**บทเรียนการประชุมวิชาการประจำปี HA National Forum ครั้งที่ 26**

ภายใต้แนวคิด “Compassionate Innovation Shaping the Future of Care
นวัตกรรมที่เปี่ยมไปด้วยความใส่ใจ สร้างมิติใหม่ของการดูแล”

**เรื่อง Digital Technology: How to Enhance Safety for All**

วันศุกร์ที่ 13 มีนาคม 2569 เวลา 08.45 – 10.15 น.

ณ ห้องสัมมนา Sapphire 205-206 ศูนย์การประชุม IMPACT FORUM เมืองทองธานี

**วิทยากรร่วมแลกเปลี่ยนเรียนรู้**

| | |
|---|---|
| *ดร. นพ.นวนรรน ธีระอัมพรพันธุ์* | *คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี* |
| *ผศ. นพ.กฤษณ์ ขวัญเงิน* | *คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่* |
| *ผศ. นพ.อนุแสง จิตสมเกษม* | *ผู้อำนวยการโรงพยาบาลวชิรพยาบาล คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช* |

**ผศ. นพ.อนุแสง จิตสมเกษม** ได้กล่าวถึงภาพรวมของระบบสุขภาพในปัจจุบันว่า มีการนำเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) มาใช้เพิ่มมากขึ้น ทั้งด้านการจัดเก็บข้อมูลผู้ป่วย การวินิจฉัย การรักษา และการบริหารจัดการทางการแพทย์ ทำให้ “ข้อมูลสุขภาพ” กลายเป็นทรัพยากรสำคัญขององค์กรทางการแพทย์ อย่างไรก็ตาม เมื่อระบบต่าง ๆ เชื่อมต่อผ่านเครือข่ายดิจิทัล ความเสี่ยงด้าน cyber security ก็เพิ่มขึ้นตามไปด้วย เช่น การโจมตีทางไซเบอร์ การรั่วไหลของข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือความผิดพลาดจากระบบ AI ซึ่งอาจส่งผลกระทบโดยตรงต่อการรักษาผู้ป่วย ความเชื่อมั่นของผู้รับบริการ และคุณภาพของระบบสุขภาพ ดังนั้น cyber security จึงไม่ใช่เพียงเรื่องของการป้องกันระบบคอมพิวเตอร์ แต่เป็น “พื้นฐานสำคัญของความปลอดภัยในการดูแลผู้ป่วย” โดยองค์กรจำเป็นต้องดำเนินการควบคู่ทั้งด้านการคุ้มครองข้อมูลส่วนบุคคล การบริหารความเสี่ยง การกำกับดูแล AI และการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ภายในองค์กร

แนวคิด “โครงสร้าง 8 มิติ การดูแลผู้ป่วยด้วยดิจิทัล” จึงถูกนำมาใช้เป็นกรอบสำคัญในการพัฒนาระบบสุขภาพดิจิทัล โดยมีเป้าหมายเพื่อให้เกิด “การดูแลที่เหมาะสม ปลอดภัย และได้ผล” สำหรับผู้ป่วย ทั้ง 8 มิติ ประกอบด้วย

**1. วัตถุประสงค์และกลยุทธ์** องค์กรต้องกำหนดเป้าหมายและทิศทางในการใช้เทคโนโลยีดิจิทัลให้ชัดเจน และสอดคล้องกับยุทธศาสตร์การดูแลผู้ป่วยขององค์กร

**2. การปกป้องผู้มีข้อจำกัด** คำนึงถึงกลุ่มผู้ป่วยหรือผู้ใช้งานที่มีข้อจำกัดด้านการเข้าถึงเทคโนโลยี เพื่อไม่ให้เกิดความเหลื่อมล้ำในการรับบริการ

**3. แผนการใช้งานและอบรม** บุคลากรควรได้รับการพัฒนาทักษะด้านดิจิทัลและ AI เพื่อให้สามารถใช้งานระบบได้อย่างถูกต้องและปลอดภัย

**4. การใช้อย่างสมเหตุสมผล** การนำ AI มาใช้ต้องอยู่บนพื้นฐานของจริยธรรม ความจำเป็น และประโยชน์ต่อผู้ป่วย ไม่ใช่ใช้เพื่อทดแทนการตัดสินใจของมนุษย์ทั้งหมด

**5. การควบคุมดูแลตามกฎหมาย** การดำเนินงานต้องสอดคล้องกับกฎหมายและมาตรฐานด้านข้อมูลสุขภาพ รวมถึง PDPA และมาตรฐานความมั่นคงปลอดภัย

**6. การบริหารความเสี่ยง** องค์กรต้องมีระบบประเมินและจัดการความเสี่ยงจากการใช้เทคโนโลยีและ AI ทั้งด้านข้อมูล ระบบ และผลกระทบต่อผู้ป่วย

**7. ผู้เชี่ยวชาญด้านเทคนิค** ควรมีทีมผู้เชี่ยวชาญที่สามารถดูแลระบบดิจิทัล ความปลอดภัยไซเบอร์และการประเมิน AI ได้อย่างเหมาะสม

**8. กำหนดแนวทางหรือมาตรฐานในการใช้ AI ทางการแพทย์** เพื่อให้เกิดความปลอดภัย โปร่งใสและตรวจสอบได้

ประเด็นสำคัญ คือ “ธรรมาภิบาลปัญญาประดิษฐ์ทางการแพทย์” เป็นแนวทางกำกับดูแลการใช้ AI ให้เกิดความปลอดภัย โปร่งใส และมีความรับผิดชอบต่อผลลัพธ์ที่เกิดขึ้น สามารถแบ่งเป็น 2 ส่วนสำคัญ ได้แก่

**1. ความรับผิดชอบเชิงเทคนิค (System/Vendor)** ผู้พัฒนาระบบหรือผู้ให้บริการ AI ต้องรับผิดชอบด้านการทดสอบและตรวจสอบคุณภาพก่อนใช้งาน การตรวจสอบความเอนเอียงของอัลกอริทึม **และ**ความโปร่งใสของข้อมูลที่ใช้ฝึกสอน เพื่อให้มั่นใจว่า AI มีความแม่นยำ น่าเชื่อถือ และไม่ก่อให้เกิดอคติในการรักษา

**2. ความรับผิดชอบทางคลินิก (Hospital/Clinical)** บุคลากรทางการแพทย์และสถานพยาบาลมีหน้าที่ประเมินความเหมาะสมในการใช้งาน AI อธิบายข้อจำกัดของระบบให้ผู้ป่วยเข้าใจ รับผิดชอบต่อผลที่เกิดขึ้น และแก้ไขปัญหาเมื่อเกิดภาวะแทรกซ้อน ซึ่งสะท้อนให้เห็นว่า AI เป็น “เครื่องมือช่วยสนับสนุน” การทำงานของบุคลากรทางการแพทย์ ไม่ใช่ผู้ตัดสินใจแทนทั้งหมด

**ผศ. นพ.กฤษณ์ ขวัญเงิน** กล่าวว่า ทุกองค์กรควรมีผู้ดูแลภาพรวมของระบบ IT เพื่อวางระบบ cyber security ของโรงพยาบาลให้มีประสิทธิภาพ เนื่องจากปัจจุบันโรงพยาบาลแต่ละแห่งไม่สามารถทำงานแยกกันได้ ต้องมีการเชื่อมโยงข้อมูลกับหน่วยงานอื่นร่วมด้วย

นอกจากนี้ โรงพยาบาลจำเป็นต้องมีระบบ software ที่รองรับการทำงานของแพทย์ พยาบาล เภสัชกรและวิชาชีพอื่น ๆ เพราะหากไม่มีระบบพื้นฐานที่ดี การนำ AI มาใช้จะทำได้ยาก ซึ่งความท้าทายสำคัญ คือ เมื่อปรับกระบวนการทำงานของแพทย์ ระบบที่เกี่ยวข้องกับพยาบาลและหน่วยงานอื่นต้องปรับตามไปด้วย ดังนั้น การออกแบบระบบให้ใช้งานง่าย (user friendly) และมี master plan ที่ดีตั้งแต่ต้น จะช่วยให้การดำเนินงานราบรื่นและลดปัญหาในอนาคต

ตัวอย่างของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ในการนำ digital health มาใช้ตามเป้าหมายมาตรฐานความปลอดภัย 3P safety goals สามารถแบ่งได้ดังนี้

**1. ด้าน Patient Safety** เป็นการนำระบบดิจิทัลมาใช้เพื่อช่วยลดความผิดพลาด เพิ่มความแม่นยำและเพิ่มประสิทธิภาพในการดูแลรักษาผู้ป่วย ซึ่งระบบเหล่านี้ช่วยให้การดูแลรักษามีความรวดเร็ว ปลอดภัยและช่วยสนับสนุนการตัดสินใจทางการแพทย์ได้ดียิ่งขึ้น เช่น ระบบ Set OR ผ่าน EMR (I-Viewer) ระบบ e-

Chart Anesthesia Record โปรแกรม E-Pharma Verification ระบบรายงานเหตุเข็มตำของบุคลากรทางการแพทย์ ระบบ 5G Smart Ambulance ประเมินอาการผู้ป่วยหน้างานได้ทันที

**2. ด้าน Personal Safety** การใช้เทคโนโลยีเพื่อดูแลความปลอดภัยของบุคลากร รวมถึงการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสม โดยระบบเหล่านี้ช่วยลดความเสี่ยงในการทำงาน เพิ่มความปลอดภัยของบุคลากร และช่วยให้การประสานงานในการดูแลผู้ป่วยมีความต่อเนื่องมากขึ้น เช่น ระบบจัดการข้อมูลส่วนบุคคล ระบบรายงานการบาดเจ็บจากการทำงานของบุคลากร และระบบการส่งต่อผู้ป่วย

**3. ด้าน People and Social Safety** การนำ digital health มาเพิ่มโอกาสในการเข้าถึงบริการสุขภาพ และสนับสนุนการดูแลสุขภาพของประชาชนอย่างทั่วถึง ช่วยให้ประชาชนสามารถเข้าถึงบริการสุขภาพได้สะดวกมากขึ้น ลดข้อจำกัดด้านเวลาและระยะทาง รวมทั้งช่วยส่งเสริมการดูแลสุขภาพของตนเองได้อย่างต่อเนื่อง เช่น ระบบบริการการแพทย์ทางไกล (telemedicine) ระบบข้อมูลสุขภาพส่วนบุคคล i-Suandok สำหรับดูข้อมูลสุขภาพผ่านโทรศัพท์มือถือ

**ดร.นพ.นวนรรน ธีระอัมพรพันธุ์** นำเสนอกรณีศึกษาที่สะท้อนความสำคัญของ cyber security คือ **เหตุการณ์ ransomware attack โรงพยาบาลสระบุรี** ที่ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ ทำให้ฐานข้อมูลผู้ป่วยถูกล็อก และส่งผลกระทบต่อการให้บริการ เหตุการณ์นี้ทำให้กระทรวงสาธารณสุข ได้แนะนำแนวทาง “3-2-1 backup rule” เพื่อป้องกันข้อมูลสูญหาย ได้แก่

- **เก็บข้อมูล 3 ชุด** ประกอบด้วยข้อมูลต้นฉบับ 1 ชุด และข้อมูลสำรอง 2 ชุด เพื่อลดความเสี่ยงหากอุปกรณ์ใดอุปกรณ์หนึ่งเกิดเสียหาย
- **เก็บข้อมูลที่ต่างกัน 2 ประเภท** เช่น ฮาร์ดดิสก์พกพา แฟลชไดรฟ์ NAS หรือบน Cloud
- **สำรองข้อมูล 1 ชุดไว้นอกระบบ** เช่น เก็บไว้ใน external hard drive ที่ไม่ได้เสียบกับคอมพิวเตอร์ตลอดเวลา เพื่อป้องกันข้อมูลสำรองถูกทำลาย หรือถูกล็อกในกรณีที่เกิดภัยพิบัติหรือถูกแฮกเกอร์โจมตี

หลักสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูล หรือ information security คือ แนวคิด “CIA Triad” ซึ่งเป็นพื้นฐานสำคัญของการดูแลข้อมูลในองค์กร โดยเฉพาะในระบบสุขภาพที่มีข้อมูลผู้ป่วยและข้อมูลทางการแพทย์จำนวนมาก จำเป็นต้องให้ความสำคัญทั้งด้านความปลอดภัย ความถูกต้อง และความพร้อมใช้งานของข้อมูล CIA Triad ประกอบด้วย 3 องค์ประกอบสำคัญ ได้แก่

**1. Confidentiality** การรักษาความลับของข้อมูล ป้องกันไม่ให้ข้อมูลสำคัญถูกเข้าถึง เปิดเผย หรือใช้งานโดยผู้ที่ไม่มีสิทธิ์ องค์กรต้องมีมาตรการควบคุมสิทธิ์การเข้าถึงข้อมูล กำหนดรหัสผ่านที่ปลอดภัย และดูแลการใช้งานระบบอย่างเหมาะสม เพื่อป้องกันข้อมูลรั่วไหลและสร้างความเชื่อมั่นให้แก่ผู้รับบริการ

**2. Integrity** การรักษาความถูกต้อง ครบถ้วนของข้อมูล และไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลายโดยมิชอบ

**3. Availability** การทำให้ระบบและข้อมูลสามารถใช้งานได้ตลอดเวลา เช่น ระบบเวชระเบียน ระบบห้องฉุกเฉิน หรือระบบสั่งยา หากระบบล่มหรือไม่สามารถเข้าถึงข้อมูลได้ อาจส่งผลกระทบต่อการดูแลผู้ป่วยโดยตรง

แนวทางสำคัญในการคุ้มครองความเป็นส่วนตัว และความปลอดภัยของข้อมูล มีดังนี้

1. การขอ informed consent ก่อนมีการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จากเจ้าของข้อมูลอย่างชัดเจน เพื่อให้ผู้ป่วยรับทราบวัตถุประสงค์ ขอบเขต และสิทธิของตนเองในการใช้ข้อมูล

2. การสร้างวัฒนธรรม ด้าน privacy การปลูกฝังให้บุคลากรทุกระดับตระหนักถึงความสำคัญของข้อมูลผู้ป่วย และถือเป็นความรับผิดชอบร่วมกันในการรักษาความลับ ความปลอดภัยของข้อมูล

3. การสร้างความตระหนักรู้แก่บุคลากร โดยการจัดอบรมและสื่อสารอย่างสม่ำเสมอเกี่ยวกับภัยคุกคามทางไซเบอร์ วิธีป้องกันข้อมูลรั่วไหล และแนวทางการใช้งานระบบอย่างปลอดภัย

4. การกำหนดนโยบายและมาตรการขององค์กร ด้าน cyber security และ privacy ที่ชัดเจน เช่น การกำหนดสิทธิ์เข้าถึงข้อมูล การใช้งานอุปกรณ์ การตั้งรหัสผ่าน และแนวทางปฏิบัติเมื่อเกิดเหตุผิดปกติ เพื่อให้ทุกคนปฏิบัติในมาตรฐานเดียวกัน

5. การติดตาม ประเมิน และประเมินความเสี่ยงอยู่เสมอ เพื่อค้นหาช่องโหว่ ปรับปรุงระบบความปลอดภัยและป้องกันภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้น

6. การอัปเดตโปรแกรมและซอฟต์แวร์อยู่เสมอ และการสร้างความปลอดภัยในระดับผู้ใช้งาน เช่น การตั้งรหัสผ่านที่เหมาะสม การไม่เปิดเผยข้อมูลสำคัญ และการใช้งานอุปกรณ์อย่างระมัดระวัง

ดังนั้น แม้องค์กรจะมีเทคโนโลยีหรือระบบความปลอดภัยที่มีประสิทธิภาพเพียงใด แต่หากบุคลากรขาดความเข้าใจหรือใช้งานอย่างไม่ระมัดระวัง ก็อาจก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยของข้อมูลได้ จึงสะท้อนให้เห็นว่า “คน” ยังคงเป็นปัจจัยสำคัญที่สุดของการรักษาความปลอดภัยทางไซเบอร์ในองค์กร

นอกจากนี้ การรักษาความปลอดภัยไซเบอร์ไม่สามารถอาศัยเพียงความเชื่อหรือการแก้ไขปัญหาเฉพาะหน้าได้ แต่ต้องอาศัยระบบที่เหมาะสม มาตรการที่ชัดเจน และความร่วมมือจากบุคลากรทุกระดับภายในองค์กร เพื่อให้การดูแลข้อมูลและระบบสุขภาพดิจิทัลเป็นไปอย่างปลอดภัย มีประสิทธิภาพ และสร้างความเชื่อมั่นให้แก่ผู้รับบริการอย่างยั่งยืน

**ผู้บันทึกบทเรียน** นายเอกราช จันทรประดิษฐ์
**ผู้ตรวจทานบทเรียน** นายเอกกนก พนาดำรง

งานจัดการความรู้ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
ตึกอำนวยการ ชั้น 1 เลขที่ 2 ถนนวังหลัง แขวงศิริราช เขตบางกอกน้อย กรุงเทพฯ 10700
โทร. 0 2419 9009 หรือ 0 2419 9750
Email: sirirajkm@mahidol.ac.th