**(ร่าง) ประกาศรูปแบบสัญญาประมวลผลข้อมูลของระบบ Health Link**

**(Data Processing Addendum)**

- ประกาศการประมวลผลข้อมูลนี้มีขอบเขตการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการ
- ประกาศนี้ถือเป็นส่วนหนึ่งของบันทึกข้อตกลงความร่วมมือ หรือเอกสารแสดงเจตจำนงในการผูกพันการเข้าร่วมโครงการจัดทำระบบดิจิทัลและเทคโนโลยีแล้วแต่กรณี เพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ (Health Information Exchange: Health Link) การลงลายมือชื่อของคู่สัญญาในบันทึกข้อตกลงความร่วมมือ หรือเอกสารแสดงเจตจำนงในการผูกพันการเข้าร่วมโครงการดังกล่าว ถือว่าคู่สัญญาตกลงผูกพันกันตามประกาศข้อตกลงนี้ด้วย
- ประกาศรูปแบบสัญญาประมวลผลข้อมูลของระบบ Health Link นี้ถูกจัดทำขึ้นเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๐ วรรคสาม

**๑. <u>ความสัมพันธ์ระหว่างคู่สัญญา</u>**

**๑.๑ หน่วยงาน หรือสถานพยาบาลที่เข้าร่วมโครงการจัดทำระบบดิจิทัลและเทคโนโลยีเพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ (Health Information Exchange: Health Link) (“ผู้ควบคุมข้อมูลส่วนบุคคล”)**

หน่วยงาน หรือสถานพยาบาลที่เข้าร่วมโครงการจัดทำระบบดิจิทัลและเทคโนโลยีเพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ (Health Information Exchange: Health Link) จะอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตลอดระยะเวลาของบันทึกข้อตกลงความร่วมมือ โดยผู้ใช้บริการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณี

**๑.๒ สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (“ผู้ประมวลผลข้อมูลส่วนบุคคล”)**

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) จะอยู่ในฐานะของผู้ประมวลข้อมูลส่วนบุคคลตลอดระยะเวลาของบันทึกข้อตกลงความร่วมมือ โดยผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณี

**๒. <u>คำจำกัดความ</u>**

หากไม่ได้มีการกำหนดไว้เป็นอย่างอื่นในสัญญาฉบับนี้และ/หรือในบันทึกข้อตกลงความร่วมมือ ให้ถ้อยคำในสัญญาฉบับนี้มีความหมายดังต่อไปนี้

๒.๑ “**สัญญา**” หมายถึง ประกาศรูปแบบสัญญาประมวลผลข้อมูลของระบบ Health Link ฉบับนี้และเอกสารแนบท้าย

๒.๒ **“สัญญาแบ่งปันข้อมูล”** หมายถึง สัญญาแบ่งปันข้อมูลส่วนบุคคลสำหรับโครงการจัดทำระบบดิจิทัลและเทคโนโลยีเพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ (Health Information Exchange: Health Link)

๒.๓ **“บุคลากร”** หมายถึง บุคคลธรรมดาต่าง ๆ ซึ่งอยู่ภายใต้ความควบคุมดูแลหรือทำงานให้กับผู้ประมวลผลข้อมูลส่วนบุคคล โดยไม่คำนึงถึงสถานการณ์ว่าจ้าง ตำแหน่ง ค่าตอบแทน เช่น เจ้าหน้าที่ ผู้แทน พนักงาน ลูกจ้าง อาสาสมัคร เด็กฝึกงาน

๒.๔ **“ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง”** หมายถึง บุคคลที่สามหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายอื่นที่เข้ามาดำเนินการประมวลผลข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือบางส่วน ภายใต้ขอบเขต ข้อตกลง ข้อกำหนด และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล

๒.๕ **“การรั่วไหลของข้อมูลส่วนบุคคล”** หมายถึง การรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๒.๖ **“แพทย์”** หมายความถึง แพทย์ ทันตแพทย์ เภสัชกร บุคลากรทางการแพทย์หรือผู้ประกอบวิชาชีพตามพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ และที่แก้ไขเพิ่มเติม ที่ได้รับมอบหมายโดยสถานพยาบาลที่เข้าร่วมโครงการฯ ตามข้อมูลทะเบียนของสถานพยาบาลที่เข้าร่วมโครงการฯ

หากมีปัญหาการตีความของคำจำกัดความใด ๆ ข้างต้นที่กำหนดนิยามไว้ ให้ตีความให้สอดคล้องไปตามนิยามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดเป็นสำคัญ ทั้งนี้ เว้นแต่ได้กำหนดนิยามไว้ในบันทึกข้อตกลงความร่วมมือหรือสัญญาแบ่งปันข้อมูล ให้พิจารณานิยามตามบันทึกข้อตกลงความร่วมมือหรือสัญญาดังกล่าวประกอบด้วย

คำจำกัดความใด ๆ ที่ไม่ได้กำหนดนิยามไว้ในสัญญาฉบับนี้ สัญญาแบ่งปันข้อมูลและบันทึกข้อตกลงความร่วมมือ ให้ตีความเป็นไปตามนิยามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ เว้นแต่กรณีได้กำหนดไว้ชัดแจ้งว่าถ้อยคำส่วนดังกล่าวให้หมายถึงนิยามตามกฎหมายอื่น ให้ตีความเป็นไปตามกฎหมายดังกล่าว

## ๓. <u>ขอบเขตการบังคับใช้</u>

๓.๑ สัญญาฉบับนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลอันเป็นการกระทำตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลภายใต้ขอบเขตการประมวลผลข้อมูลส่วนบุคคลตามบันทึกข้อตกลงความร่วมมือและให้ถือว่าสัญญานี้เป็นส่วนหนึ่งของบันทึกข้อตกลงความร่วมมือ หรือเอกสารแสดงเจตจำนง แล้วแต่กรณี

๓.๒ หน่วยงาน หรือสถานพยาบาลที่เข้าร่วมโครงการฯ ยอมรับว่า เพื่อวัตถุประสงค์ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หน่วยงานหรือสถานพยาบาลที่เข้าร่วมโครงการฯ อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลมีฐานะผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลหรือผู้ควบคุมข้อมูลส่วนบุคคล

๓.๓ ในการดำเนินการที่เกี่ยวข้องกับบันทึกข้อตกลงความร่วมมือส่วนใด หากผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนดังกล่าว ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณีนั้นๆ

๓.๔ กรณีมีข้อตกลงข้อใดระหว่างสัญญาฉบับนี้ และบันทึกข้อตกลงความร่วมมือหรือข้อกำหนดใด มีการขัดหรือแย้งหรือไม่ชัดเจนในส่วนที่เป็นการกำหนดหน้าที่ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล ให้ถือตามข้อตกลงในสัญญาฉบับนี้

**๔. <u>การประมวลผลข้อมูลส่วนบุคคล</u>**

๔.๑ ลักษณะและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคล ประเภทของเจ้าของข้อมูลส่วนบุคคล การดำเนินการประมวลผลข้อมูล และระยะเวลาในการประมวลผลข้อมูลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการประมวลผลภายใต้บันทึกข้อตกลงความร่วมมือ ให้เป็นไปตามรายละเอียดปรากฏตามเอกสาร **รายละเอียดการประมวลผลข้อมูลส่วนบุคคล <u>เอกสารแนบท้ายประกาศหมายเลข ๑</u>**

๔.๒ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณี รวมถึงการแจ้งและการได้รับความยินยอมตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด และการออกคำสั่งในการประมวลผลข้อมูลส่วนบุคคลต่อผู้ประมวลผลข้อมูลส่วนบุคคล

**๕. <u>หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล</u>**

๕.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลจะทำการประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการดำเนินการภายใต้ข้อตกลงความร่วมมือและเป็นไปตามคำสั่งที่เป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ทำการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นใดหรือที่ไม่เป็นไปตามข้อตกลงในสัญญาฉบับนี้หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลจะแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยพลัน เมื่อผู้ประมวลผลข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลไม่เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๕.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลจะปฏิบัติตามคำร้องขอหรือคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลที่ให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการแก้ไข โอน ลบ หรือประมวลผลข้อมูลส่วนบุคคลในประการอื่น หรือให้ระงับ บรรเทา หรือแก้ไขการประมวลผลข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยพลัน

๕.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเก็บรักษาข้อมูลส่วนบุคคลทั้งหมดเป็นความลับ และจะไม่เปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือสัญญาฉบับนี้ให้อำนาจในการเปิดเผยหรือเป็นการปฏิบัติตามกฎหมาย ในกรณีที่เป็นการประมวลผลหรือเปิดเผยข้อมูลส่วนบุคคลโดยปฏิบัติตามกฎหมาย ตามคำสั่งของศาล ตามคำสั่งของเจ้าพนักงานผู้ปฏิบัติตามกฎหมาย หรือตามคำสั่งของหน่วยงานผู้กำกับดูแลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบล่วงหน้าเป็นลายลักษณ์อักษรถึงข้อกำหนดทางกฎหมายนั้น

๕.๔ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติหน้าที่ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดได้ โดยคำนึงถึงลักษณะของการประมวลผลข้อมูลและข้อมูลที่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบ รวมถึงในเรื่องที่เกี่ยวกับสิทธิของเจ้าของข้อมูล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และการรายงานหรือการปรึกษาต่อหน่วยงานผู้กำกับดูแลผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

**๖. <u>การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ</u>**

ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วงจะไม่ส่งหรือโอน (Transfer) ข้อมูลส่วนบุคคลภายใต้สัญญานี้ไปยังต่างประเทศโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

กรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลแล้ว ผู้ประมวลผลข้อมูลส่วนบุคคล สามารถถ่ายโอนข้อมูลส่วนบุคคลภายใต้สัญญานี้ไปยังต่างประเทศได้ ทั้งนี้ การถ่ายโอนข้อมูลส่วนบุคคลดังกล่าวจะต้องกระทำภายใต้ข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ/หรือตามคำสั่งเป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

**๗. <u>มาตรการคุ้มครองความปลอดภัยของข้อมูล</u>**

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ทั้งมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ตามความเหมาะสม

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมข้างต้นจะต้องคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในบันทึกข้อตกลงความร่วมมือ โดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูล เช่น ความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การละเมิด การโอน และการเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

ทั้งนี้ มาตรการรักษาความปลอดภัยข้างต้นต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และไม่ต่ำกว่ารายละเอียดปรากฏตามเอกสาร **รายละเอียดมาตรการคุ้มครองความปลอดภัยของข้อมูล เอกสารแนบท้ายประกาศ หมายเลข ๒**

**๘. การแจ้งเตือนหากเกิดการรั่วไหลของข้อมูลส่วนบุคคล**

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้ล่วงรู้หรือทราบถึงเหตุแห่งการรั่วไหลของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการดังต่อไปนี้โดยเร็ว ภายในระยะเวลา ๒๔ ชั่วโมง

(ก) ส่งมอบข้อมูลที่จำเป็นแก่ผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างสะดวก โดยข้อมูลเช่นว่านั้น หมายความรวมถึงแต่ไม่จำกัดเฉพาะลักษณะของการรั่วไหลของข้อมูลส่วนบุคคล ประเภทและจำนวนโดยประมาณของบันทึกข้อมูลส่วนบุคคลที่รั่วไหลและเจ้าของข้อมูลดังกล่าว ผลกระทบที่อาจเกิดขึ้นได้จากการรั่วไหลของข้อมูล มาตรการที่ได้ดำเนินการแล้วหรือที่จะเสนอให้ดำเนินการ และมาตรการที่จะเยียวยาผลกระทบที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูลส่วนบุคคลนั้น และ

(ข) ให้ความร่วมมืออย่างเต็มที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล และดำเนินการใด ๆ ตามที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดเพื่อช่วยดำเนินการตรวจสอบ บรรเทา และเยียวยาการรั่วไหลของข้อมูลส่วนบุคคลนั้น

ในการนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่แจ้งการรั่วไหลของข้อมูลส่วนบุคคลแก่บุคคลที่สาม โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลก่อน เว้นแต่กรณีที่เป็นการปฏิบัติตามกฎหมาย

หากมีข้อกำหนดตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือประกาศหรือคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำหนดขั้นตอน ระยะเวลา หรือวิธีการปฏิบัติต่างๆไว้เพิ่มเติมในภายภาคหน้าเพื่อใช้กำหนดรายละเอียดและวิธีการปฏิบัติระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในเรื่องนี้ ให้ยึดถือและปฏิบัติตามกฎหมาย ประกาศหรือคำสั่งดังกล่าวเป็นสำคัญ

**๙. <u>บุคลากรของผู้ประมวลผลข้อมูลส่วนบุคคล</u>**

๙.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับรองว่าจะจำกัดการเข้าถึงข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยให้เข้าถึงได้เฉพาะบุคลากรที่จำเป็นจะต้องรู้และเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องได้เท่าที่จำเป็นสำหรับการปฏิบัติงานเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องเท่านั้น

๙.๒ ผู้ประมวลผลข้อมูลจะดำเนินการใด ๆ ดังต่อไปนี้ เพื่อรับรองว่าบุคลากรของผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งสามารถเข้าถึงข้อมูลส่วนบุคคล

(ก) ได้รับทราบถึงลักษณะที่เป็นความลับของข้อมูลส่วนบุคคลและจะต้องอยู่ภายใต้ข้อกำหนดในการรักษาความลับและข้อจำกัดการใช้อันเกี่ยวกับข้อมูลส่วนบุคคล

(ข) ได้รับการฝึกอบรมเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลและการปฏิบัติหน้าที่ของบุคลากร

(ค) ตระหนักถึงหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลและหน้าที่และความรับผิดชอบของบุคลากรภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

**๑๐. <u>ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง</u>**

๑๐.๑ ภายใต้ที่กำหนดในสัญญานี้ และเพื่อเป็นการสนับสนุน และเป็นประโยชน์ในการดำเนินโครงการฯ ผู้ควบคุมข้อมูลส่วนบุคคลอนุญาตให้ สขญ. จ้าง และ/หรือมอบหมายงานเกี่ยวกับการประมวลข้อมูลส่วนบุคคลตามสัญญานี้ ให้แก่ผู้ประมวลผู้ข้อมูลส่วนบุคคลช่วงดำเนินการแทนได้ ไม่ว่าทั้งหมดหรือบางส่วน

๑๐.๒ การดำเนินการตามข้อ ๙.๑ สขญ. จัดต้องจัดทำความตกลงกับผู้ประมวลผลข้อมูลช่วง โดย สขญ. ต้องกำกับดูแลผู้ประมวลผลข้อมูลส่วนบุคคลช่วง กำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วง จำกัดการเข้าถึงข้อมูลส่วนบุคคลโดยให้เข้าถึงข้อมูลส่วนบุคคลได้เท่าที่จำเป็นภายใต้วัตถุประสงค์ของโครงการฯ และต้องกำหนดการคุ้มครองและการรักษาความปลอดภัยอย่างน้อยในระดับเดียวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามสัญญานี้

๑๐.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลยังคงต้องรับผิดต่อผู้ควบคุมข้อมูลส่วนบุคคล สำหรับการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงตามสัญญาประมวลผลข้อมูลช่วง

**๑๑. <u>การร้องเรียน คำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและบุคคลภายนอก และหนังสือให้ชี้แจง</u>**

๑๑.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีมาตรการทางเทคนิคและในเชิงองค์กรตามที่เหมาะสม และให้ข้อมูลข้างต้นแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยพลันตามที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องการเพื่อช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการในเรื่องดังต่อไปนี้

(ก) คำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

(ข) คำร้องเรียนจากเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(ค) หนังสือให้ชี้แจ้งหรือการประเมินที่ออกให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยเจ้าหน้าที่ผู้มีอำนาจภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑๑.๒ กรณีที่มีเจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูล กรณีที่ได้รับคำร้องเรียน การแจ้งหรือการติดต่อสื่อสารใด ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลไม่ว่าโดยทางตรงหรือทางอ้อม หรือที่เกี่ยวข้องกับการปฏิบัติหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งบุคคลซึ่งผู้ควบคุมข้อมูลส่วนบุคคลในระบบแต่งตั้งมอบหมายเพื่อตัดสินชี้ขาดเกี่ยวกับการดำเนินการตามคำร้องขอฯ คำร้องเรียน หรือคำชี้แจง ภายใน ๒ วัน

๑๑.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ตอบสนองต่อคำร้องเรียน การแจ้ง การติดต่อสื่อสารใด ๆ หรือคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เว้นแต่จะได้รับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคลเป็นลาย

ลักษณ์อักษร ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องให้ความร่วมมือและความช่วยเหลืออย่างเต็มที่ต่อผู้ควบคุมข้อมูลส่วนบุคคลในการตอบสนองต่อคำร้องเรียน การแจ้ง การติดต่อสื่อสารใด ๆ หรือคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยให้ดำเนินการตามแนวทางหรือคำตัดสินซึ่งบุคคลซึ่งผู้ควบคุมข้อมูลส่วนบุคคลในระบบแต่งตั้งมอบหมายเพื่อตัดสินชี้ขาดเกี่ยวกับการดำเนินการตามคำร้องขอฯ คำร้องเรียน หรือคำชี้แจงเป็นผู้กำหนด โดยให้คำนึงถึงระยะเวลาที่กฎหมายกำหนดให้ต้องดำเนินการเป็นสำคัญ

**๑๒. <u>การชดใช้ค่าสินไหมทดแทน</u>**

ในกรณีเกิดความเสียหายแต่ละฝ่ายรับรองว่าหากฝ่ายใดมีความรับผิดใดเกิดขึ้นจากการที่อีกฝ่ายไม่ได้ปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอันตนต้องพึงปฏิบัติและการไม่ปฏิบัติหน้าที่ดังกล่าวทำให้อีกฝ่ายได้รับความเสียหายหรือต้องรับผิดต่อบุคคลใด ฝ่ายดังกล่าวจะชดใช้ต่ออีกฝ่ายตามความเสียหายที่เกิดขึ้น

**๑๓. <u>ระยะเวลาและการสิ้นสุดสัญญา</u>**

๑๓.๑ สัญญาฉบับนี้มีผลใช้บังคับตราบที่

(ก) บันทึกข้อตกลงความร่วมมือยังมีผลใช้บังคับ หรือการแสดงเจตจำนงตามเอกสารแสดงเจตจำนงยังคงมีผลใช้บังคับ หรือ

(ข) ผู้ประมวลผลข้อมูลส่วนบุคคล ยังคงประมวลผลหรือเก็บรักษาข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับตามข้อกำหนดและเงื่อนไขการใช้บริการ ระบบดิจิทัลและเทคโนโลยีเพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ (Health Information Exchange: Health Link) ไว้ในความครอบครองหรือการควบคุม

๑๓.๒ ข้อกำหนดใด ๆ ภายใต้สัญญาฉบับนี้ไม่ว่าจะได้ระบุโดยชัดแจ้งหรือโดยนัย ซึ่งควรมีผลใช้บังคับหรือยังคงมีผลใช้บังคับต่อไปถึงแม้ว่าบันทึกข้อตกลงความร่วมมือ หรือการแสดงเจตจำนงตามเอกสารแสดงเจตจำนง สิ้นสุดลงแล้ว เพื่อคุ้มครองข้อมูลส่วนบุคคลให้มีผลใช้บังคับต่อไป

๑๓.๓ ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมีการแก้ไขเปลี่ยนแปลงอันส่งผลต่อการปฏิบัติหน้าที่ตามบันทึกข้อตกลงความร่วมมือ หรือเอกสารแสดงเจตจำนง ไม่ว่าทั้งหมดหรือแต่บางส่วนก็ดี ทั้งสองฝ่ายตกลงปฏิบัติตามกฎหมายที่มีการแก้ไขอย่างเคร่งครัด เว้นแต่กฎหมายดังกล่าวมีการแก้ไขจนถึงขนาดที่

ทำให้ไม่สามารถดำเนินการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่แก้ไขได้ ฝ่ายหนึ่งฝ่ายใดสามารถบอกเลิกบันทึกข้อตกลงความร่วมมือได้ โดยแจ้งเป็นลายลักษณ์อักษรพร้อมทั้งเหตุผลกรณีที่ไม่สามารถปฏิบัติตามกฎหมายดังกล่าวได้โดยชัดแจ้งให้อีกฝ่ายหนึ่งทราบล่วงหน้าไม่น้อยกว่า ๙๐ วัน

**๑๔.<u>การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อสิ้นสุดสัญญา</u>**

ในกรณีที่บันทึกข้อตกลงความร่วมมือสิ้นสุดลงไม่ว่าด้วยเหตุใดก็ตาม ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการโดยอย่างปลอดภัยในการลบหรือทำลายข้อมูลส่วนบุคคลทั้งหมดซึ่งเกี่ยวข้องกับบันทึกข้อตกลงความร่วมมือที่อยู่ในความครอบครองหรือการควบคุมของผู้ประมวลผลข้อมูลส่วนบุคคล โดยต้องดำเนินการตามมาตรฐานความปลอดภัยที่เหมาะสม

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการดังกล่าวหลังจาก ๙๐ วัน นับตั้งแต่วันที่สัญญาสิ้นสุดลง ทั้งนี้ เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลมิให้สูญเสียข้อมูลส่วนบุคคลของตนไปโดยอุบัติเหตุเพราะเหตุที่สัญญาสิ้นสุดลง ทั้งนี้ จะต้องดำเนินการดังกล่าวให้เสร็จสิ้นภายใน ๗ วัน หลังจากพ้นระยะเวลาดังกล่าวแล้ว

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องรับรองเป็นลายลักษณ์อักษรว่าได้ดำเนินการทำลายข้อมูลส่วนบุคคลภายใน ๗ วัน นับแต่วันที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้ลบหรือทำลายข้อมูลส่วนบุคคลเสร็จสิ้นแล้ว

ผู้ประมวลผลข้อมูลส่วนบุคคลอาจยกเว้นการปฏิบัติตามข้อกำหนดข้างต้นได้ได้เฉพาะในกรณีดังต่อไปนี้

(ก) มีความจำเป็นที่จะต้องเก็บข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการตรวจสอบหรือปฏิบัติตามกฎหมาย กฎ หรือคำสั่งของหน่วยงานที่มีอำนาจควบคุมหรือหน่วยงานราชการที่มีผลใช้บังคับ

ในกรณีที่มีกฎหมาย กฎ ระเบียบ หรือคำสั่งของหน่วยงานผู้กำกับดูแลหรือหน่วยงานราชการกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเก็บข้อมูลหรือเอกสารที่มีข้อมูลส่วนบุคคลซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องลบหรือทำลายดังกล่าวข้างต้นนั้น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษรให้ทราบถึงข้อกำหนดในการเก็บดังกล่าว ให้รายละเอียดของข้อมูลและเอกสารที่ต้องเก็บ ข้อกำหนดให้เก็บรักษาข้อมูลตามกฎหมายและกำหนดระยะเวลาในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อข้อกำหนดในการเก็บข้างต้นสิ้นสุดลง

(ข) มีความจำเป็นที่จะต้องเก็บข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถเก็บข้อมูลส่วนบุคคลเฉพาะส่วนเท่าที่จำเป็นต่อวัตถุประสงค์การดำเนินการดังกล่าวเท่านั้น

**๑๕. <u>การบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล</u>**

๑๕.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลภายใต้สัญญาฉบับนี้ให้เป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ และจะต้องดำเนินการให้บันทึกดังกล่าวนั้นถูกต้องและเป็นปัจจุบัน (“บันทึกการประมวลผลข้อมูล”)

๑๕.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการให้เป็นที่แน่ใจว่าบันทึกการประมวลผลข้อมูลนั้นมีรายละเอียดข้อมูลเพียงพอที่จะทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตรวจสอบได้ว่าผู้ประมวลผลข้อมูลส่วนบุคคลได้ปฏิบัติหน้าที่ตามข้อกำหนดของสัญญาฉบับนี้ และผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องนำส่งสำเนาบันทึกการประมวลผลข้อมูลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลตามที่ผู้ควบคุมข้อมูลส่วนบุคคลร้องขอ

๑๕.๓ บันทึกรายการประมวลผลข้อมูลจะต้องมีรายการอย่างน้อยประกอบด้วย ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล รายละเอียดของผู้ประมวลผลข้อมูลส่วนบุคคลช่วง วัตถุประสงค์ของการประมวลผลข้อมูล ประเภทของการประมวลผลข้อมูล การเข้าถึง การควบคุม และการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การโอนข้อมูลส่วนบุคคลไปต่างประเทศ การรักษาความปลอดภัย และคำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย ทั้งนี้ ต้องจัดทำให้เป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

**๑๖. <u>การตรวจสอบ</u>**

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องอนุญาตและอำนวยความสะดวก รวมถึงให้ความช่วยเหลือสนับสนุนการตรวจสอบ (audit) ของผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือหน่วยงานตรวจสอบอื่น ๆ ที่อาจมีขึ้นอันเกี่ยวเนื่องกับความปลอดภัยของข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และ/หรือสัญญาฉบับนี้

**๑๗. <u>กฎหมายที่ใช้บังคับ</u>**

สัญญานี้อยู่ภายใต้บังคับและการตีความตามกฎหมายไทย แต่ละฝ่ายตกลงที่จะเสนอข้อพิพาทต่อศาลที่มีเขตอำนาจในประเทศไทยเพื่อระงับข้อพิพาทใด ๆ ที่เกิดจากหรือเกี่ยวกับสัญญาฉบับนี้

ข้าพเจ้าได้อ่านและเข้าใจเนื้อหาของสัญญานี้โดยตลอดแล้ว และเห็นว่าถูกต้องตรงกับเจตนารมณ์ของข้าพเจ้าทุกประการ จึงได้ลงลายมือชื่อและประทับตราสำคัญ (ถ้ามี) ในบันทึกข้อตกลง หรือเอกสารแสดงเจตจำนง แล้วแต่กรณี

**<u>เอกสารแนบท้ายประกาศ หมายเลข ๑</u>**

**รายละเอียดการประมวลผลข้อมูลส่วนบุคคล**

| | |
|---|---|
| **ระยะเวลาการประมวลผลข้อมูลส่วนบุคคล** | ตลอดระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลเข้าร่วมโครงการฯ |
| **ลักษณะและวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล** | การให้บริการระบบสารสนเทศ Health Link เพื่อวัตถุประสงค์ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลประวัติสุขภาพของผู้เข้ารับการรักษาเพื่อให้แพทย์ของหน่วยงานที่อยู่ภายในโครงการฯเรียกดูประกอบการรักษาพยาบาล |
| **ประเภทของข้อมูลส่วนบุคคล** | **ข้อมูลส่วนบุคคลทั่วไป**<br>- ข้อมูลส่วนตัว ชื่อ ข้อมูลการติดต่อ เช่น คำนำหน้า ชื่อ-นามสกุล เลขที่บัตรประจำตัวประชาชน วันเดือนปีเกิด หมายเลขโทรศัพท์มือถือ อีเมล ที่อยู่ เพศ อายุ ข้อมูลผู้ติดต่อ ข้อมูลระดับมาตรฐานการยืนยันตัวตน (IAL) ข้อมูลผู้สมัครรายวัน ข้อมูลหน่วยงาน ข้อมูลประวัติการทำงาน ข้อมูลสถิติรายวัน เป็นต้น<br>- ข้อมูลสถานะการให้ความยินยอม เช่น ข้อมูลการแสดงและเพิกถอนความยินยอมเข้าร่วมโครงการฯ ข้อมูลการแสดงและเพิกถอนความยินยอมให้สถานพยาบาลนำข้อมูลเข้าสู่ระบบฯ ช่องทางการจัดการความยินยอม รหัสสถานพยาบาลที่แสดงความยินยอม (ถ้ามี) ชื่อสถานพยาบาลที่แสดงความยินยอม (ถ้ามี) สถานะการพิมพ์แบบฟอร์มความยินยอม (ถ้ามี) สถานะระบุว่าดำเนินการโดยผู้มีอำนาจกระทำแทนหรือไม่ (ถ้ามี) เป็นต้น<br>**ข้อมูลส่วนบุคคลอ่อนไหว**<br>- ข้อมูลสุขภาพ เช่น ข้อมูลเพศ ข้อมูลการแพ้ ข้อมูลโรคประจำตัว ข้อมูลอาการของผู้ป่วย ข้อมูลโรควินิจฉัย ข้อมูลการจ่ายยา ข้อมูลวัคซีนที่เคยได้รับ ข้อมูลหัตถการ ข้อมูลตรวจสุขภาพ ข้อมูล |

| | |
|---|---|
| | - ค่าผลตรวจทางการแพทย์ ข้อมูลสัญญาณชีพ ข้อมูลผลตรวจห้องปฏิบัติการ ข้อมูลการตรวจทางพยาธิวิทยา ข้อมูลผลสรุปภาพถ่ายทางการแพทย์ ข้อมูลการเข้ารับบริการทางการแพทย์ ข้อมูลจิตเวช ข้อมูลพันธุกรรม ข้อมูลโรคติดเชื้อเอชไอวี (HIV) หรือโรคเอดส์ (AIDS) ข้อมูลโรคติดต่อทางเพศสัมพันธ์ (STDs) ข้อมูลสุขภาพประกอบคดีความ เป็นต้น |
| **กลุ่มหรือประเภทของเจ้าของข้อมูลส่วนบุคคล** | ผู้เข้ารับการรักษาซึ่งมีประวัติอยู่ ณ สถานพยาบาลหรือหน่วยงานที่เข้าร่วมโครงการและถูกส่งข้อมูลเข้าระบบ Health Link |
| **ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล** | ตลอดระยะเวลาที่บันทึกข้อตกลงความร่วมมือมีผลบังคับใช้ จนถึงระยะเวลาไม่ต่ำกว่า ๙๐ วันหลังจากบันทึกข้อตกลงความร่วมมือดังกล่าวสิ้นสุด |
| **ที่มาข้อมูล** | หน่วยงานที่เข้าร่วมโครงการ |
| **ผู้มีสิทธิเข้าถึงข้อมูล** | แพทย์และบุคลากรที่เกี่ยวข้องของหน่วยงานที่เข้าร่วมโครงการ |

**<u>หน้าที่ในการประมวลผลข้อมูล</u>**

**๑. การประมวลผลข้อมูลของผู้เข้ารับการรักษาพยาบาลบนระบบ Health Link**

สขญ. มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลของผู้เข้ารับการรักษาพยาบาล เพื่อให้สถานพยาบาลที่เข้าร่วมโครงการฯ และหน่วยงานที่เกี่ยวข้องที่มีอำนาจ สามารถดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กระทำได้

หากการประมวลผลข้อมูลส่วนบุคคลของผู้เข้ารับการรักษาพยาบาลในระบบ Health Link ใช้ฐานการประมวลผลตาม มาตรา ๒๔ วรรคหนึ่ง ความยินยอม หรือ มาตรา ๒๖ วรรคหนึ่ง ความยินยอมโดยชัดแจ้งแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สขญ. จะต้องจัดให้มีช่องทางเพื่อให้ผู้เข้ารับการรักษาพยาบาลสามารถแสดงความยินยอมเข้าร่วมโครงการฯ จัดการความยินยอมให้สถานพยาบาลที่เข้าร่วมโครงการฯ นำส่งข้อมูลส่วนบุคคลเข้าสู่ระบบ Health Link และถอนความยินยอมออกจากโครงการฯ รวมถึงจัดให้มีการยืนยันและพิสูจน์ตัวตน โดยที่ สขญ. สามารถร่วมมือกับบุคคลที่สาม เช่น ธนาคารกรุงไทย และ/หรือบุคคลที่เกี่ยวข้องในฐานะตัวแทนของสถานพยาบาลที่เข้าร่วมโครงการฯ เพื่อปฏิบัติหน้าที่ตามสัญญาฉบับนี้ ทั้งนี้ ในกรณีที่

สถานพยาบาลที่เข้าร่วมโครงการฯ จะดำเนินการในกิจกรรมใดภายใต้หน้าที่ของ สขญ. สถานพยาบาลที่เข้าร่วมโครงการฯ ตกลงจะปฏิบัติตามมาตรฐานที่ สขญ. กำหนด

สขญ. มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลของผู้เข้ารับการรักษาพยาบาลเพื่อวัตถุประสงค์ ดังนี้

- เพื่อให้แพทย์ในสถานพยาบาลที่เข้าร่วมโครงการฯ เรียกดูข้อมูลสุขภาพทางอิเล็กทรอนิกส์เพื่อการรักษาพยาบาล
- เพื่อพัฒนาประสิทธิภาพการให้บริการทางการแพทย์ของสถานพยาบาลที่เข้าร่วมโครงการฯ
- เพื่อให้ประชาชนเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้
- เพื่อพัฒนาประสิทธิภาพและส่งเสริมการให้บริการของโครงการฯ
- เพื่อปฏิบัติตามเงื่อนไขการให้บริการของโครงการฯ
- เพื่อเชื่อมโยงกับแอปพลิเคชันหรือกิจกรรมอื่น ๆ อันจะเป็นประโยชน์แก่สาธารณสุขโดยรวม
- เพื่อพัฒนาความปลอดภัยของเครือข่ายและข้อมูล
- เพื่อปฏิบัติตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายฉบับอื่น บัญญัติให้กระทำได้

สขญ. จะเรียกดึงข้อมูลสุขภาพของผู้เข้ารับการรักษาพยาบาลแต่ละรายจากสถานพยาบาลที่เข้าร่วมโครงการฯ เมื่อมีการใช้งานข้อมูลสุขภาพของผู้เข้ารับบริการการรักษาพยาบาลรายนั้น ๆ บนระบบ Health Link เท่านั้น และจัดเก็บข้อมูลสุขภาพดังกล่าวไว้ในระบบ Health Link ชั่วคราวตามระยะเวลาเท่าที่จำเป็น เว้นแต่สถานพยาบาลที่เข้าร่วมโครงการฯ กำหนดเป็นอย่างอื่น โดยสขญ. สามารถจัดเก็บข้อมูลส่วนบุคคลบางส่วนเกินระยะเวลาชั่วคราวข้างต้นตามความเหมาะสมเพื่อประสิทธิภาพการทำงานของระบบ Health Link

**๒. การประมวลผลข้อมูลแพทย์และผู้ดูแลระบบ Health Link ฝั่งสถานพยาบาล**

สขญ. มีหน้าที่ประมวลผลข้อมูลของแพทย์และผู้ดูแลระบบ Health Link ฝั่งสถานพยาบาล เพื่อให้ผู้ใช้ดังกล่าวสามารถใช้ระบบ Health Link ได้ตามวัตถุประสงค์ของโครงการฯ หรือตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กระทำได้ โดยที่ สขญ. อาจถือเป็นผู้ควบคุมข้อมูลส่วนบุคคลของข้อมูลบางส่วนของแพทย์และผู้ดูแลระบบ Health Link ฝั่งสถานพยาบาล เมื่อผู้ใช้ดังกล่าวได้ยอมรับและตกลงที่จะปฏิบัติตามข้อกำหนดและเงื่อนไขการใช้บริการของระบบ Health Link

สขญ. จะต้องระบุ พิสูจน์ และยืนยันตัวตนของแพทย์ โดยที่ สขญ. สามารถร่วมมือกับบุคคลที่สาม เช่น แพทยสภา และ/หรือบุคคลอื่นที่เกี่ยวข้องในฐานะตัวแทนของสถานพยาบาลที่เข้าร่วมโครงการฯ เพื่อปฏิบัติหน้าที่ตามสัญญาฉบับนี้

ภายใต้คำสั่งของสถานพยาบาลที่เข้าร่วมโครงการฯ ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล สขญ. มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลของแพทย์และผู้ดูแลระบบ Health Link ฝั่งสถานพยาบาลเพื่อวัตถุประสงค์ ดังนี้

- เพื่อพัฒนาประสิทธิภาพการให้บริการทางการแพทย์ของสถานพยาบาลที่เข้าร่วมโครงการฯ
- เพื่อควบคุมคุณภาพและเพิ่มประสิทธิภาพของบริการระบบ Health Link
- เพื่อพัฒนา Health Link ตามที่สถานพยาบาลที่เข้าร่วมโครงการฯ กำหนด
- เพื่อปฏิบัติตามเงื่อนไขการให้บริการของโครงการฯ
- เพื่อความปลอดภัยของเครือข่ายและข้อมูล

**๓. การออกแบบ พัฒนา และทดสอบระบบ Health Link**

สขญ. มีหน้าที่เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นตามตารางด้านบนจากสถานพยาบาลที่เข้าร่วมโครงการฯ เพื่อออกแบบ พัฒนา และทดสอบระบบ Health Link กับสถานพยาบาลที่เข้าร่วมโครงการฯ และหน่วยงานอื่นใดที่มีการตกลงร่วมกัน โดย สขญ. มีหน้าที่จัดให้เจ้าของข้อมูลส่วนบุคคลในกิจกรรมดังกล่าว แสดงความยินยอมให้สถานพยาบาลที่เข้าร่วมโครงการฯ เพิ่มจากข้อ ๑ เพื่อออกแบบ พัฒนา และทดสอบระบบ Health Link เว้นแต่ สถานพยาบาลที่เข้าร่วมโครงการฯ มีส่วนร่วมในการประมวลผลข้อมูลในกิจกรรมข้างต้นโดยตรง หรือสถานพยาบาลที่เข้าร่วมโครงการฯ มอบหมายให้ สขญ. สามารถดำเนินการประมวลผลข้อมูลได้โดยไม่ต้องให้เจ้าของข้อมูลส่วนบุคคลแสดงความยินยอมก่อน

สถานพยาบาลที่เข้าร่วมโครงการฯ มีหน้าที่รับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเพียงผู้เดียวสำหรับข้อมูลส่วนบุคคลและการประมวลผลข้อมูลส่วนบุคคลของสถานพยาบาลที่เข้าร่วมโครงการฯ ที่อยู่นอกขอบเขตการจัดการควบคุมดูแลของสถานพยาบาลที่เข้าร่วมโครงการฯ อาทิ การจัดเตรียม เรียกดึง คัดกรอง แปลง นำส่ง ตรวจสอบข้อมูลที่เชื่อมเข้าสู่ระบบ Health Link จากสถานพยาบาลที่เข้าร่วมโครงการฯ หรือกิจกรรมอื่นๆ ที่เกี่ยวข้อง ตามบันทึกข้อตกลงความร่วมมือ โดย สขญ. มีหน้าที่รับผิดชอบในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งกระทำการตามคำสั่งหรือการมอบหมายจากสถานพยาบาลที่เข้าร่วมโครงการฯ เท่านั้น และไม่มีหน้าที่และความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลในหน้าที่ใด ๆ ตามที่สถานพยาบาลที่เข้าร่วมโครงการฯ ได้มอบหมายให้ สขญ. ประมวลผู้ข้อมูลส่วนบุคคลหรือรับผิดชอบแทนตามข้อกำหนดอื่นในสัญญา โดยเฉพาะด้านความรับผิดชอบในการจัดให้มีฐานการประมวลผลข้อมูลส่วนบุคคล และในการจัดให้เจ้าของข้อมูลส่วนบุคคลแสดงความยินยอมในการประมวลผลข้อมูลข้างต้น และการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้อง

ทั้งนี้ สขญ. มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลของผู้เข้ารับการรักษาพยาบาลเพื่อเชื่อมโยงข้อมูลจากสถานพยาบาลที่เข้าร่วมโครงการฯ เข้าสู่ระบบ Health Link ในส่วนที่สถานพยาบาลที่เข้าร่วมโครงการฯ เป็นผู้ควบคุมข้อมูลส่วนบุคคลเพียงผู้เดียว เพื่อการรักษาความปลอดภัยของเครือข่ายและระบบ Health Link และเพื่อการออกแบบ พัฒนา และทดสอบระบบ Health Link

**๔. กิจกรรมอื่น ๆ เพื่อสนับสนุนโครงการฯ**

สขญ. มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลเพื่อให้บริการระบบ Health Link และบริการอื่น ๆ ตามวัตถุประสงค์ของโครงการฯ เช่น การส่งเสริมบริการของโครงการฯ การประชาสัมพันธ์โครงการฯ การนำข้อมูลไปวิเคราะห์ และการนำส่งข้อมูลไปยังหน่วยงานอื่น ๆ เป็นต้น โดยที่ สขญ. สามารถร่วมมือกับบุคคลที่สามในฐานะตัวแทนของสถานพยาบาลที่เข้าร่วมโครงการฯ เพื่อปฏิบัติหน้าที่ตามสัญญาฉบับนี้ ทั้งนี้ สขญ. สามารถนำข้อมูลไปดำเนินการในกิจกรรมอื่นตามที่สัญญาฉบับนี้ หรือตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กระทำได้

สถานพยาบาลที่เข้าร่วมโครงการฯ อาจมอบหมายให้ สขญ. ประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมได้ ภายใต้ขอบเขตที่กฎหมายกำหนด โดย สขญ. จะทำการประมวลผลข้อมูลดังกล่าว ทั้งนี้ จะต้องเป็นกรณีมีความจำเป็นเพื่อให้บริการ หรือเป็นการช่วยให้สถานพยาบาลที่เข้าร่วมโครงการฯ สามารถปฏิบัติหน้าที่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดเท่านั้น โดยการดำเนินการดังกล่าวสถานพยาบาลที่เข้าร่วมโครงการฯ จะต้องทำเป็นลายลักษณ์อักษรเท่านั้น

ในกรณีที่ สขญ. พิจารณาแล้วเห็นว่า การออกคำสั่งตามข้อ ๑ - ๔ นั้นเป็นการออกคำสั่งที่ละเมิดต่อกฎหมาย สขญ. จะทำการแจ้งสถานพยาบาลที่เข้าร่วมโครงการฯ และมีสิทธิปฏิเสธในการดำเนินการกิจกรรมนั้นทันที

**<u>เอกสารแนบท้ายประกาศ หมายเลข ๒</u>**

**รายละเอียดมาตรการคุ้มครองความปลอดภัยของข้อมูล**

กลไกการรักษาความปลอดภัยข้อมูลระบบ Health Link

๑. มีการยืนยันตัวตนของประชาชนและแพทย์

๒. มีการเข้ารหัสข้อมูลระหว่างจัดส่งและในฐานข้อมูลเพื่อปกป้องความลับของข้อมูล

๓. มีการซ่อนตำแหน่งเครื่องแม่ข่าย และตั้งกฎ Firewall เพื่อจำกัดการเข้าถึง โดยป้องกันการโจมตี DDoS

๔. มีการจัดเก็บข้อมูลแยกส่วนและบริการเพื่อจำกัดผลกระทบในกรณีที่ระบบถูกเจาะ

๕. มีการสำรองข้อมูลเพื่อปกป้องต่อ Ransomware และการสูญเสียข้อมูล

๖. มีการใช้ระบบ Cloud NT ซึ่งรองรับมาตรฐาน ISO ๒๗๐๐๑ และมีระดับขั้นต่ำในการใช้งานในระดับ SLA ๙๙.๘%

๗. มีการตรวจสอบความปลอดภัยระบบ รวมถึงมีการ Audit การคุ้มครองข้อมูลส่วนบุคคล

๘. สามารถจำกัดช่วงเวลาการใช้งานของแพทย์

๙. สามารถจำกัดผู้เข้าใช้งานระบบโดยจำกัดวง IP ของผู้ใช้งานของแต่ละสถานพยาบาล

๑๐. มีการตรวจสอบผู้เข้าใช้งานจากข้อมูลอุปกรณ์ของผู้ใช้ (Browser fingerprinting)

๑๑. มีการทดสอบเจาะระบบผ่านทางด้านบุคลากร กระบวนการ และระบบสารสนเทศ โดยเตรียมความพร้อมในการดูแลระบบและการตอบสนองเหตุการณ์ภัยคุกคามไซเบอร์

๑๒. มีการดักจับพฤติกรรมผิดปกติและการระงับการเรียกดึงข้อมูล

๑๓. มีการป้องกันระบบ login และจำกัดจำนวนครั้งการ login ผิด