัสด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ทั้งนี้ แพทย์หรือสถานประกอบการสามารถเข้าถึงข้อมูลที่อยู่ในบัตรสุขภาพอิเล็กทรอนิกส์ต่อเมื่อได้รับการยินยอมจากผู้ป่วยเท่านั้น เพราะผู้ป่วยเป็นบุคคลเดียวที่สามารถถอดรหัสภายในบัตร โดยการใส่รหัสลับส่วนบุคคลลงในเครื่องอ่านบัตรที่ติดตั้งไว้ภายในห้องตรวจของคลินิกและโรงพยาบาล (Personal Identification Number Code–PIN Code) นอกจากนี้ เพื่อให้ระบบการทำงานผ่านบัตรสมาร์ทการ์ดมีประสิทธิภาพสูงสุด ระบบบริหารจัดการบัตรจึงถูกออกแบบให้รัดกุมและตอบสนองต่อความจำเป็นของผู้ใช้งานในทุกขั้นตอนและทุกด้าน ดังนี้

1. การผลิตบัตร โดยบริษัทผู้ผลิตบัตร

2. การส่งมอบบัตรแก่หน่วยงานประกันสุขภาพ เพื่อออกบัตรแก่ผู้ประกันตน รวมถึงลงทะเบียนในระบบบริหารจัดการบัตร (Card Management System–CMS) ซึ่งเป็นเครือข่ายส่วนกลางของทั้งระบบ

3. การใช้งานบัตรในส่วนของผู้ประกันตน ทุกครั้งที่เข้ารับการรักษาพยาบาล โดยแพทย์จะป้อนข้อมูลการรักษา การออกใบสั่งยา รวมถึงข้อมูลใหม่ ๆ และส่งไปยังผู้ควบคุมโปรแกรม (Application operator) คอมพิวเตอร์ เพื่อปรับปรุงฐานข้อมูลส่วนบุคคลให้เป็นปัจจุบัน

4. ในกรณีที่บัตรสุขภาพอิเล็กทรอนิกส์สูญหายหรือชำรุด หน่วยงานผู้ออกบัตรต้องกู้ข้อมูลและเข้ารหัสพร้อมกับออกบัตรใหม่ให้แก่ผู้ประกันตน (Martin Szomszor และ Patty Kostkova, 2010, p. 196–198)

Denis Protti ศึกษาเกี่ยวกับ **"การมุ่งหน้าสู่ระบบเวชระเบียนอิเล็กทรอนิกส์ที่มีความเป็นหนึ่งเดียวและครอบคลุมพลเมืองทุกคนในแคว้นอันดาลูซีอา ราชอาณาจักรสเปน (Moving toward a Single Comprehensive**

Electronic Health Record for Every Citizen in Andalucia, Spain)" พบว่า รัฐบาลแคว้นให้ความสำคัญต่อความคิดเห็นและข้อเสนอแนะของแพทย์ โดยเฉพาะมิติด้านความปลอดภัยและการควบคุมคุณภาพการรักษาพยาบาล ดังนั้น ระบบเวชระเบียนอิเล็กทรอนิกส์ของแคล้นอันดาลูซีอา หรือ DIRAYA จึงถูกพัฒนาออกแบบ และวางโครงสร้าง ด้วยความร่วมมือระหว่างคณะแพทย์และบริษัทเทคโนโลยีสารสนเทศ โดยรัฐบาลได้จดทะเบียนทรัพย์สินทางปัญญา เพื่อเป็นเจ้าของระบบแต่เพียงผู้เดียว ทั้งนี้ DIRAYA ทำงานบนพื้นฐานการดูแลรักษาที่ยึดผู้ป่วยเป็นศูนย์กลาง (Patient-centered philosophy) โดยให้อำนาจแก่บุคคล ในการบริหารจัดการเวชระเบียนส่วนตัว และข้อมูลอื่น ๆ ภายในบัตรสุขภาพอิเล็กทรอนิกส์ รวมถึง อิสรภาพในการเข้ารับบริการรักษาพยาบาล โดยไม่จำกัดเวลาและสถานที่ เพราะแพทย์และสถานประกอบการสามารถเข้าถึงข้อมูลของประชากรที่ถูกรวบรวมไว้ในระบบเดียว ได้อย่างสะดวกรวดเร็วมากขึ้น ทั้งนี้ ระบบ DIRAYA มีส่วนจำเพาะซึ่งทำหน้าที่ต่าง ๆ ดังนี้

1. ฐานข้อมูลผู้ใช้งาน (User Database–UDB) เมื่อมีการลงทะเบียน UDB จะทำหน้าที่ระบุตัวตนและบรรจุข้อมูลทั่วไป (Administrative data) ของผู้ใช้งานลงในฐานข้อมูลส่วนกลางของระบบ ประกอบด้วย หลักประกันสุขภาพภาครัฐ (Public health coverage) สิทธิในการรับบริการเภสัชกรรม (Pharmaceutical services) และแพทย์ปฐมภูมิที่ผู้รับบริการแต่ละรายได้คัดเลือกไว้ (Primary doctor) โดยข้อมูลต่าง ๆ เหล่านี้เข้าถึงได้โดยผ่านบัตรสุขภาพอิเล็กทรอนิกส์ของแต่ละบุคคลเท่านั้น

2. ศูนย์กลางการปฏิบัติการด้านการเข้าถึงข้อมูล (Operator-centralized access module–OCAM) เมื่อผู้ให้บริการต้องการเข้าถึงข้อมูลของผู้ป่วยที่เข้ารับการรักษาพยาบาล หลังจากผู้รับบริการได้ถอดรหัสบัตรสุขภาพอิเล็กทรอนิกส์ส่วนบุคคลแล้ว ผู้ให้บริการจะสามารถเข้าถึงข้อมูลจำเพาะต่าง ๆ ที่ได้มีการลงทะเบียนไว้ใน OCAM เท่านั้น เช่น แพทย์ปฐมภูมิสามารถใช้งานส่วนจำเพาะสำหรับการแพทย์ปฐมภูมิ (Primary care module) ส่วนจำเพาะสำหรับการขอคำปรึกษาระหว่างกัน (Cross-consultation request module) และส่วนจำเพาะสำหรับข้อมูลในการรับวัคซีน (Vaccine module) ในขณะที่ส่วนอื่น ๆ จะไม่สามารถเข้าถึงได้ เนื่องจากไม่ได้รับอนุญาตจาก OCAM นั่นเอง ทั้งนี้ หากต้องการเข้าถึงข้อมูลจำเพาะอื่น ๆ จำเป็นต้องพิสูจน์ตัวตน ด้วยการลงทะเบียนและยื่นคำร้องขอต่อ OCAM ก่อนเสมอ

3. ส่วนจำเพาะด้านโครงสร้าง (Structure module) เป็นส่วนที่จัดเก็บฐานข้อมูลของสถานประกอบการและหน่วยบริการต่าง ๆ ที่อยู่ในระบบสาธารณสุขของรัฐ โดยหน่วยงานต่าง ๆ ต้องทำการลงทะเบียนกับ DIRAYA ทั้งนี้ ส่วนจำเพาะด้านโครงสร้างจะทำหน้าที่ช่วยเหลือด้านการประสานงานและแลกเปลี่ยนข้อมูลทางการแพทย์ระหว่างหน่วยงานต่าง ๆ อาทิ การปรึกษาหารือข้ามหน่วยงาน (Cross-consultation) และการส่งมอบแบบทดสอบวินิจฉัย (Diagnostic tests) ระหว่างหน่วยแพทย์ปฐมภูมิและโรงพยาบาลเชี่ยวชาญเฉพาะด้าน เป็นต้น

ในส่วนของระบบการทำงาน DIRAYA มีบริการต่าง ๆ ดังนี้

1. การรวบรวมและจัดเก็บฐานข้อมูลการรักษาพยาบาล ของประชากรภายในแคว้น จากหน่วยบริการปฐมภูมิ (Primary Healthcare–PHCs) หน่วยบริการการแพทย์ฉุกเฉิน (Emergency services) หน่วยบริการจิตเวช (Mental health Services) และสถานพยาบาลที่ให้บริการรักษาพยาบาลผู้ป่วยนอกเฉพาะทาง

(Outpatient specialized care) โดยข้อมูลทั้งหมดจะถูกรวบรวมไว้ที่ NUHSA และสามารถเข้าถึงได้ในทุกสถานทุกเวลา ทั้งนี้ ข้อมูลต่าง ๆ จะถูกจัดแบ่งอยู่ใน 3 ลำดับชั้น ซึ่งในสองส่วนแรก ผู้ให้บริการส่วนต่าง ๆ สามารถใช้งานร่วมกันได้ แต่ในชั้นที่สามจะมีองค์ประกอบแตกต่างกันไป ขึ้นอยู่กับการใช้งานของผู้ให้บริการและผู้รับบริการ โดยในชั้นแรกจะประกอบด้วยข้อมูลทางสุขภาพทั่วไป เช่น ข้อมูลด้านครอบครัวและสังคม (Socio-family information) ปัญหาสุขภาพ (Health problem) ประวัติส่วนตัวและครอบครัว (Personal and family records) และ อาการภูมิแพ้ต่าง ๆ (Allergies) เป็นต้น ในส่วนที่สองจะประกอบด้วย ข้อมูลด้านการบำบัดวินิจฉัย (Therapeutic and diagnostic measures) การปรึกษาหารือข้ามหน่วยงาน (Cross-consultation) ข้อมูลด้านการวิเคราะห์ (Analysis) แบบทดสอบวินิจฉัย (Diagnostic test) การรักษาโรคด้วยยา (Drug treatment) และแบบสอบถามต่าง ๆ (Questionnaires) เป็นต้น ในส่วนสุดท้ายจะเป็นส่วนที่แตกต่างจากสองส่วนแรก ประกอบไปด้วยข้อมูลตารางบันทึกการเข้ารับการรักษา (Attendance sheet) ระหว่างผู้ให้บริการและผู้รับบริการ โดยตารางบันทึกจะแตกต่างกันไป ขึ้นอยู่กับประเภทของการให้บริการและผู้ให้บริการ อาทิ แพทย์ปฐมภูมิ แพทย์ผู้เชี่ยวชาญเฉพาะด้าน นักสังคมสงเคราะห์ โปรแกรมสุขภาพต่าง ๆ ฯลฯ

2. การระบุตัวบุคคลบนพื้นฐานของเทคโนโลยีสมาร์ทการ์ด (Smartcard technology)

3. การนัดหมายแพทย์แบบรวมศูนย์กลาง (Centralized appointment system) โดยประชากรสามารถนัดเวลาพบแพทย์ (bookings) ขอความคิดเห็นที่สองทางการแพทย์ (Request second opinions) และขอเปลี่ยนแพทย์ผู้ดูแลรักษาผ่านระบบออนไลน์ ซึ่งหน่วยการแพทย์ปฐมภูมิและสถานพยาบาลต่าง ๆ ล้วนให้บริการผ่านระบบนี้ทั้งสิ้น นอกจากนี้ การนัดเพื่อส่งตัวผู้ป่วย (Referral booking) ระหว่างแพทย์ปฐมภูมิและแพทย์ผู้เชี่ยวชาญเฉพาะด้าน ต้องทำผ่านระบบออนไลน์เช่นกัน โดยต้องทำให้แล้วเสร็จภายในระยะเวลา 2 เดือน ซึ่งแพทย์ผู้เชี่ยวชาญ ไม่สามารถปฏิเสธการส่งตัวผู้ป่วย แต่ถ้าไม่สามารถตอบรับ มีสิทธิมอบหมายให้แพทย์ผู้เชี่ยวชาญรายอื่นมาดูแลรักษาผู้ป่วยแทนได้ เป็นการแบ่งเบาภาระของหน่วยปฐมภูมิ ทำให้แพทย์มีเวลาในการดูแลรักษาผู้ป่วยทั่วไปอย่างมีประสิทธิภาพมากขึ้น

4. การออกใบสั่งยาอิเล็กทรอนิกส์ ที่เชื่อมต่อระหว่างแพทย์และเภสัชกร โดยปราศจากการใช้กระดาษ ในการบำบัดรักษาผู้ป่วยรายต่าง ๆ แพทย์ปฐมภูมิและแพทย์ผู้เชี่ยวชาญเฉพาะด้านสามารถทำการรักษาต่อเนื่องได้นานสุดเป็นเวลาหนึ่งปี ในระยะเวลานี้ ผู้ป่วยสามารถทำการเบิกจ่ายยาที่ร้านขายยาท้องถิ่น (community pharmacy) ได้อย่างต่อเนื่อง โดยไม่ต้องนัดพบแพทย์ในครั้งต่อ ๆ ไป เป็นการอำนวยความสะดวกแก่ผู้รับบริการ และทำให้แพทย์มีเวลารักษาผู้ป่วยรายอื่นมากขึ้น ทั้งนี้ เภสัชกรท้องถิ่น (Local pharmacist) จะทำการเข้าระบบและตรวจสอบข้อมูลการออกใบสั่งยาในบัตรสุขภาพอิเล็กทรอนิกส์ และจัดยาให้ตรงตามความจำเป็นตามระยะเวลาที่แพทย์กำหนดไว้ เป็นการลดค่าใช้ด้านยาของรัฐ เพราะการทุจริตเบิกจ่ายยาทำได้ยากมากภายใต้ระบบดังกล่าว นอกจากนี้ เภสัชกรยังสามารถบันทึกประวัติการจ่ายยาและรายงานให้แพทย์ทราบเกี่ยวกับผลข้างเคียงต่าง ๆ ที่เกิดขึ้นจากการใช้ยาอีกด้วย

5. **การเข้าถึงบริการเครือข่ายเชื่อมโยงสำหรับประชากร (Web access services)** โดยประชากรสามารถเข้าระบบเพื่อแก้ไขข้อมูลทั่วไป (Administrative data) และตรวจสอบข้อมูลทางคลินิกส่วนบุคคล (Personal clinical data) เช่น การออกใบสั่งยา (Prescriptions) เวชระเบียน (Health records) รายงานการจำหน่ายผู้ป่วย (Discharged reports) และบันทึกการรับวัคซีน (Vaccine records) รวมถึงการสมัครใช้งานและออกบัตรใหม่ นอกจากนี้ ยังสามารถเลือกแพทย์เฉพาะทางด้านเวชศาสตร์ครอบครัว (Family doctors) และกุมารแพทย์ (Pediatrician) ผ่านระบบออนไลน์ได้อีกด้วย

6. **ศูนย์ให้บริการข้อมูลประชาชน 24 ชั่วโมง**

7. **การคลังข้อมูล (Data warehouse) และระบบสนับสนุนการตัดสินใจ (Decision Support System–DSS)** สำหรับการบริหารงานทางคลินิกที่ดี (Clinical governance) และการจัดการเชิงกลยุทธ์ (Strategic management)

8. **ระบบการแพทย์ทางไกล (Telemedicine system)** เป็นเครือข่ายอิเล็กทรอนิกส์ที่ทำงานอยู่บนพื้นฐานของการสื่อสารพร้อมภาพและเสียง (Video conferencing) และการถ่ายโอนข้อมูลทางไกล อาทิ ภาพคลื่นไฟฟ้าหัวใจ (Electrocardiograms) ภาพรังสีหรือภาพถ่ายเอ็กซเรย์ (Radiological images) และเอกสารทั่วไป (Documents) เป็นต้น โดยศูนย์การติดต่อสื่อสารการแพทย์ทางไกลส่วนกลาง (Central telemedicine communications center) ทำหน้าที่บริหารเครือข่ายและตัวกลางในการประสานงานระหว่างสถานพยาบาลต่าง ๆ ตั้งแต่ระดับชุมชนไปจนถึงระดับส่วนภูมิภาค

9. **การรอเรียกรับบริการออนไลน์ (Waiting list system)** (Denis Protti, 2007, p. 114–122)

Hans Lohr และคณะ ศึกษาเกี่ยวกับ **"การรักษาความปลอดภัยของระบบสุขภาพอิเล็กทรอนิกส์บนเครือข่ายประมวลผลและจัดเก็บข้อมูลออนไลน์ (Securing the e-Health cloud)"** พบว่า ความปลอดภัยด้านข้อมูลของผู้รับบริการทางการแพทย์ เป็นสิ่งสำคัญที่สุดและต้องได้รับการป้องกันและแก้ไขอย่างมีประสิทธิภาพ เพราะการรั่วไหลของข้อมูล อาจมีผลกระทบที่รุนแรงต่อสถานะทางสังคมของผู้ป่วย โดยธนาคารและบริษัทประกันอาจปฏิเสธธุรกรรมทางการเงิน หรือบริษัทและห้างร้านอาจปฏิเสธการจ้างงาน เนื่องจากสุขภาวะของบุคคลนั้นไม่เอื้ออำนวย นอกจากนี้ หากบัตรสุขภาพอิเล็กทรอนิกส์ชำรุดหรือสูญหาย ข้อมูลต่าง ๆ ที่อยู่ในบัตรหรือข้อมูลที่ถูกจัดเก็บในระบบเครือข่ายออนไลน์ (Cloud system) ที่จำเป็นต้องใช้บัตรในการถอดรหัสข้อมูล (Cryptographic Key) จะสูญหายไปด้วยหรือไม่ ดังนั้น ผู้บริหารเครือข่ายส่วนกลางจึงต้องมีการบริหารจัดการการถอดรหัสข้อมูล (Cryptographic key management) โดยมีระบบจัดเก็บฐานข้อมูลสำรอง (Backup data) ในกรณีที่มีความจำเป็นต้องป้อนข้อมูลที่มีอยู่ลงในบัตรใหม่ ทั้งนี้ หากผู้บริหารเครือข่ายส่วนกลางมีการจัดเก็บฐานข้อมูลของผู้ใช้บริการบัตรแต่ละราย แปลว่ามีบุคคลนอกเหนือจากเจ้าของบัตรที่สามารถเข้าถึงข้อมูลการต่าง ๆ ได้ จึงไม่สามารถรับประกันความปลอดภัยของผู้รับบริการได้อีกต่อไป ดังนั้น จึงต้องมีการปรับปรุงการจัดเก็บและการประมวลผลข้อมูล โดยนำระบบการจำลองการทำงานของโดเมนที่เชื่อถือได้มาใช้ (Trusted Virtual Domains–TVDs) เพื่อป้องกันการรั่วไหลของข้อมูลและรักษาความเป็นส่วนตัวของผู้รับบริการได้มากที่สุด

ในการนี้ TVDs คือการสร้างโดเมนส่วนตัว (Privacy domains concept) เพื่อปกปิดข้อมูลบางส่วนให้บุคคลทั่วไปไม่สามารถเข้าถึงได้ โดยการแยกข้อมูลต่าง ๆ ออกจากกัน และอนุญาตให้เข้าถึงได้แค่บางส่วนเท่านั้น สำหรับระบบสุขภาพอิเล็กทรอนิกส์ ควรแบ่งเป็นสามโดเมน โดยจำแนกตามลักษณะข้อมูลและการปฏิบัติงาน ดังนี้

1. การบริการชำระค่ารักษาพยาบาล (Medical billing services) ประกอบด้วยชุดคำสั่งการทำงานด้านการบัญชี (Accounting software) โดยแพทย์และเจ้าหน้าที่งานประกันสุขภาพเท่านั้น ที่สามารถเข้าถึงและบริหารจัดการข้อมูลต่าง ๆ ได้

2. การบริหารจัดการเวชระเบียนอิเล็กทรอนิกส์ของผู้ป่วย (Electronic Health Record–EHR Server) ประกอบด้วยชุดคำสั่งการทำงานด้านการบริหารจัดการเวชระเบียนของผู้ป่วย (EHR software) โดยแพทย์เท่านั้น ที่สามารถเข้าถึงข้อมูลส่วนนี้ได้

3. บริการอื่น ๆ (Other services) คือโดเมนทั่วไปที่ไม่จำกัดการใช้งาน ซึ่งประกอบด้วยโปรแกรมทั่วไป (Untrusted programs) เช่น โปรแกรมที่ช่วยค้นหาหรืออ่านเอกสารบนอินเตอร์เน็ต (Web browser) หรือโปรแกรมรับส่งอีเมล์ (E-mail client) เป็นต้น

ทั้งนี้ เมื่อมีการโอนถ่ายข้อมูลไปยังอุปกรณ์อื่น ๆ ไม่ว่าจะเป็นทางออนไลน์ผ่านโดเมนทั่วไปหรือทางกายภาพผ่านอุปกรณ์เก็บข้อมูลแบบพกพา (Handy drives) ระบบ TVDs จะทำการเข้ารหัสข้อมูลโดยอัตโนมัติ เพื่อให้ระบบปฏิบัติงานที่มีชุดคำสั่งตรงกันสามารถเข้าถึงข้อมูลได้เท่านั้น ในทางตรงกันข้าม อุปกรณ์ปลายทางที่ไม่มีการติดตั้งชุดคำสั่ง จะไม่สามารถเปิดดูหรือแก้ไขข้อมูลได้เลย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น (Hans Lohr และคณะ, 2010)

Mohammad Tauhidul Alam และ Liakot Ali ศึกษาเกี่ยวกับ **"ระบบสุขภาพอิเล็กทรอนิกส์อัจฉริยะในรูปแบบที่ปลอดภัย (A model of a secured smart e-Health system)"** พบว่า ระบบสุขภาพอิเล็กทรอนิกส์ที่ดีจะต้องออกแบบอย่างมีประสิทธิภาพและมีระบบรักษาความปลอดภัยที่มั่นคง โดยมีอุปกรณ์การทำงาน (Hardware) ที่ประกอบด้วยบัตรสุขภาพอิเล็กทรอนิกส์และเครื่องอ่านบัตรที่ติดตั้งในจุดบริการของสถานพยาบาลทุกแห่ง ซึ่งบัตรสุขภาพสามารถแบ่งออกเป็น 3 ชนิด คือ บัตรสีขาวสำหรับบุคคลทั่วไป บัตรสีน้ำเงินสำหรับผู้อาวุโส และบัตรสีเขียวสำหรับผู้พิการ และชุดคำสั่งการทำงาน (Software) ที่แบ่งออกเป็นส่วนที่ทำงานผ่านเว็บไซต์ (Web based module) ผ่านระบบประมวลผลและจัดเก็บข้อมูลออนไลน์ (Cloud system) ในรูปแบบของศูนย์ข้อมูล และส่วนของบัตรสุขภาพอิเล็กทรอนิกส์สำหรับการออกบัตร การรับรองตัวตนผู้ใช้งาน (Authentication) ผ่านการระบุตัวตนทางเครือข่าย (Network identification–NID) และการบริหารจัดการความปลอดภัย (Security management) ด้วยการนำระบบควบคุมการเข้าถึงข้อมูลตามสถานะของผู้ใช้งาน (Role-based access control–RBAC) และกระบวนการถอดรหัสตามขั้นตอน (Encryption algorithm) ในการแลกเปลี่ยนเอกสารการแพทย์มาใช้ ทั้งนี้ เป็นการทำงานผ่านเว็บไซต์ประกอบด้วย 9 ขั้นตอน ดังนี้

1. ขั้นตอนการระบุตัวตนและการลงทะเบียน (Verification and registration process) โดยประชากรทุกคนต้องได้รับการระบุตัวตนทางเครือข่ายผ่านฐานข้อมูลประชากรแห่งชาติ (National database–NDB)

หลังจากนั้น จึงสามารถทำการลงทะเบียนเพื่อรับบัตรสุขภาพอิเล็กทรอนิกส์ได้ นอกจากนี้ ผู้ให้บริการเอง รวมถึงสถานประกอบพยาบาลต่าง ๆ ก็ต้องลงทะเบียนในระบบเช่นกัน

2. ขั้นตอนการเข้าระบบ (Login process) โดยผู้ให้บริการและผู้รับบริการต่างได้รับรหัสผ่านของตนเอง และจำเป็นต้องใช้ทุกครั้ง เมื่อต้องการเข้าถึงข้อมูลต่าง ๆ ในระบบสุขภาพอิเล็กทรอนิกส์

3. ขั้นตอนการเข้าดูเวชระเบียนผู้ป่วย (View patient's medical record process) โดยผู้ใช้งานต้องทำการถอดรหัส เมื่อต้องการเข้าดูเวชระเบียนของแต่ละบุคคลที่บรรจุไว้ในระบบ

4. ขั้นตอนการออกใบสั่งยาอิเล็กทรอนิกส์ (e-Prescription process) โดยแพทย์สามารถตรวจสอบข้อมูลของผู้ป่วยที่เข้ารับการรักษา ตั้งแต่ประวัติการแพ้ยาจนถึงประวัติการตรวจวินิจฉัยโรคต่าง ๆ เพื่อสั่งจ่ายยาให้เหมาะสมกับการรักษาโรคที่เป็นอยู่ในปัจจุบัน

5. ขั้นตอนการทดสอบทางพยาธิวิทยา (Patient pathology test process) โดยเจ้าหน้าที่ในห้องปฏิบัติการทางพยาธิวิทยา จะรับคำสั่งและทำการทดสอบผู้ป่วยตามที่แพทย์มอบหมาย ผ่านทางบัตรสุขภาพอิเล็กทรอนิกส์

6. ขั้นตอนการนำเข้ารายงานทางพยาธิวิทยา (Upload pathology report process) โดยนักเทคนิคการแพทย์จะนำส่งรายงานการทดสอบทางพยาธิวิทยา ขึ้นสู่สารบบชั่วคราว (Temporary directory) เพื่อนำส่งให้แพทย์ทำการตรวจสอบ

7. ขั้นตอนการตรวจสอบรายงานทางพยาธิวิทยา (Check pathology report process) โดยแพทย์จะทำการวินิจฉัยผลการทดสอบทางพยาธิวิทยา และนำส่งข้อมูลพร้อมกับเข้ารหัส ไปยังสารบบส่วนตัวของผู้ป่วย

8. ขั้นตอนการเข้ารหัสและการถอดรหัสข้อมูล (File encryption/decryption process) โดยแพทย์จะทำการเข้ารหัสข้อมูล ทุกครั้งที่มีการรักษาพยาบาล และผู้ป่วยจะถอดรหัสข้อมูล ทุกครั้งที่เข้ารับการรักษาพยาบาล ผ่านบัตรสุขภาพอิเล็กทรอนิกส์

9. ขันตอนการรับผู้ป่วยใน (Patient admission process) โดยโรงพยาบาลจะทำการระบุตัวตนของผู้ป่วยผ่านบัตรสุขภาพอิเล็กทรอนิกส์ และทำการรับเข้าเป็นผู้ป่วยใน พร้อมกับมอบหมายแพทย์เจ้าของไข้

ในส่วนของการรักษาความปลอดภัย ได้แบ่งการดำเนินงานตามลำดับชั้นต่าง ๆ ประกอบด้วยชั้นความปลอดภัยในการทำงานของบัตรอัจฉริยะ (Smart card security) ชั้นความปลอดภัยด้านการระบุตัวตนและการควบคุมการเข้าถึงข้อมูล (Authenticity and access control mechanism) ชั้นความปลอดภัยในการแลกเปลี่ยนเอกสาร (Document exchange security) และชั้นความปลอดภัยในการเข้าถึงข้อมูลส่วนกลาง (Central access log) ทั้งนี้ ความปลอดภัยด้านการระบุตัวตนและการควบคุมการเข้าถึงข้อมูลจะถูกควบคุมโดยระบบควบคุมการเข้าถึงข้อมูลตามสถานะของผู้ใช้งาน ที่ช่วยป้องกันไม่ให้ข้อมูลรั่วไหลสู่บุคคลที่ไม่เกี่ยวข้องโดยไม่จำเป็น ซึ่งมีรายละเอียดต่าง ๆ ดังนี้

1. กลุ่มผู้ป่วย (Patients) สามารถอ่านเวชระเบียนส่วนบุคคลและแก้ไขปรับปรุงข้อมูลส่วนตัวเท่านั้น

2. กลุ่มแพทย์ (Doctors) สามารถอ่านและแก้ไขเพิ่มเติมเวชระเบียน ข้อมูลการทดสอบทางพยาธิวิทยา และออกใบสังยาแก่ผู้ป่วย

3. กลุ่มพยาบาล (Nurses) สามารถอ่านใบสั่งยาและภาวะอนามัยของผู้ป่วยที่อยู่ในความดูแลเท่านั้น

4. กลุ่มนักเทคนิคการแพทย์ (Medical technologists) สามารถอ่านคำสั่งการทดสอบทางพยาธิวิทยาตามที่แพทย์มอบหมายและนำส่งรายงานการทดสอบเข้าสู่ระบบเท่านั้น

5. กลุ่มเภสัชกร (Pharmacists) สามารถอ่านใบสั่งยาได้เท่านั้น

6. โรงพยาบาล (Hospital) สามารถอ่านข้อมูลทั่วไปและเพิ่มเติมข้อมูลสำหรับผู้ป่วยที่เข้ารับการรักษาเป็นผู้ป่วยในเท่านั้น

7. ห้องปฏิบัติการทางพยาธิวิทยา (Pathology lab) สามารถอ่านคำสั่งการทดสอบทางพยาธิวิทยาตามที่แพทย์มอบหมายและนำส่งรายงานการทดสอบเข้าสู่ระบบเท่านั้น

8. แผนกเภสัชกรรม (Pharmacy) สามารถอ่านใบสั่งยาได้เท่านั้น (Mohammad Tauhidul Alam และ Liakot Ali, 2016)

บทสรุปและข้อเสนอแนะของผู้ศึกษา

การจัดทำบัตรรักษาพยาบาลแบบบัตรสุขภาพอิเล็กทรอนิกส์เป็นการนำหลักการทำงานของบัตรเครดิตมาประยุกต์ใช้ เพื่อตรวจสอบและพิสูจน์ตัวบุคคล รวมถึงการเบิกจ่ายตรงได้ทันที รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 บัญญัติหน้าที่ของรัฐในการจัดบริการด้านสาธารณสุขไว้อย่างชัดเจนในมาตรา 55 โดยรัฐต้องพัฒนาการบริการสาธารณสุขให้มีคุณภาพและมีมาตรฐานสูงขึ้นอย่างต่อเนื่อง องค์การอนามัยโลก ยังระบุด้วยว่าด้วยการนำระบบข้อมูลสารสนเทศ (Health Information System) มาใช้จะช่วยส่งเสริมการพัฒนาระบบบริการสุขภาพให้มีประสิทธิภาพมากขึ้น ดังนั้น รัฐบาลควรให้ความสำคัญและเพิ่มขีดความสามารถของบัตรสุขภาพอิเล็กทรอนิกส์ โดยเพิ่มบทบาทการทำงานให้ครอบคลุมทุกบริการที่เกี่ยวข้องกับการรักษาพยาบาล ทั้งนี้ จากการศึกษาดังกล่าว มีข้อเสนอแนะต่าง ๆ ดังนี้

1. ควรมีการนำระบบบัตรสุขภาพอิเล็กทรอนิกส์แบบสมาร์ทการ์ดมาใช้ (Smart card) โดยมีการฝังแผงไมโครโปรเซสเซอร์ (Microprocessor chip) ที่บรรจุชุดคำสั่งที่จำเป็นต่าง ๆ เอาไว้ พร้อมพื้นที่ความจุสำหรับบันทึกข้อมูลทั่วไปของผู้ป่วย รวมถึงพื้นที่การจัดเก็บข้อมูลภายนอก (Server storage) สำหรับการบริหารจัดการเวชระเบียนอิเล็กทรอนิกส์ของผู้ป่วย (Electronic Health Records–EHRs) การออกใบสั่งยาอิเล็กทรอนิกส์ (E-prescriptions) และการชำระค่าบริการรักษาพยาบาล (Medical Billing)

2. การนำระบบการเข้ารหัสมาใช้ (Cryptography) เพื่อเก็บรักษาข้อมูลส่วนตัวของผู้ป่วย ด้วยการซ่อนความหมายของข้อความ และการถอดรหัสด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ทั้งนี้แพทย์หรือสถานประกอบการสามารถเข้าถึงข้อมูลที่อยู่ในบัตรสุขภาพอิเล็กทรอนิกส์ ต่อเมื่อได้รับการยินยอมจากผู้ป่วยเท่านั้น เพราะผู้ป่วยเป็นบุคคลเดียวที่สามารถถอดรหัสภายในบัตร โดยการใส่รหัสลับส่วนบุคคลลงในเครื่องอ่านบัตรที่ติดตั้งไว้ภายในห้องตรวจของคลินิกและโรงพยาบาล (Personal Identification Number Code–PIN Code)

3. ระบบเวชระเบียนอิเล็กทรอนิกส์ควรถูกพัฒนา ออกแบบ และวางโครงสร้าง ด้วยความร่วมมือระหว่างคณะแพทย์และบริษัทเทคโนโลยีสารสนเทศ โดยรัฐบาลควรเป็นเจ้าของระบบแต่เพียงผู้เดียว เพื่อความปลอดภัยและความมีประสิทธิภาพของระบบโดยรวม

4. ควรนำระบบการจำลองการทำงานของโดเมนที่เชื่อถือได้มาใช้ (Trusted Virtual Domains–TVDs) เพื่อป้องกันการรั่วไหลของข้อมูลและรักษาความเป็นส่วนตัวของผู้รับบริการได้มากที่สุด โดยการสร้างโดเมนส่วนตัว (Privacy domains concept) เพื่อปกปิดข้อมูลบางส่วน โดยบุคคลทั่วไปไม่สามารถเข้าถึงได้ด้วยการแยกข้อมูลต่าง ๆ ออกจากกัน และอนุญาตให้เข้าถึงได้แค่บางส่วนเท่านั้น ทั้งนี้ เมื่อมีการโอนถ่ายข้อมูลไปยังอุปกรณ์อื่น ๆ ไม่ว่าจะเป็นทางออนไลน์ผ่านโดเมนทั่วไปหรือทางกายภาพผ่านอุปกรณ์เก็บข้อมูลแบบพกพา (Handy drives) ระบบ TVDs จะทำการเข้ารหัสข้อมูลโดยอัตโนมัติ เพื่อให้ระบบปฏิบัติงานที่มีชุดคำสั่งตรงกันสามารถเข้าถึงข้อมูลได้เท่านั้น ในทางตรงกันข้าม อุปกรณ์ปลายทางที่ไม่มีการติดตั้งชุดคำสั่งจะไม่สามารถเปิดดูหรือแก้ไขข้อมูลได้เลย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น

5. บัตรสุขภาพอิเล็กทรอนิกส์ควรแบ่งออกเป็น 3 ชนิด เพื่อความสะดวกในการใช้งาน คือ บัตรสีขาวสำหรับบุคคลทั่วไป บัตรสีน้ำเงินสำหรับผู้อาวุโส และบัตรสีเขียวสำหรับผู้พิการ

6. ควรนำระบบควบคุมการเข้าถึงข้อมูลตามสถานะของผู้ใช้งานมาใช้ (Role-based access control–RBAC) เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลสู่บุคคลที่ไม่เกี่ยวข้องโดยไม่จำเป็นโดยผู้ใช้งานกลุ่มต่าง ๆ ในโรงพยาบาล สามารถเข้าถึงข้อมูลได้ เฉพาะในส่วนที่ตัวเองรับผิดชอบเท่านั้น

บรรณานุกรม

ภาษาไทย

กฤษณ์ ขุนลึก. (กันยายน 2560). **รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 กับ แนวทางการปฏิรูประบบบริการสาธารณสุข แก่ประชาชนไทย.** วารสารการบริหารปกครอง, 6, 40–57

กรมบัญชีกลางชี้แจงโครงการจัดทำบัตรสมาร์ทการ์ดรักษาพยาบาลข้าราชการ. (19 พฤษภาคม 2560). สืบค้น 7 กันยายน 2560 จาก http://www.thaigov.go.th/news/contents/details/3841

ป.ช.ช.แฉ พบขรก.เอื้อประโยชน์บริษัทยาอื้อ! ชง รบ.คุมเข้มป้องกันเบิกจ่ายยาภาครัฐ. (20 กรกฎาคม 2560). สืบค้น 7 กันยายน 2560 จาก https://www.matichon.co.th/news/607088

ปิดช่อง 'งบ' รั่วไหล 'บัตรรักษาขรก.' แก้ทุจริตได้? (2 สิงหาคม 2560). สืบค้น 7 กันยายน 2560 จาก http://www.thansettakij.com/content/186583

"หมอมงคล" ถามกรมบัญชีกลาง ปมบัตรรักษา ขรก. ชี้ไร้ประโยชน์ แก้ทุจริตไม่ได้ สิ้นเปลืองงบ. (18 กรกฎาคม 2560) สืบค้น 7 กันยายน 2560 จาก https://www.hfocus.org/content/2017/07/14245

ภาษาต่างประเทศ

Denis Protti. (2007). **Moving toward a Single Comprehensive Electronic Health Record for Every Citizens in Andalucia, Spain.** Healthcare Quarterly, 10(4), 114–123

Hans Lohr, Ahmad-Reza Sadeghi and Marcel Winandy. (January 2010). **Securing the E-health cloud.** สืบค้น 7 กันยายน 2560 จาก https://www.researchgate.net/publication/221629904_Securing_the_E-health_cloud

Martin Szomszor and Patty Kostkova. (2010). **Electronic Healthcare : Third International Conference, eHealth 2010, Casablanca, Morocco, December 13-15, 2010, Revised Selected Papers.** Switzerland : Springer International Publishing AG.

Mohammad Tauhidul Alam and Liakot Ali. (March 2010). **A Model of a Secured Smart e-Health System.** สืบค้น 7 กันยายน 2560 จาก http://ieomsociety.org/ieom_2016/pdfs/656.pdf