Logo

คู่สัญญา

บันทึกข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement) (ฉบับวันที่ เมษายน ๒๕๖๗)

โครงการ....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก).....

ระหว่าง

คณะแพทยศาสตร์ กับ....(ชื่อคู่สัญญา).....

ทำที่ .....

วันที่ ..... เดือน ..... พ.ศ. .....

บันทึกข้อตกลงนี้ทำขึ้นระหว่าง

บริษัท/ ห้าง/ ร้าน .....
มีสำนักงานตั้งอยู่ที่ .....
.....
โดย ..... ตำแหน่ง .....
เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้ เรียกว่า “บริษัท” กับ

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ (หรือ โรงพยาบาลมหาราชนครเชียงใหม่) เลขที่ ๑๑๐ ถนนอินทวโรรส ตำบลศรีภูมิ อำเภอเมือง จังหวัดเชียงใหม่ ๕๐๒๐๐ โดย ..... ตำแหน่ง คณบดีคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ เป็นผู้มีอำนาจลงนามผูกพัน ตามหนังสือมอบอำนาจ/ คำสั่งมหาวิทยาลัยเชียงใหม่ที่ ..... ลงวันที่ ..... ซึ่งต่อไปในบันทึกข้อตกลงนี้ เรียกว่า **“คณะฯ”**

ตามที่ทั้งสองฝ่ายได้ทำข้อตกลง ..... ฉบับลงวันที่ ..... ทั้งสองฝ่ายจึงตกลงทำบันทึกข้อตกลงฉบับนี้ โดยให้บันทึกข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาดังกล่าว ดังมีข้อความต่อไปนี้

<u>บทนิยาม</u>

ข้อ ๑ หากไม่ได้มีการกำหนดไว้เป็นอย่างอื่นในข้อตกลงนี้ ให้ถ้อยคำในบันทึกข้อตกลงนี้มีความหมายดังต่อไปนี้

“ข้อมูล (Data)” หมายความว่า สิ่งที่สื่อความหมายให้รู้ข้อความ เรื่องราว ข้อเท็จจริง ความเห็นหรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะจัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง

การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลส่วนบุคคล (personal data)” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“เจ้าของข้อมูลส่วนบุคคล (data subject)” หมายถึง บุคคลธรรมดาซึ่งข้อมูลส่วนบุคคลเป็นข้อมูลเกี่ยวกับผู้นั้น และสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม และให้หมายความรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถด้วย

“การประมวลผลข้อมูล (data processing)” หมายถึง การกระทำอย่างหนึ่งหรือหลายอย่างที่ได้กระทำต่อข้อมูลหรือชุดข้อมูล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ก็ตาม ซึ่งรวมถึงการเก็บรวบรวม (collection) การบันทึก (recording) การจัดระบบ (organization) การจัดโครงสร้าง (structuring) การจัดเก็บหรือเก็บรักษา (storage) การดัดแปลงหรือการเปลี่ยนแปลงแก้ไข (adaptation or alternation) การค้นคืน (retrieval) การปรึกษา (consultation) การใช้ (use) การเปิดเผยโดยการส่งผ่าน การเผยแพร่ หรือการทำให้พร้อมใช้งานโดยวิธีการอื่นใด (disclosure by transmission, dissemination or otherwise making available) การปรับแนวหรือการรวมเข้ากัน (alignment or combination) การจำกัด (restriction) การลบ (erasure) และการทำลาย (destruction)

“การลบ (erasure)” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้น ถูกลบออกจากระบบและไม่อาจกู้คืนได้โดยเจ้าของข้อมูลส่วนบุคคล บริษัทฯ หรือคณะฯ ทั้งนี้ ไม่ว่าในเวลาใดๆ

“ภัยคุกคามทางไซเบอร์ (cyber threat)” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“การบันทึกข้อตกลง” หมายถึง บันทึกข้อตกลงการประมวลผลข้อมูลและเอกสารแนบท้ายบันทึกข้อตกลงนี้ (ถ้ามี)

<u>ขอบเขตการบังคับใช้</u>

ข้อ ๒ บันทึกข้อตกลงนี้ ใช้บังคับการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทฯ และคณะฯ เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม และกำหนดหน้าที่ความรับผิดชอบของคู่สัญญาอย่างเหมาะสม และเพื่อให้การดำเนินการตามข้อตกลง..... เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยบันทึกข้อตกลงนี้ถือเป็นส่วนหนึ่งของข้อตกลง ..... และให้มีผลใช้บังคับ ตั้งแต่วันที่ ..... ถึงวันที่ .....

ความสัมพันธ์ระหว่างคู่สัญญา

ข้อ ๓ ในการประมวลผลข้อมูลส่วนบุคคลตามสัญญาและบันทึกข้อตกลงนี้

คณะฯ จะอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (controller) ตลอดระยะเวลาของสัญญา และมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยคณะฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณี

บริษัทฯ จะอยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (processor) ตลอดเวลาของสัญญา และดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัทฯ และไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคลในขอบเขตของสัญญาและบันทึกข้อตกลงนี้ โดยบริษัทฯ ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับกรณี

การประมวลผลข้อมูลส่วนบุคคล

ข้อ ๔ บริษัทฯ ตระหนักและยอมรับว่า การใช้บริการ ..... ตามข้อตกลง ..... และบันทึกข้อตกลงนี้ ถือเป็นการมีคำสั่งให้บริษัทฯ อาจทำการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้ ไม่ว่าทั้งหมดหรือเพียงบางส่วน เท่าที่จำเป็นเพื่อการดำเนินการตามบันทึกข้อตกลงหรือตามกฎหมาย

- ข้อมูล .....(ระบุข้อมูลที่ใช้ทำการประมวลผล).....
- ข้อมูล .....
- ข้อมูล .....
- ข้อมูล .....
- ข้อมูล .....
- ข้อมูลส่วนบุคคลอื่นที่ได้มีการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามสัญญาและบันทึกข้อตกลงนี้

ข้อ ๕ บริษัทฯ จะทำการประมวลผลข้อมูลส่วนบุคคล ตามข้อ ๔ เพื่อให้บรรลุวัตถุประสงค์ของบันทึกข้อตกลงและกระบวนการอื่นๆ ที่เกี่ยวข้อง ซึ่งรวมถึงกรณีใดกรณีหนึ่งต่อไปนี้

(๑) เมื่อ ..... ซึ่งมีฐานในการประมวลผลข้อมูล ส่วนบุคคลที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลดังในตาราง โดยถือเป็นการที่คณะฯ มีคำสั่งให้บริษัทฯ อาจทำการประมวลผลข้อมูลส่วนบุคคล ตามข้อ ๔ ได้

วัตถุประสงค์	ฐานในการประมวลผลข้อมูลส่วนบุคคล
(ก)	
(ข)	

(๒) เมื่อบุคลากรของคณะฯ ที่มีอำนาจหน้าที่เกี่ยวกับการปฏิบัติตามข้อตกลงได้มีคำสั่งที่ชอบด้วยกฎหมายให้บริษัทฯ ดำเนินการ และเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของข้อตกลง

(๓) เมื่อบริษัทฯ ได้รับคำสั่งที่เป็นลายลักษณ์อักษรจากคณะฯ และเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของสัญญา

(๔) เมื่อบริษัทฯ มีเหตุจำเป็นต้องทำการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามกฎหมาย หรือกรณีอื่นที่สามารถกระทำได้ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยจะต้องแจ้งให้คณะฯ ทราบโดยไม่ชักช้าด้วย

ข้อ ๖ ในกรณีที่บริษัทฯ พิจารณาแล้วเห็นว่า การออกคำสั่งให้ทำการประมวลผลข้อมูลส่วนบุคคลตามข้อ ๕ นั้น เป็นการออกคำสั่งที่ขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรืออยู่นอกเหนือไปจากวัตถุประสงค์ของสัญญา บริษัทฯ จะไม่ทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งนั้น โดยไม่ถือว่าเป็นการกระทำผิดสัญญา หรือบันทึกข้อตกลงนี้ และคณะฯ จะแจ้งให้บริษัทฯ ทราบโดยพลัน

ในกรณีที่บริษัทฯ ทำการประมวลผลข้อมูลส่วนบุคคล ตามข้อ ๕ (๑) (๒) หรือ (๓) และปรากฏข้อเท็จจริงว่าการประมวลผลข้อมูลส่วนบุคคลดังกล่าวขัดต่อกฎหมาย หรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ความรับผิดในความเสียหายหรือการกระทำดังกล่าวให้เป็นไปตามบันทึกข้อตกลงนี้

ข้อ ๗ เพื่อให้บริษัทฯ สามารถทำการประมวลผลข้อมูลส่วนบุคคลตามสัญญาอย่างถูกต้องตามกฎหมาย คณะฯ ตกลงและรับรองว่า ก่อนการเปิดเผยข้อมูลส่วนบุคคลให้แก่บริษัทฯ และก่อนหรือในขณะที่บริษัทฯ จะทำการประมวลผลข้อมูลส่วนบุคคล ตามข้อ ๕ คณะฯ ได้พิจารณาแล้วว่า การประมวลผลข้อมูลส่วนบุคคลดังกล่าว มีฐานในการประมวลผลข้อมูลส่วนบุคคล (lawful basis for processing personal data) ที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และในกรณีที่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล คณะฯ รับรองว่า คณะฯ ได้ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และได้รับความยินยอมโดยชอบด้วยกฎหมายแล้ว ทั้งนี้ เว้นแต่จะเป็นข้อมูลส่วนบุคคลที่คณะฯ ได้เก็บรวบรวมไว้ก่อนวันที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลใช้บังคับ ซึ่งสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม

ข้อ ๘ คณะฯ รับทราบและตกลงที่จะปฏิบัติหน้าที่ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูล ส่วนบุคคลกำหนดให้เป็นหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ตลอดจนหน้าที่ความรับผิดชอบตามกฎหมายอื่น ซึ่งรวมถึง

(๑) การแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล (privacy notice)

(๒) การประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

(๓) การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

(๔) การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

(๕) การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(๖) การดำเนินการที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

(๗) การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็นหรือ เมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

(๘) การดำเนินการเพื่อป้องกันมิให้บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่ผู้นั้น

(๙) การจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่จะเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๑๐) การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ/หรือเจ้าของข้อมูลส่วนบุคคล โดยไม่ชักช้า ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ดำเนินการ

(๑๑) การแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (เฉพาะกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร)

(๑๒) การจัดทำบันทึกรายการ (record of processing activities) เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(๑๓) การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ดำเนินการ

ข้อ ๙ บริษัทฯ รับทราบและตกลงที่จะปฏิบัติหน้าที่ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้เป็นหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล ตลอดจนหน้าที่ความรับผิดชอบตามกฎหมายอื่น ซึ่งรวมถึง

(๑) การดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๒) การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) การจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๔) การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลและสำนักคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ดำเนินการ

ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

ข้อ ๑๐ เพื่อประโยชน์ในการปฏิบัติตามสัญญา เมื่อมีความจำเป็น บริษัทฯ อาจมอบหมายงานเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือแต่บางส่วนให้บุคคลอื่น (“ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง”) ดำเนินการแทนหรือช่วยสนับสนุนในการดำเนินการได้ ทั้งนี้ บริษัทฯ ยังต้องเป็นผู้รับผิดชอบในงานที่ได้มอบหมายไปตามสัญญาและบันทึกข้อตกลงนี้ รวมถึงจะต้องดำเนินการให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงรับทราบและปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และสัญญาและบันทึกข้อตกลงนี้ รวมทั้งจะต้องดำเนินการให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงมีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมในระดับที่ไม่ต่ำกว่าหน้าที่ความรับผิดชอบของคณะฯ ตามบันทึกข้อตกลงนี้

การให้ความร่วมมือในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมาย

ข้อ ๑๑ คณะฯ จะให้ความร่วมมือ ช่วยเหลือ และสนับสนุนให้บริษัทฯ สามารถเข้าถึงข้อมูล ส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลและตอบสนองต่อคำขอของเจ้าของข้อมูลส่วนบุคคลที่เป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้ภายในเวลาอันควร

ข้อ ๑๒ ในกรณีที่บริษัทฯ ได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคลที่เป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล บริษัทฯ ต้องแจ้งให้คณะฯ ทราบและส่งคำขอนั้นต่อไปยังคณะฯ โดยไม่ชักช้า โดยจะไม่ทำการตอบสนองต่อคำขอดังกล่าวเอง เว้นแต่จะมีการตกลงไว้เป็นอย่างอื่น

ข้อ ๑๓ คู่สัญญาจะให้ความร่วมมือ ช่วยเหลือ และสนับสนุนการดำเนินการที่เกี่ยวข้องของคู่สัญญาอีกฝ่ายหนึ่งตามสมควร เพื่อให้ฝ่ายนั้นสามารถปฏิบัติให้เป็นไปตามกฎหมายและพันธกรณีต่างๆ ได้ หรือในกรณีที่มีคำสั่งโดยชอบด้วยกฎหมายจากหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐเกี่ยวกับหน้าที่ของคู่สัญญา หรือเพื่อพิสูจน์ว่าคู่สัญญาได้ปฏิบัติตามที่กฎหมายกำหนดและตามที่กำหนดในสัญญาและบันทึกข้อตกลงนี้ ในส่วนที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล

<u>มาตรการรักษาความมั่นคงปลอดภัย</u>

ข้อ ๑๔ บริษัทฯ มีหน้าที่จัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ สำหรับการประมวลผลข้อมูลส่วนบุคคลตามสัญญาและบันทึกข้อตกลงนี้ โดยจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ข้อ ๑๕ ในการกำหนดมาตรการ ตามข้อ ๑๔ ให้บริษัทฯ คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการดังต่อไปนี้ เท่าที่จำเป็นและเหมาะสมกับบริบท

(๑) **Identify** : การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลทั้งที่เป็นข้อมูลอิเล็กทรอนิกส์และข้อมูลในรูปแบบอื่น ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล ในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

(๒) **Protect** : มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) **Detect** : มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์และเหตุการละเมิดข้อมูลส่วนบุคคล

(๔) **Respond** : มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์หรือเหตุการละเมิดข้อมูลส่วนบุคคล

(๕) **Recover** : มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์หรือเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อ ๑๖ มาตรการป้องกันความเสี่ยงของบริษัทฯ ตามข้อ ๑๕ (๒) ควรประกอบด้วยมาตรการอย่างน้อยดังนี้ ในส่วนที่เกี่ยวกับระบบสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคล เท่าที่จะสามารถจะกระทำได้

(๑) มาตรการรักษาความมั่นคงปลอดภัยด้านการบริหารจัดการ (administrative security) ซึ่งรวมถึงการกำหนดและสื่อสารนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

(๒) มาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพ (physical security) ของอุปกรณ์และส่วนประกอบของระบบสารสนเทศและข้อมูลที่จัดเก็บ

(๓) มาตรการรักษาความมั่นคงปลอดภัยด้านผู้ใช้งาน (user security) ซึ่งรวมถึงการฝึกอบรมและสร้างเสริมความตระหนักรู้และด้านความสำคัญของการคุ้มครองข้อมูลและการรักษาความมั่นคงปลอดภัย (security awareness training) แก่บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่น ที่เป็นผู้ใช้งานหรือผู้ที่เกี่ยวข้องกับระบบสารสนเทศและข้อมูลส่วนบุคคล การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ที่ใช้ในการจัดเก็บและการประมวลผลข้อมูลส่วนบุคคล (access control) การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลหรือระบบสารสนเทศ และการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) โดยคำนึงถึงบทบาทหน้าที่ ความจำเป็นในการใช้งาน และความมั่นคงปลอดภัยเป็นสำคัญ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล หรือการลักขโมยอุปกรณ์ที่ใช้ในการจัดเก็บหรือการประมวลผลข้อมูลส่วนบุคคล และการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล (audit trails) ให้เหมาะสม

(๔) มาตรการรักษาความมั่นคงปลอดภัยด้านข้อมูล (data security) ซึ่งรวมถึงมาตรการควบคุมการเข้าถึงข้อมูลที่เก็บรักษาไว้อย่างเหมาะสม และการสำรองข้อมูล

(๕) มาตรการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ (system security) ซึ่งรวมถึงการปรับปรุงระบบปฏิบัติการและแอปพลิเคชันของเครื่องคอมพิวเตอร์แม่ข่าย (server) ให้เป็นปัจจุบันอยู่เสมอ การตั้งค่าความมั่นคงปลอดภัย (security configurations) ที่เหมาะสม การมีระบบสำรอง และการป้องกันภัยคุกคามจากมัลแวร์

(๖) มาตรการรักษาความมั่นคงปลอดภัยด้านสินทรัพย์สารสนเทศ (asset security) ซึ่งรวมถึงความมั่นคงปลอดภัยทางกายภาพและการปรับปรุงระบบปฏิบัติการและแอปพลิเคชันของเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่างๆ (endpoints) ที่ใช้งานระบบสารสนเทศให้เป็นปัจจุบันอยู่เสมอ และการป้องกันภัยคุกคามจากมัลแวร์

(๗) มาตรการรักษาความมั่นคงปลอดภัยด้านซอฟต์แวร์และแอปพลิเคชัน (software and application security) ซึ่งรวมถึงการออกแบบและทดสอบความมั่นคงปลอดภัยของซอฟต์แวร์และแอปพลิเคชันการประเมินและกำกับดูแลกระบวนการพัฒนาซอฟต์แวร์ (software development process) ที่เหมาะสม โดยคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ไม่ว่าจะเป็นซอฟต์แวร์หรือแอปพลิเคชันที่พัฒนาเอง หรือนำมาใช้จากภายนอก หรือให้บุคคลภายนอกพัฒนาให้ก็ตาม รวมทั้งกระบวนการบำรุงรักษา (maintenance) ซอฟต์แวร์และแอฟพลิเคชันที่เหมาะสม

ข้อ ๑๗ บริษัทฯ จะต้องทบทวนมาตรการตามข้อ ๑๔ ข้อ ๑๕ และข้อ ๑๖ เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงความก้าวหน้าทางเทคโนโลยี ค่าใช้จ่ายในการดำเนินการ ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูลประกอบกัน

ข้อ ๑๘ บริษัทฯ จะใช้ความพยายามตามสมควรให้การเข้าถึงและการประมวลผลข้อมูลส่วนบุคคลจำกัดเฉพาะบุคลากรของบริษัทฯ หรือบุคคลที่ได้รับมอบหมายซึ่งมีความจำเป็นในการเข้าถึง หรือการประมวลผลข้อมูลส่วนบุคคล เพื่อดำเนินการให้เป็นไปตามสัญญา และดำเนินการให้บุคคลดังกล่าวรักษาความลับในการประมวลผลข้อมูลส่วนบุคคล และปฏิบัติตามหน้าที่ความรับผิดชอบของบริษัทฯ ในสัญญาและบันทึกข้อตกลงนี้

ข้อ ๑๙ บริษัทฯ มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ สำหรับการประมวลผลข้อมูลส่วนบุคคลในส่วนที่อยู่นอกเหนือความควบคุมและความรับผิดชอบของบริษัทฯ ตลอดจนการประมวลผลข้อมูลส่วนบุคคลที่บริษัทฯ หรือบุคคลอื่นดำเนินการในนามบริษัทฯ เพื่อเปิดเผยโดยการส่งผ่านการเผยแพร่ หรือการทำให้พร้อมใช้งานโดยวิธีการอื่นใดให้แก่บริษัทฯ ก่อนที่บริษัทฯ จะทำการประมวลผลข้อมูลส่วนบุคคลนั้นในส่วนของตน

<u>การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross-Border Data Transfer)</u>

ข้อ ๒๐ บริษัทฯ จะไม่ส่งหรือโอน (transfer) ข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศ เว้นแต่จะได้รับความยินยอมจากคณะฯ เป็นลายลักษณ์อักษร หรือเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ไม่รวมถึงการส่งผ่าน (transit) ข้อมูลส่วนบุคคลในต่างประเทศ ที่ไม่มีการเข้าถึงข้อมูลส่วนบุคคลโดยบุคคลอื่นนอกเหนือจากบุคลากรหรือพนักงานของบริษัทฯ หรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

<u>เหตุการละเมิดข้อมูลส่วนบุคคล (Personal Data Breaches)</u>

ข้อ ๒๑ บริษัทฯ มีหน้าที่สอดส่องดูแลและมีมาตรการตรวจสอบและเฝ้าระวัง (detective measures) การกระทำที่อาจมีลักษณะเป็นการเข้าถึงหรือการประมวลผลข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดย มิชอบ ตามสมควร และเมื่อทราบเหตุการละเมิดข้อมูลส่วนบุคคล บริษัทฯ มีหน้าที่ตอบสนองต่อเหตุดังกล่าวในเบื้องต้นตามสมควรเพื่อลดความเสี่ยงหรือผลกระทบจากเหตุดังกล่าว ตลอดจนเพื่อรวบรวมข้อมูลจราจรทางคอมพิวเตอร์และพยานหลักฐานที่เกี่ยวข้องสำหรับการดำเนินการต่อไป

ข้อ ๒๒ บริษัทฯ มีหน้าที่แจ้งให้คณะฯ ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในความรับผิดชอบของบริษัทฯ โดยไม่ชักช้า ภายใน ๔๘ (สี่สิบแปด) ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยอย่างน้อยจะต้องให้ข้อมูลต่อไปนี้แก่คณะฯ เป็นลายลักษณ์อักษรโดยเร็วเท่าที่จะสามารถกระทำได้

(๑) รายละเอียดของเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และผลที่อาจเกิดขึ้น

(๒) การดำเนินการที่ได้กระทำไปเพื่อตอบสนองต่อเหตุดังกล่าว

(๓) ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเหตุดังกล่าว (หากเป็นไปได้)

(๔) ความเห็นต่อเหตุดังกล่าวและมาตรการที่ควรดำเนินการต่อไป

ข้อ ๒๓ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ/หรือเจ้าของข้อมูลส่วนบุคคล เป็นหน้าที่ความรับผิดชอบของคณะฯ โดยบริษัทฯ จะต้องให้ความร่วมมือตามสมควรเพื่อให้คณะฯ สามารถดำเนินการต่อไป

ข้อ ๒๔ หลังเกิดเหตุการละเมิดข้อมูลส่วนบุคคล คู่สัญญามีหน้าที่รับผิดชอบดำเนินการในส่วนของตนเพื่อเยียวยาผู้ได้รับผลกระทบจากเหตุดังกล่าว และทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสมและเพียงพอ

<u>การลบและการเก็บรักษาข้อมูลส่วนบุคคล</u>

ข้อ ๒๕ บริษัทฯ มีหน้าที่ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลตามบันทึกข้อตกลงนี้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ภายในเวลา ๕ ปี นับแต่วันที่สัญญาสิ้นสุดลง หรือเมื่อไม่มีความจำเป็นต้องทำการประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากคณะฯ ให้เก็บรักษาข้อมูลดังกล่าวไว้นานกว่านั้น

ข้อ ๒๖ บริษัทฯ อาจเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ที่ไม่ขัดต่อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๒๗ เมื่อสัญญาสิ้นสุดลง หรือก่อนที่บริษัทฯ จะดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลตามบันทึกข้อตกลงนี้ เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ คณะฯ อาจแจ้งให้บริษัทฯ ส่งสำเนาข้อมูลส่วนบุคคลตามบันทึกข้อตกลงนี้ให้แก่คณะฯ ได้ โดยไม่กระทบต่อสิทธิและหน้าที่ของบริษัทฯ ในการเก็บรักษาข้อมูลไว้ตามความจำเป็นตามบันทึกข้อตกลงนี้ โดยหน้าที่ในการปฏิบัติการให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่น ต่อการประมวลผลข้อมูลส่วนบุคคลของข้อมูลส่วนบุคคลที่บริษัทฯ ส่งให้คณะฯ เป็นความรับผิดชอบของคณะฯ เอง

ข้อ ๒๙ เมื่อสัญญาสิ้นสุดลง ในระหว่างที่บริษัทฯ ยังไม่ได้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลตามบันทึกข้อตกลงนี้ เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามข้อ ๒๕ ให้บริษัทฯ ยังมีหน้าที่ความรับผิดชอบตามบันทึกข้อตกลงนี้เท่าที่จำเป็นและไม่ขัดกับกฎหมาย เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทฯ รับผิดชอบในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

<u>ขอบเขตของความรับผิด</u>

ข้อ ๓๐ เว้นแต่จะกำหนดไว้เป็นอย่างอื่น บริษัทฯ ไม่ต้องรับผิดในความเสียหายหรือการกระทำอันเกิดจากการปฏิบัติตามบันทึกข้อตกลงนี้ หรือตามคำสั่งของคณะฯ เพื่อให้บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลตามสัญญา

ข้อ ๓๑ กรณีบริษัทฯ ต้องรับผิดชดใช้ค่าเสียหายหรือชำระค่าปรับ อันเนื่องจากการปฏิบัติตามบันทึกข้อตกลง หรือตามคำสั่งของคณะฯ เพื่อให้บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลตามสัญญา ไม่ว่าจะด้วยเหตุผลใดก็ตาม บริษัทฯ มีสิทธิเรียกร้องให้คณะฯ ชดใช้เงินจำนวนดังกล่าวให้แก่บริษัทฯ เว้นแต่จะพิสูจน์ได้ว่าความรับผิดดังกล่าว เป็นการกระทำผิดโดยเจตนาหรือเป็นความบกพร่องของบริษัทฯ เองหรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วงของบริษัทฯ

<u>การเปลี่ยนแปลงแก้ไขบันทึกข้อตกลง</u>

ข้อ ๓๒ กรณีที่จำเป็นต้องมีการเปลี่ยนแปลงแก้ไขบันทึกข้อตกลงเพื่อให้คู่สัญญาสามารถทำการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อไปได้อย่างเหมาะสมและมีประสิทธิภาพ ให้คู่สัญญาฝ่ายที่ประสงค์จะแก้ไขเพิ่มเติมบันทึกข้อตกลงนี้ แจ้งให้อีกฝ่ายทราบล่วงหน้าเป็นเวลาไม่น้อยกว่า ๓๐ วัน และเมื่อทั้งสองฝ่ายให้ความยินยอมในการแก้ไขเพิ่มเติมแล้ว ให้จัดทำบันทึกข้อตกลงฉบับแก้ไขเพิ่มเติมเป็นหนังสือ และลงนามผูกพันโดยมีผู้มีอำนาจลงนามผูกพันนิติบุคคล และให้ถือว่าการแก้ไขเพิ่มเติมดังกล่าว เป็นส่วนหนึ่งของบันทึกข้อตกลงนี้ โดยให้มีผลใช้บังคับตั้งแต่วันที่ลงนามในบันทึกข้อตกลงฉบับแก้ไขเพิ่มเติมนั้น เว้นแต่จะกำหนดเป็นอย่างอื่นในบันทึกข้อตกลงฉบับแก้ไขดังกล่าว

บันทึกข้อตกลงนี้ทำขึ้นทั้งสองฉบับมีข้อความถูกต้องตรงกัน ทั้งสองฝ่ายได้อ่านและเข้าใจบันทึกข้อตกลงนี้โดยละเอียดตลอดแล้ว เห็นว่าตรงตามเจตนารมณ์ที่ได้ให้ไว้ต่อกันทุกประการ จึงได้ลงลายมือชื่อไว้เป็นสำคัญต่อหน้าพยานและแต่ละฝ่ายต่างได้ยึดถือไว้ฝ่ายละฉบับ

บริษัทฯ ..... คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

ลงชื่อ ..... บริษัทฯ ลงชื่อ ..... คณะฯ

(.....) (.....)

ลงชื่อ ..... พยาน ลงชื่อ ..... พยาน

(.....) (.....)