บทที่ 1

บทนำ

ภูมิหลัง

องค์กรภาครัฐและเอกชนนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำหรับบริหารจัดการข้อมูลสารสนเทศในองค์กร ซึ่งมีทั้งข้อมูลที่เป็นความลับและเปิดเผยได้ จากการรายงานข่าวผ่านสื่อสาธารณะพบปัญหาด้านความมั่นคงปลอดภัยสารสนเทศมีการคุกคามจากบุคคลที่ไม่ได้รับอนุญาตให้เข้าสู่ระบบเพิ่มขึ้นทั้งในประเทศและต่างประเทศ ทำให้องค์กรต่างๆ สร้างมาตรการเพื่อแก้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ ประเทศไทยตระหนักถึงความสำคัญของปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ จึงออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อใช้เป็นกฎหมายในการควบคุมดูแลการใช้ระบบคอมพิวเตอร์ในประเทศไทย และมีพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (แก้ไขเพิ่มเติม ฉบับที่ 2 พ.ศ. 2551) ซึ่งใช้ในการควบคุมดูแลการทำธุรกรรมทางอิเล็กทรอนิกส์ในประเทศไทย (วศิน รำพึงกิจ, 2552, หน้า 54–58) โดยมีมาตรา 35 กำหนดให้ “คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับถือว่ามีผล โดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใดๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้” อาศัยอำนาจตามมาตรา 35 นี้ จึงได้มีการตราพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ขึ้น ซึ่งมีข้อกำหนดที่เกี่ยวข้อง 3 มาตรา ได้แก่ มาตรา 5 มาตรา 7 และมาตรา 8 ได้ให้ความสำคัญกับปัญหาด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดย

หน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากลอาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ (สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2557, หน้า 7)

การดำเนินการของแต่ละองค์กร ประกอบด้วยส่วนงานหลายส่วน ร่วมกันดำเนินงานให้บรรลุจุดประสงค์ขององค์กร องค์กรจึงได้นำระบบสารสนเทศมาประยุกต์ใช้กับกระบวนการทำงาน เช่น การควบคุมเครื่องจักรเพื่อผลิตสินค้า การบริหารจัดการเอกสารและข้อมูล การพัฒนาโปรแกรมประยุกต์ การติดต่อสื่อสารภายในองค์กร เป็นต้น ระบบคอมพิวเตอร์ขององค์กรจึงได้มีการเชื่อมต่อเป็นเครือข่ายภายในแต่ละหน่วยงาน สามารถทำงานได้สะดวกรวดเร็วขึ้น ใช้งานทรัพยากรสารสนเทศต่างๆ ร่วมกันได้เกิดประสิทธิภาพในการดำเนินงาน นอกจากนี้ขององค์กรมีการเชื่อมต่อกับเครือข่ายภายนอกเพื่อใช้อินเทอร์เน็ต สำหรับใช้ในการติดต่อสื่อสารกับองค์กรอื่นๆ หรือใช้ในการให้บริการเว็บเซอร์วิสขององค์กร ด้วยการประยุกต์ใช้ระบบสารสนเทศกับการดำเนินงานขององค์กรส่งผลให้ทรัพยากรสารสนเทศขององค์กรถูกจัดเก็บอยู่ในสื่ออิเล็กทรอนิกส์ ทำให้การเข้าถึงทรัพยากรสารสนเทศกระทำได้สะดวกผ่านช่องทางระบบเครือข่าย (วราภรณ์ ธวิทย์ชัยพร, 2549, หน้า 9–10)

สารสนเทศขององค์กรเป็นสิ่งสำคัญที่องค์กรต้องป้องกันรักษา สารสนเทศของโรงพยาบาล โรงพยาบาลส่งเสริมสุขภาพตำบล คือ ข้อมูลการรักษาผู้ป่วย ซึ่งข้อมูลการรักษาผู้ป่วยซึ่งประกอบด้วย ชื่อ เลขบัตรประจำประชาชน ประวัติการรักษาทั้งหมดของผู้ป่วย ซึ่งข้อมูลต้องเก็บเป็นความลับตามความคุ้มครองของพระราชบัญญัติสุขภาพไม่สามารถเปิดเผยสู่สาธารณะได้ รวมถึงต้องเก็บรักษาสารสนเทศเหล่านี้ให้สามารถเข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น หากข้อมูลการรักษาผู้ป่วยเกิดรั่วไหล จะส่งผลเสียต่อภาพลักษณ์ ความน่าเชื่อถือขององค์กร และที่สำคัญคือส่งผลเสียประชาชนผู้เป็นเจ้าของสารสนเทศ ดังนั้น สารสนเทศและส่วนที่เกี่ยวข้องจึงต้องได้รับการดูแลอย่างรอบคอบ

รัดกุม และป้องกันภัยคุกคามความมั่นคงปลอดภัยที่มีต่อสารสนเทศขององค์กร (วราภรณ์ ธวิทย์ชัยพร, 2549, หน้า 9–10)

ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ หมายถึง วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใด ที่กระทำอันตรายต่อสารสนเทศและส่วนที่เกี่ยวข้อง มีวัตถุประสงค์เพื่อบุกรุกระบบสารสนเทศขององค์กร ขัดขวางหรือทำลายไม่ให้ระบบสารสนเทศให้บริการได้ตามปกติ การโจรกรรมสารสนเทศขององค์กร ยึดครองระบบสารสนเทศขององค์กร (เศรษฐพงค์ มะลิสุวรรณ, 2552; เสฏฐวุฒิ แสนนาม, 2556) จากการพัฒนาทางเทคโนโลยีคอมพิวเตอร์ทำให้คอมพิวเตอร์และอุปกรณ์สนับสนุนมีสมรรถนะสูงขึ้นและราคาลดลง สามารถเข้าถึงความรู้ ข่าวสารต่างๆ ได้ง่ายและสะดวก รวมถึงเครื่องมือที่ใช้ในการคุกคามความมั่นคงปลอดภัยสารสนเทศ สามารถหาได้ง่าย เช่น ในเครือข่ายอินเตอร์เน็ต เป็นต้น เอกสารที่เกี่ยวกับการบุกรุกก็หาได้ง่าย เช่น บทความเกี่ยวกับช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของซอฟแวร์ รวมถึงวิธีการโจมตีระบบสารสนเทศรูปแบบต่างๆ เป็นต้น ดังนั้น หากประชาชนทั่วไปใช้ข้อมูลเหล่านี้ในทางเป็นประโยชน์จะส่งผลให้ระบบสารสนเทศขององค์กรเกิดเสถียรภาพ บริการสารสนเทศได้อย่างมีประสิทธิภาพและรักษาความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร แต่หากใช้ข้อมูลเหล่านี้ในทางที่ไม่ดีแล้ว จะเกิดโทษอย่างมหันต์ คือ สารสนเทศขององค์กรมีความเสี่ยงต่อภัยคุกคามมากขึ้น การป้องกันภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจึงเป็นเรื่องที่องค์กรต่างๆ ต้องสนใจ และป้องกันภัยคุกคามเหล่านี้ได้โดยการติดตั้งอุปกรณ์ป้องกันภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

อุปกรณ์สำหรับป้องกันภัยคุกคามที่นิยมและใช้งานแพร่หลาย ได้แก่ ไฟร์วอลล์ (Firewall) ไอพีเอส (IPS) ไอดีเอส (IDS) พร็อกซี (Proxy) เป็นต้น อุปกรณ์เหล่านี้มีราคาค่อนข้างสูง แต่เมื่อนำมาใช้งานกับองค์กรแล้ว พบว่าไม่สามารถป้องกันภัยคุกคามได้เต็มที่ เนื่องจากอุปกรณ์เหล่านี้เป็นเพียงส่วนหนึ่งของการป้องกันภัยคุกคามความมั่นคงปลอดภัยสารสนเทศเท่านั้น (วราภรณ์ ธวิทย์ชัยพร, 2549, หน้า 4)

นอกจากปัญหาภัยคุกคามความมั่นคงปลอดภัยสารสนเทศซึ่งเกิดจากผู้บุกรุกภายนอกแล้ว ยังพบปัญหาการใช้งานเทคโนโลยีสารสนเทศไปในทางที่ไม่เหมาะสมของบุคลากร หรือการใช้ทรัพยากรสารสนเทศขององค์กรเพื่อประโยชน์ส่วนบุคคล องค์กรจึงต้องมีการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ โดยทั่วไปแล้วองค์กรจะมีการจัดการความมั่นคงปลอดภัยสารสนเทศอยู่แล้ว แต่การจัดการนั้นไม่ครอบคลุมสารสนเทศและส่วนเกี่ยวข้องทั้งหมด ซึ่งสามารถปรับปรุงการจัดการนั้นได้โดยการอ้างอิงกับกรอบ

มาตรฐานการจัดการ ซึ่งมีหน่วยงานดูแลรับผิดชอบ ปรับปรุงหลักการจัดการนั้นอย่างสม่ำเสมอ

มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ที่เป็นมาตรฐานสากลเป็นที่ยอมรับจากภาครัฐและเอกชนทั้งในประเทศและต่างประเทศ คือ กรอบมาตรฐาน ISO/IEC27001 ระบบจัดการความมั่นคงปลอดภัย(Information Security Management System: ISMS) ได้ผ่านการปรับปรุงและเผยแพร่ในปี ค.ศ. 2005 โดยหน่วยงานองค์การระหว่างประเทศว่าด้วยมาตรฐาน (International Organization for Standardization : ISO) และคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์ (International Electrotechnical Commission : IEC) โดย ISO/IEC27001:2005 มีชื่อเต็มว่า ISO/IEC 27001:2005 – Information technology –– Security techniques –– Information security management systems – Requirements การจัดสร้างระบบ ISO/IEC27001:2005 จะมีกระบวนการและขั้นตอนที่สำคัญ คือ PDCA (Plan –Do – Check – Act) ที่ซึ่งช่วยป้องกันภัยคุกคามที่ก่อให้เกิดผลกระทบและความสูญเสียของสารสนเทศ อีกทั้งยังช่วยแก้ไขปัญหาขจัดช่องโหว่ ลดความเสี่ยงขององค์กรได้ (ชูเกียรติ ประเสริฐสุข, 2551)

จากการทบทวนวรรณกรรมพบว่างานวิจัยที่ได้ศึกษาเกี่ยวกับการจัดการความมั่นคงปลอดภัยสารสนเทศโดยอ้างอิงมาตรฐาน ISO/IEC27001 ทำให้สารสนเทศและส่วนที่เกี่ยวข้องมีความมั่นคงปลอดภัยมากยิ่งขึ้น เช่น เฉลิม สุวรรณะ (2554) ได้วิจัยเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา ศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี พบว่า การจัดการความมั่นคงปลอดภัยของโรงพยาบาลหลังจากที่ได้ปรับปรุงตามมาตรฐาน ISO/IEC27001 โดยการประเมินความเสี่ยงและดำเนินการแก้ไขเพื่อลดความเสี่ยงตามหัวข้อที่องค์กรให้ความสำคัญก่อนนั้น ผลการแก้ไข ทำให้ความเสี่ยงต่อภัยคุกคามความมั่นคงปลอดภัยสารสนเทศลดลงอยู่ในระดับกลางและต่ำ ซึ่งสอดคล้องกับงานวิจัยของ ว่าที่ร้อยตรี ภูมินทร์ ภูดวงสี (2550) ซึ่งได้วิจัยเรื่องการศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา บริษัท NEC Corporation (Thailand) Ltd. พบว่า จากการศึกษาข้อมูลนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรและการประเมินความเสี่ยงขององค์กร โดยอ้างอิงมาตรฐาน ISO/IEC27001 และจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรทำให้ความเสี่ยงภัยคุกคามด้านต่างๆ ลดลง ซึ่งสอดคล้องกับงานวิจัยของ วศิน รำพึงกิจ (2552) ที่ได้ศึกษาเรื่อง การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษา

ความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย ซึ่งได้ศึกษาสภาพปัญหาปัจจุบัน จากนั้นจึงได้อ้างอิงมาตรฐาน ISO/IEC27001 เพื่อแนะแนวทางในการแก้ปัญหาในเชิงนโยบายการจัดการ และลดความเสี่ยงของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่ต่ำลง นอกจากนี้ยังมีงานวิจัยที่ศึกษาสภาพปัจจุบันของการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร เปรียบเทียบกับมาตรฐาน ISO/IEC27001 เพื่อหาแนวทางในการจัดการความมั่นคงปลอดภัยที่สมบูรณ์มากยิ่งขึ้น ได้แก่ งานวิจัยของ วิภาวรรณ คุ้มศิริ (2552) ที่ได้ศึกษา เรื่อง การสร้างมาตรการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ .2550 กรณีศึกษาองค์กรกระจายเสียง และแพร่ภาพแห่งประเทศไทย

ปัญหาความเสี่ยงและภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ได้ยกระดับและความรุนแรงจากการที่ก่อความเสียหายทางเศรษฐกิจมาเป็น ภัยคุกคามทางการแพทย์ที่สามารถส่งผลกระทบต่อความปลอดภัยในชีวิตและสุขภาพของประชาชนเป็นวงกว้างได้ ตัวอย่างเช่น การข่มขู่คุกคามโจมตีข้อมูลระบบคอมพิวเตอร์ที่เกิดกับระบบการควบคุมการจ่ายยาของมลรัฐเวอร์จิเนีย การแพร่ระบาดไวรัสคอนฟิกเกอร์ (Conficker) ที่ทำให้เครื่องสร้างภาพด้วยสนามแม่เหล็กไฟฟ้า (Manetic Resonance Imaging: MRI) และอุปกรณ์ทางการแพทย์ติดไวรัสคอมพิวเตอร์ชนิดนี้ ทั้งในประเทศสหรัฐอเมริกา อังกฤษ และอินเดีย ส่วนประเทศไทยก็มีเครื่องสร้างภาพด้วยสนามแม่เหล็กไฟฟ้า (MRI) ติดไวรัสชนิดนี้ด้วย ซึ่งส่งผลกระทบให้เครื่องมือทางการแพทย์ที่ติดไวรัสไม่สามารถให้บริการได้ หรือรายงานผลที่ผิดพลาด และแพทย์ไม่สามารถตัดสินใจสั่งการรักษา เพราะเกรงข้อผิดพลาดที่เกิดอันตรายต่อผู้ป่วย (สุธี ทุวิรัตน์, 2552) หรือเหตุการณ์ระบบบริการสุขภาพแห่งชาติของสหราชอาณาจักรถูกมัลแวร์เรียกค่าไถ่ (WannaCry) โจมตี ซึ่งส่งผลกระทบทำให้โรงพยาบาลและคลินิกต่างๆ ไม่สามารถรับคนไข้เข้ารักษา รวมถึงต้องยกเลิกนัดหมายต่างๆ ของคนไข้ (บีบีซี, 2560)

โรงพยาบาลได้นำระบบสารสนเทศมาเป็นเครื่องมือบริหารจัดการข้อมูลในโรงพยาบาล โดยเฉพาะข้อมูลผู้ป่วย เพื่อให้การวินิจฉัยและรักษาพยาบาลผู้ป่วยทันการณ์ ซึ่งการรักษาผู้ป่วยบุคลากรทางการแพทย์จะบันทึกข้อมูลการรักษาของผู้ป่วยไว้ในเวชระเบียน เช่น ประวัติส่วนตัวของผู้ป่วย ประวัติครอบครัวของผู้ป่วย การเจ็บป่วยที่ผ่านมา การตรวจร่างกาย การตรวจวิเคราะห์ทางห้องปฏิบัติการ เป็นต้น โดยเวชระเบียนมี 2 รูปแบบ คือ

เวชระเบียนในรูปแบบเอกสาร และเวชระเบียนในรูปแบบอิเล็กทรอนิกส์บันทึกเป็นข้อมูลในคอมพิวเตอร์ ซึ่งข้อมูลการรักษาผู้ป่วยจะถูกปกปิดเป็นความลับโดยจริยธรรมการให้บริการของบุคลากรทางการแพทย์ หากข้อมูลการรักษาของผู้ป่วยถูกเปิดเผย ย่อมมีผลกระทบต่อผู้ป่วยและญาติของผู้ป่วย ดังนั้น โรงพยาบาลจึงควรจัดระบบในการรักษาความลับและมีการควบคุมกำกับให้มีการปฏิบัติอย่างจริงจัง โดยการรักษาความลับข้อมูลของผู้ป่วยในเวชระเบียนที่เป็นเอกสาร โรงพยาบาลหลายแห่งจะมีเจ้าหน้าที่ของโรงพยาบาลเป็นผู้นำส่งเวชระเบียนไปยังห้องต่างๆ ให้แทนผู้ป่วยหรือญาติ หรือในบางแห่งที่ไม่สามารถจัดเจ้าหน้าที่บริการได้ มักจะนำเวชระเบียนใส่ซองมิดชิด เพื่อป้องกันที่ไม่เกี่ยวข้องสามารถเข้าถึงบันทึกในเวชระเบียนได้ (สุรชัย ปัญญาพฤทธิ์พงศ์, 2552) ส่วนข้อมูลเวชระเบียนในรูปแบบอิเล็กทรอนิกส์ซึ่งจัดเก็บในระบบสารสนเทศของโรงพยาบาลนั้น จะรักษาความลับของข้อมูลผู้ป่วยโดยการกำหนดสิทธิการเข้าถึงข้อมูลได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นโดยการกำหนดสิทธิในบัญชีผู้ใช้ (Account) ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล และเก็บรายละเอียดการบันทึก แก้ไข ว่ากระทำโดยบัญชีผู้ใช้ใด เพื่อให้สามารถติดตามย้อนหลังได้ โดยต้องกำหนดนโยบายไม่ให้เจ้าหน้าที่ของโรงพยาบาลใช้งานบัญชีผู้ใช้ร่วมกัน

กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เป็นองค์กรที่นำระบบสารสนเทศมาใช้ในการบริหารจัดการข้อมูลสารสนเทศและแลกเปลี่ยนสารสนเทศระหว่างกลุ่มเครือข่ายบริการสุขภาพ ประกอบด้วยโรงพยาบาลชุมชน 1 แห่ง คือ โรงพยาบาลโคกศรีสุพรรณ และโรงพยาบาลส่งเสริมสุขภาพตำบล 5 แห่ง คือ โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา มีหน้าที่รับผิดชอบบริการด้านการแพทย์ให้กับประชาชนในอำเภอโคกศรีสุพรรณ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ ได้ประยุกต์ใช้ระบบสารสนเทศเพื่อให้บริการแก่ประชาชนโดยการนำระบบ HOSxP สำหรับให้บริการในโรงพยาบาลชุมชน และ HOSxP PCU สำหรับให้บริการในโรงพยาบาลส่งเสริมสุขภาพตำบล โดยระบบ HOSxP และ HOSxP PCU เป็นระบบเวช–ระเบียนและยา การใช้งานระบบ HOSxP ครอบคลุมตั้งแต่ระบบคิว ระบบผู้ป่วยนอก ระบบผู้ป่วยใน รวมถึงระบบห้องตรวจต่างๆ ระบบห้องยา และระบบการออกใบเสร็จ รวมถึงการทำรายงานต่างๆ ส่งให้หน่วยงานต้นสังกัด ดังนั้น ระบบสารสนเทศของโรงพยาบาลจึงมีข้อมูลการรักษาผู้ป่วยเก็บรักษาไว้ ซึ่งข้อมูลผู้ป่วยนี้ได้รับการคุ้มครองตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลด้านสุขภาพ

ของบุคคล คือ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 ที่บัญญัติว่า “ข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใดๆ ผู้ใดจะอาศัยอำนาจ หรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่น เพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้” (สำนักงานคณะกรรมการสุขภาพแห่งชาติ, 2552, หน้า 3) และทางโรงพยาบาลและส่วนเกี่ยวข้องต้องปฏิบัติตามประกาศสิทธิผู้ป่วยซึ่ง แพทยสภา สภาการพยาบาล สภาเภสัชกรรม ทันตแพทยสภา และคณะกรรมการควบคุมการประกอบโรคศิลปะ ได้ร่วมกันประกาศสิทธิของผู้ป่วย เมื่อวันที่ 16 เมษายน 2541 ในข้อ 7 ผู้ป่วยมีสิทธิที่จะได้รับการปกปิดข้อมูลเกี่ยวกับตนเอง จากผู้ประกอบวิชาชีพด้านสุขภาพ โดยเคร่งครัด เว้นแต่จะได้รับความยินยอมจากผู้ป่วยหรือการปฏิบัติหน้าที่ตามกฎหมาย กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ มีนโยบายในการเชื่อมโยงข้อมูลการรักษาผู้ป่วยในแต่ละโรงพยาบาลในเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณไว้ด้วยกัน เพื่อใช้งานข้อมูลการรักษาของผู้ป่วยร่วมกัน เป็นการอำนวยความสะดวกแก่ประชาชนผู้รับการรักษา และยังอำนวยความสะดวกต่อบุคลากรทางการแพทย์ที่จะได้รับข้อมูลที่ถูกต้องครบถ้วน และสมบูรณ์ จากการสัมภาษณ์เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร พบว่ายังไม่มีนโยบายในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ มีเพียงการแนะนำการใช้งานคอมพิวเตอร์ให้เกิดความมั่นคงปลอดภัยจากผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายฯ เท่านั้น (ผิน ฮ่มป่า, สัมภาษณ์, 22 มิถุนายน 2558) ส่งผลให้ระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพเสี่ยงต่อภัยคุกคามความมั่นคงปลอดภัยต่างๆ รวมถึงมาตรา 5 มาตรา 7 และมาตรา 8 ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จึงควรมีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขึ้น

จากปัญหาดังกล่าว ผู้วิจัยจึงสนใจที่จะศึกษาวิจัยเกี่ยวกับ การจัดการความมั่นคงปลอดภัยสารสนเทศ โดยเลือกศึกษากลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ในประเด็นการจัดการความมั่นคงปลอดภัยสารสนเทศตามกรอบมาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 อย่างไร และปัจจัยใดบ้างที่ส่งผลต่อความสำเร็จในการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ซึ่งผลการวิจัยครั้งนี้ทำให้ได้องค์ความรู้ใหม่เกี่ยวกับปัจจัยและการจัดการความมั่นคงปลอดภัยสารสนเทศ ที่เหมาะสมกับบริบทของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร และยังสามารถนำผลการวิจัยมาใช้เป็นแนวทางในการปรับปรุงแก้ไขช่องโหว่ ลดความเสี่ยง สามารถให้บริการแก่ประชาชนได้อย่างมีประสิทธิภาพมากที่สุด และสามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในหน่วยงานที่มีลักษณะคล้ายคลึงกัน

คำถามการวิจัย

ในการวิจัยครั้งนี้ผู้วิจัยได้กำหนดคำถามการวิจัย ไว้ดังนี้

1. การจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครเป็นอย่างไร

2. การจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กับกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ แตกต่างกันหรือไม่ อย่างไร

3. ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายโรงพยาบาล บริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เป็นอย่างไร

4. แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายโรงพยาบาล บริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครควรเป็นอย่างไร

ความมุ่งหมายของการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยได้กำหนดความมุ่งหมายของการวิจัย ไว้ดังนี้

1. เพื่อศึกษาบริบทการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

2. เพื่อศึกษาการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กับกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

3. เพื่อศึกษาปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

4. เพื่อพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

ความสำคัญของการวิจัย

1. ด้านวิชาการ

ผลจากการวิจัยทำให้ทราบถึงปัจจัยและแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ที่เหมาะสมกับบริบทของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

2. ด้านการประยุกต์ใช้งาน

สามารถนำความรู้ที่ได้เป็นแนวทางในการปรับปรุงแก้ไข การอุดช่องโหว่ เพื่อให้การจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีประสิทธิภาพและประสิทธิผลมากที่สุด และสามารถนำไปเป็นแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อนำไปประยุกต์ใช้ในองค์กร/หน่วยงานที่มีบริบทคล้ายคลึงกัน

ขอบเขตของการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยเลือกและกำหนดขอบเขตของหน่วยการวิจัย คือ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

กรอบแนวคิดการวิจัย

ในการวิจัยครั้งนี้ผู้วิจัยได้กำหนดกรอบแนวคิดของการวิจัยจากการทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง ประกอบด้วย

1. บริบทกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

2. ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ แบ่งออกเป็น 2 ประเภท ได้แก่ ปัจจัยภายในองค์กร และปัจจัยภายนอกองค์กร โดยปัจจัยภายในองค์กรได้แก่ 1) แผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร 2) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร 3) ฮาร์ดแวร์ 4) ซอฟแวร์ 5) บุคลากร 6) ผู้บริหาร 7) ผู้รับบริการ 8) ข้อมูล และปัจจัยภายนอกองค์กร ได้แก่ กฎหมาย และภัยคุกคามความมั่นคงปลอดภัย

3. มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 ประกอบไปด้วยมาตรการการจัดการความมั่นคงปลอดภัยสารสนเทศ จำนวน 11 หมวด ได้แก่ 1) นโยบายความมั่นคงปลอดภัย 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร 3) การบริหารจัดการทรัพย์สินขององค์กร 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร 7) การควบคุมการเข้าถึง 8) การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร 11) การปฏิบัติตามข้อกำหนด

4. แนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

จากแนวคิดและวรรณกรรมข้างต้น ผู้วิจัยได้พัฒนากรอบแนวคิดในการวิจัย ดังภาพประกอบ 1

ภาพประกอบ 1 กรอบแนวคิดการวิจัย

นิยามศัพท์เฉพาะ

1. ปัจจัยที่มีผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ หมายถึง องค์ประกอบที่มีผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยได้ดังนี้

1.1 ปัจจัยภายในองค์กร หมายถึง องค์ประกอบที่เกิดขึ้นภายในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกอบด้วย 1) แผนงานและ

งบประมาณด้านระบบสารสนเทศขององค์กร 2) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร 3) ฮาร์ดแวร์ 4) ซอฟแวร์ 5) บุคลากร 6) ผู้บริหาร 7) ผู้รับบริการ 8) ข้อมูล

1.2 ปัจจัยภายนอกองค์กร องค์ประกอบที่เกิดขึ้นภายนอกกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกอบด้วย 1) กฎหมาย และ 2) ภัยคุกคามความมั่นคงปลอดภัย

2. มาตรฐานการรักษาความมั่นคงปลอดภัย หมายถึง นโยบาย มาตรการ กระบวนการ แนวปฏิบัติ สำหรับควบคุมให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ ช่วยสร้างความมั่นใจในการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้สามารถดำเนินไปอย่างต่อเนื่อง มีประสิทธิภาพ และเป็นที่ยอมรับ เช่น ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 เป็นต้น

3. ระบบสารสนเทศ หมายถึง โครงสร้างพื้นฐานทางด้านสารสนเทศ ซอฟต์แวร์ที่ให้บริการ บุคลากรผู้ปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และข้อมูลที่ใช้ปฏิบัติงานของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร พัฒนาขึ้นเพื่อใช้ในการให้บริการขององค์กร

4. สารสนเทศ หมายถึง ข้อมูลประวัติผู้ป่วย และข้อมูลการรักษาผู้ป่วยของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่จัดเก็บในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์

5. หน่วยงานของรัฐ หมายถึง กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคลคณะบุคคลหรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐ ไม่ว่าในการใดๆ