มหาวิทยาลัยมหิดล
Mahidol University

กระบวนการปกปิดความลับ ความเป็นส่วนตัว และข้อมูลของผู้เข้าร่วมการวิจัย

จรณิต แก้วกังวาล
คณะเวชศาสตร์เขตร้อน

นิยามคำศัพท์
เกี่ยวกับ
ความเป็นส่วนตัวและการปกปิดความลับ

Beyond the HIPAA Privacy Rule; Enhancing Privacy, Improving Health Through Research
Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: National Academies Press (US); 2009.

ความเป็นส่วนตัว = สิทธิของบุคคล

(Privacy) ที่เป็นอิสระจากการถูกแทรกแซง หรือก้าวล่วงโดยบุคคลอื่น

การปกปิดความลับ
(Confidentiality)

= ภาระผูกพัน ของบุคคล หรือ องค์กร
ในการปกป้องข้อมูล (Safeguard) ที่ได้รับมา

= ความสัมพันธ์เชิงความไว้เนื้อเชื่อใจ (Trust relationship)
ระหว่าง นักวิจัย กับ ผู้เข้าร่วมโครงการวิจัย

ความมั่นคงปลอดภัย (Security) = วิธีการ (Measures) ที่ใช้ในการปกป้องข้อมูล

- ด้านกายภาพ (Physical)
- ด้านการบริหารจัดการ (Administrative)
- ด้านเทคนิควิธีการ (Technical)

ข้อมูลที่สามารถระบุตัวบุคคลได้ (Identified data)

ข้อมูลที่สามารถระบุตัวตนได้ทางตรง

(Direct identified information):

- *ข้อมูลพึงปกปิด*

  (Highly restricted information)

  - เลขประจำตัวประชาชน
  - เลขที่ผู้ป่วย

ข้อมูลที่สามารถระบุตัวบุคคลได้ (Identified data)

ข้อมูลที่สามารถระบุตัวตนทางอ้อม

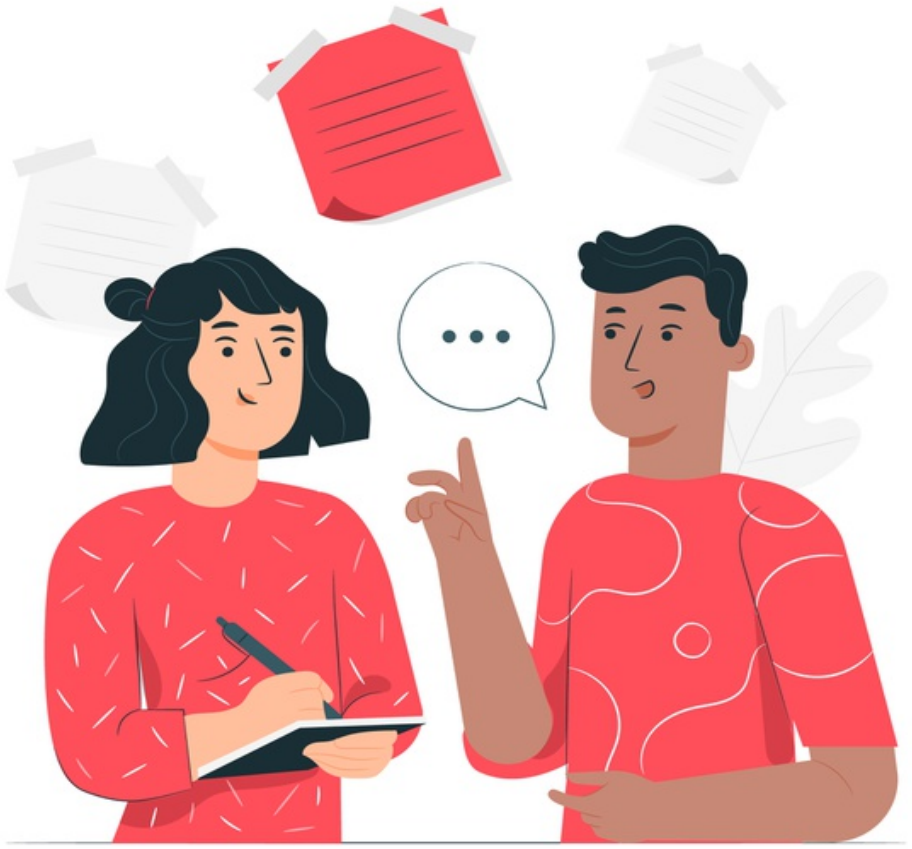
(Indirect identified information):

- *ข้อมูลที่ควรจำกัดในการเปิดเผย*

  (Restricted information)

  - เพศ
  - การศึกษา
  - อาชีพ
  - วัน-เดือน-ปีเกิด

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive personal information)



ข้อมูล ที่อาจมีผลกระทบ

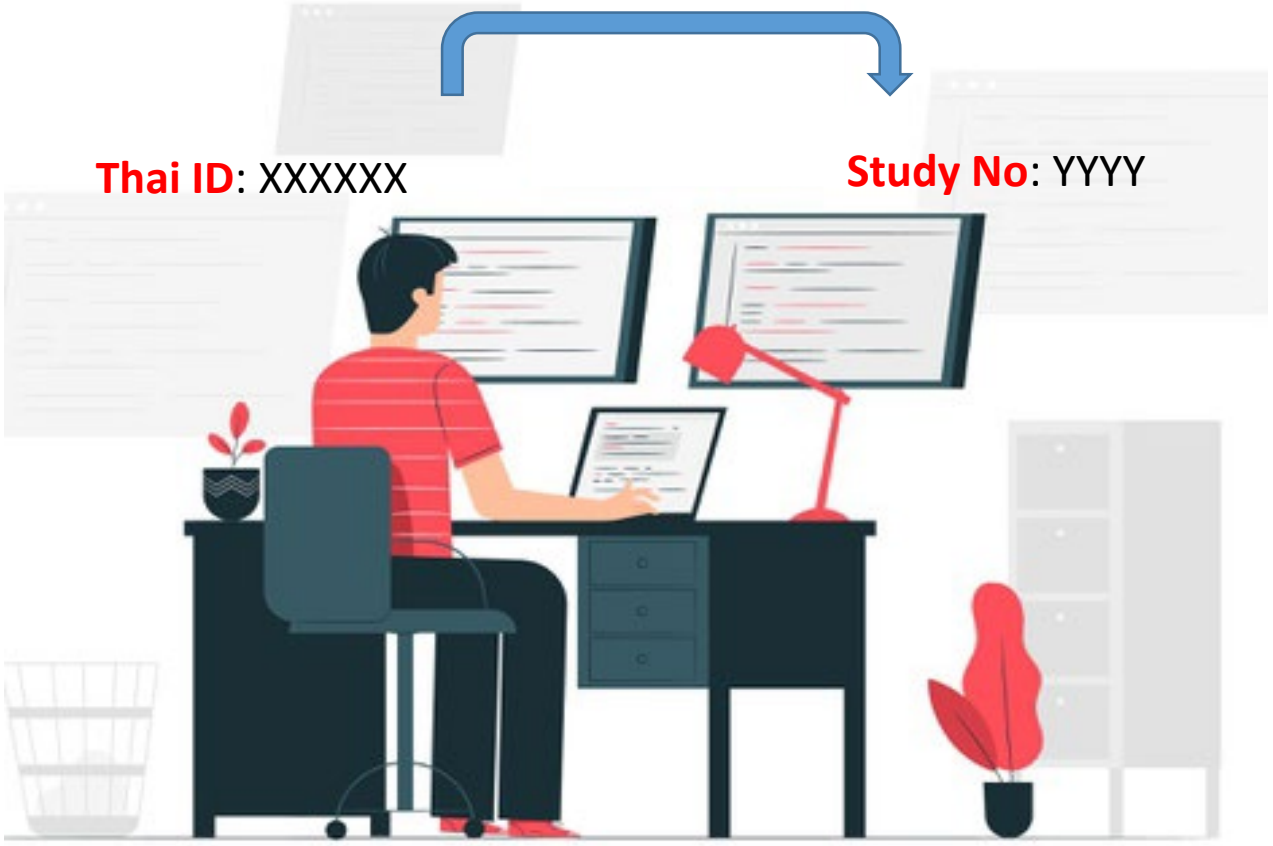
- ด้านโทษภัย (Harm)
- ก่อให้เกิดตราประทับ (Stigmatization)

- ทัศนคติหรือแนวปฏิบัติในเรื่องเพศสัมพันธ์
- พฤติกรรมผิดกฎหมาย
- ความคิดฆ่าตัวตาย
- การล่วงละเมิดทางเพศ
- ข้อมูลทางด้านพันธุกรรม

การแปลงค่าข้อมูลเพื่อไม่ให้ระบุถึงตัวบุคคลได้ (De-identified data)

การให้ค่ารหัส (Coded information)

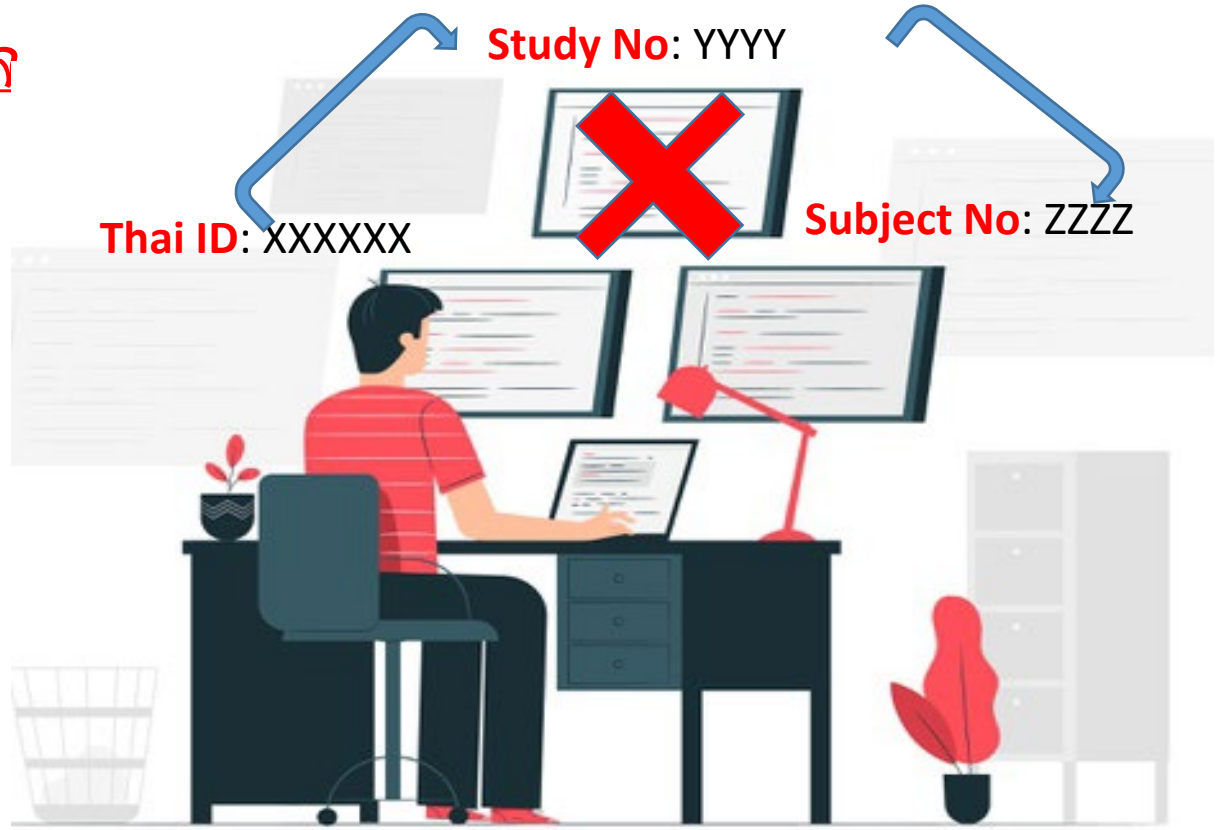
- สร้างค่าใหม่ขึ้นมาทดแทนค่าตัวแปรที่อาจระบุตัวบุคคล/ชุมชนได้
- ทีมงานวิจัยเฉพาะบางคนเข้าถึงรายการเชื่อมโยงตัวแปร



การแปลงค่าข้อมูลเพื่อไม่ให้ระบุถึงตัวบุคคลได้ (De-identified data)

การตัดการเชื่อมโยงข้อมูลที่ใช้ระบุตัวบุคคล (Anonymized information)

- แปลงค่าข้อมูลที่ระบุตัวบุคคลได้
- กำจัดรายการที่สามารถระบุตัวบุคคล กับรหัสทดแทนทั่วไป
- คงเหลือแต่รหัสทดแทนที่ไม่อาจย้อนกลับไปยังค่าข้อมูลตัวตนบุคคลเดิมได้อีก



ข้อมูลที่ไม่อาจระบุตัวตนได้ (Anonymous information)

ข้อมูลที่ไม่อาจระบุตัวบุคคลได้

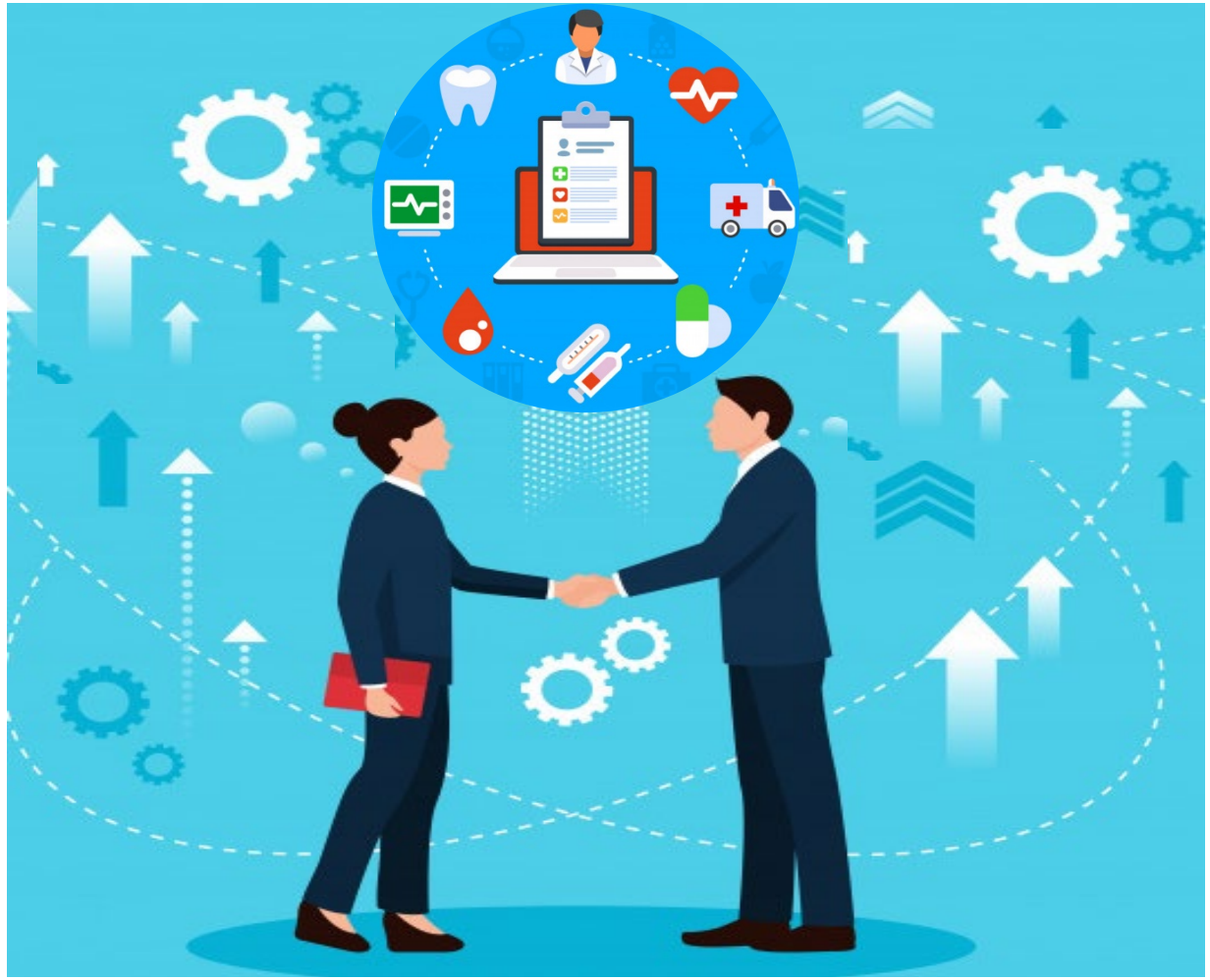
- ตั้งแต่แรกจัดเก็บ
- ถูกตัดการเชื่อมโยงไปสู่ข้อมูลส่วนบุคคลไว้แล้ว

- ข้อมูล/สิ่งส่งตรวจจากธนาคารเลือด
- ส่วนชิ้นเนื้อพยาธิวิทยาที่เหลือจากผลการผ่าตัด

การแบ่งปันข้อมูล (Data sharing)

การแบ่งปันข้อมูลสำหรับการวิจัยอื่น
เพื่อก่อให้เกิดประโยชน์สูงสุด
ในวงการวิทยาศาสตร์ และต่อสังคม

- ค่าข้อมูลที่เป็นตัวเลข/รหัสค่าข้อมูล (Data / Information)
- สิ่งส่งตรวจ (Specimen)
- ชีววัตถุ (Biological materials)



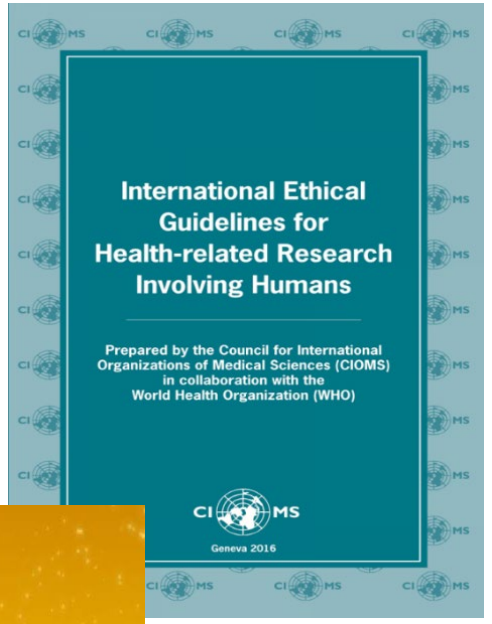
กฎหมาย-แนวปฏิบัติ
เกี่ยวกับ
ความเป็นส่วนตัวและการปกปิดความลับ

การรักษาความเป็นส่วนตัว และการปกปิดความลับ ของข้อมูล/สิ่งส่งตรวจ

- การจัดเก็บ (Collection & Storage)
- การใช้ (Use)
- การแบ่งปัน (Sharing)

กฎหมาย และ แนวปฏิบัติ:

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- CIOMS 2016 - Collection, storage and use of material/data
  - Guideline 11: Biologic material and related data
  - Guideline 12: Data in health-related research
  - Guideline 24:: Data sharing



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ผู้ควบคุมข้อมูลส่วนบุคคล
มีอำนาจหน้าที่ตัดสินใจ

- เก็บ-รวบรวม
- ใช้
- เปิดเผย

ข้อมูลส่วนบุคคล
ข้อมูลที่ระบุตัวบุคคล

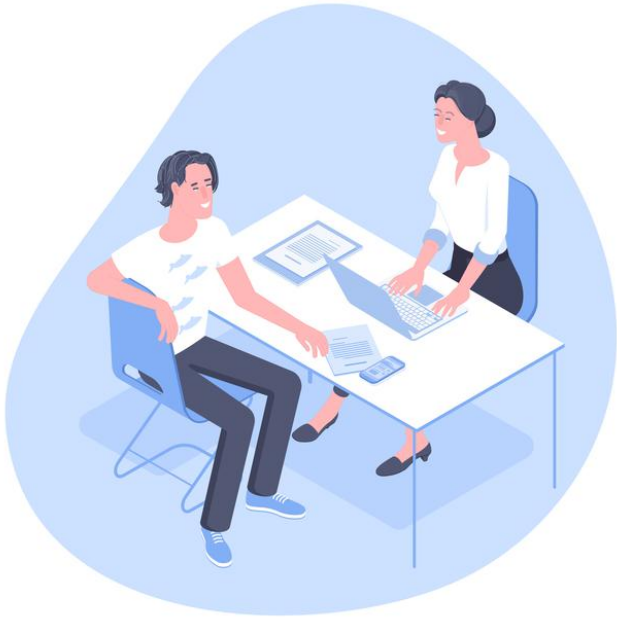
- ทางตรง
- ทางอ้อม

ผู้ประมวลผลข้อมูลส่วนบุคคล
ดำเนินการตามคำสั่ง หรือ
ในนามของผู้ควบคุมข้อมูล

- เก็บ-รวบรวม
- ใช้
- เปิดเผย

การเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูล

- เจ้าของข้อมูลให้ความยินยอมไว้ก่อนหรือในขณะนั้น
- การขอความยินยอม
  - เป็นหนังสือ หรือ ผ่านระบบอิเล็กทรอนิกส์
  - ต้องแจ้ง วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย
  - ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
  - ใช้ภาษาที่อ่านง่าย
  - ไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์...



การเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูล

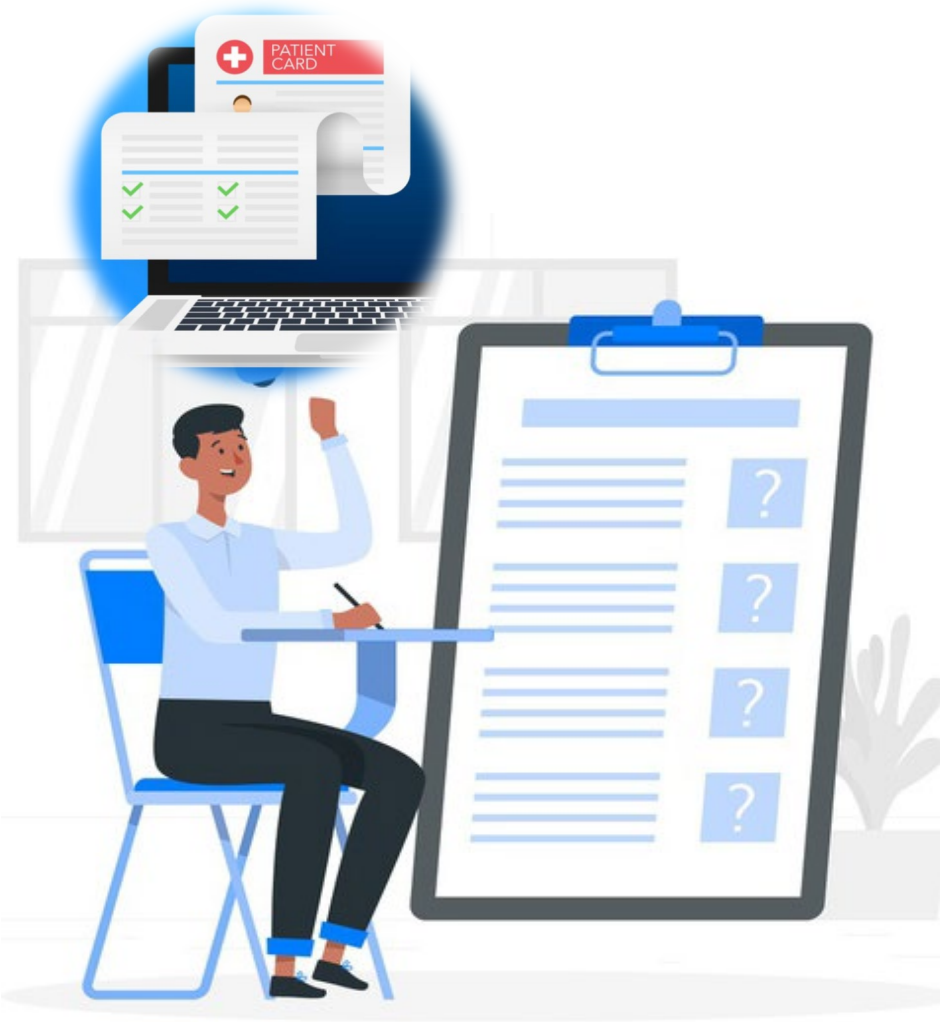
- แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บ
  - วัตถุประสงค์
  - ผลกระทบที่เป็นไปได้
  - ข้อมูลที่จะจัดเก็บ และ ระยะเวลาในการเก็บ
  - แหล่งที่ข้อมูลอาจจะถูกเปิดเผย
  - ข้อมูลเผู้ควบคุมข้อมูล (สถานที่ติดต่อ และ วิธีการติดต่อ)
  - สิทธิของเจ้าของข้อมูล

- ต้องแจ้งวัตถุประสงค์ใหม่ และได้รับความยินยอมก่อน... หากจะใช้ข้อมูลแตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้

มาตรา 21 & 23

การเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูล

- สิทธิของเจ้าของข้อมูลส่วนบุคคล
  - ขอเข้าถึง/รับสำเนาข้อมูลที่เกี่ยวกับตน
  - ขอให้เปิดเผยถึงการได้มาของข้อมูล
  - ขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตน
  - คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
  - ดำเนินการลบ หรือทำลาย
  - ระงับการใช้ ข้อมูล



การเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูล

- ห้ามมิให้เก็บรวบรวมข้อมูล โดยไม่ได้รับความยินยอม เกี่ยวกับ
  - เชื้อชาติ เผ่าพันธุ์
  - ความคิดเห็น ทางการเมือง ลัทธิ ศาสนา
  - พฤติกรรมทางเพศ
  - ประวัติอาชญากรรม
  - ข้อมูลสุขภาพ ความพิการ
  - ข้อมูลพันธุกรรม ข้อมูลชีวภาพ
- จัดเก็บเพื่อให้บรรลุวัตถุประสงค์เท่าที่จำเป็น
- มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ

การเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูล

- ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลจากแหล่งอื่น เว้นแต่ได้แจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ...
- บุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผย จะต้องไม่ใช้ เปิดเผยข้อมูล เพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ ที่ได้แจ้งไว้

- ในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
  - ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
  - เมื่อผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล ได้จัดให้มีมาตรการคุ้มครองที่เหมาะสม

มาตรา 25 & 27-29

บทบาท หน้าที่ และความรับผิดชอบ ของ ผู้ควบคุมข้อมูลส่วนบุคคล

- ดำเนินการให้ข้อมูล ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- ป้องกันมิให้ผู้ได้รับข้อมูล ใช้ หรือเปิดเผย ข้อมูลโดยมิชอบ
- จัดให้มีระบบการตรวจสอบ เพื่อลบ หรือทำลายข้อมูล เมื่อ
  - พ้นกำหนดระยะเวลาการเก็บรักษา
  - เจ้าของข้อมูลร้องขอ
  - เจ้าของข้อมูลถอนความยินยอม

มาตรา 35 & 37

CIOMS 2016:

Guideline 11: Collection, storage and use of biological materials and related data

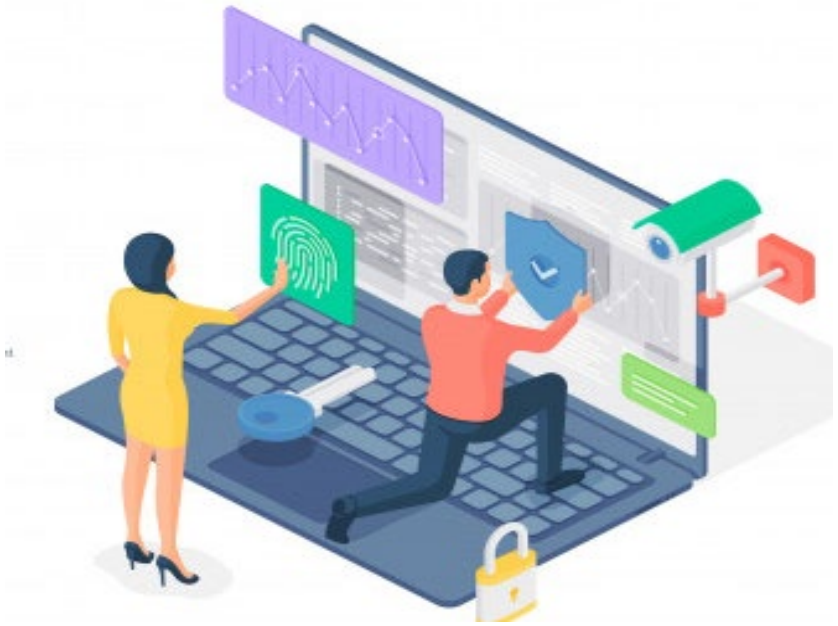
When biological materials and related data, such as health or employment records, are collected and stored, institutions must have a governance system to obtain authorization for future use of these materials in research. Researchers must not adversely affect the rights and welfare of individuals from whom the materials were collected.

Guideline 12: Collection, storage, and use of data in health-related research

When data are stored, institutions must have a governance system to obtain authorization for future use of these data in research. Researchers must not adversely affect the rights and welfare of individuals from whom the data were collected.

การเปิดเผย และ แบ่งปัน ข้อมูล สำหรับการวิจัยอื่น

- สถาบันต้องจัดให้มี ระบบควบคุม และบริหารจัดการข้อมูล (Governance system):
  - เป็นระบบที่ไว้วางใจได้
  - มีการขอคำยินยอมจากผู้ให้ข้อมูล (Donor)
  - มีการรักษาความลับ ปกป้องไม่ให้มีการเชื่อมโยงข้อมูลที่จัดเก็บ กับ ข้อมูลที่ระบุตัวบุคคลได้
  - มีระบบที่สามารถคุ้มครองสิทธิ และ ความเป็นอยู่ของผู้ให้ข้อมูล



CIOMS Guidelines 11 & 12

การเปิดเผย และ แบ่งปัน ข้อมูล สำหรับการวิจัยอื่น

- หน่วยงานที่จะเปิดเผย/แบ่งปันข้อมูล ควรจะต้อง
  - มีการลงนามข้อตกลงการใช้ข้อมูล (Data use agreement)
  - มีมาตรการปกป้องอื่นๆ นอกจากการแปลงรหัสการเข้าถึงข้อมูลที่ระบุตัวบุคคลได้ (De-identification)
  - มีมาตรการด้านความมั่นคงปลอดภัยของข้อมูล (Data security) ที่เหมาะสม
  - จัดให้มีกรรมการอิสระที่ดูแลการเผยแพร่ข้อมูล

การเปิดเผย และ แบ่งปัน ข้อมูล สำหรับการวิจัยอื่น

- ผู้รับผิดชอบให้ข้อมูล
  - ต้องให้ข้อมูลที่เป็นแบบแปลงรหัสเข้าถึงข้อมูลส่วนบุคคล (Anonymized / Coded data) เท่านั้น
  - จำกัดการเข้าถึงตัวข้อมูล (Limiting access)
  - Iแจ้งให้ผู้ให้ข้อมูลทราบในเบื้องต้น ในเรื่องข้อจำกัดของมาตรการการปกป้องรักษาความลับของข้อมูล (Limitations. of confidentiality)

ข้อจำกัดของมาตรการการปกป้องรักษาความลับของข้อมูล

- แม้ว่าจะมีมาตรการควบคุมปกป้องที่ดีเพียงใด ก็ยังมีความเป็นไปได้ที่ข้อมูลจะ รั่วไหล หรือ ถูกขโมย

- การระบุตัวบุคคล มีความเป็นไปได้ เพราะ
  - ข้อมูลจากหลายๆแหล่งข้อมูล อาจถูกนำมาเชื่อมโยงกันได้
  - ประเด็นวิจัยอาจมีความจำเพาะเจาะจง
  - อาจมีเทคนิคใหม่ๆที่ทำให้อนุมานลักษณะข้อมูลพื้นฐานได้

- ข้อมูลอาจถูกบังคับให้ต้องเปิดเผย ในกรณีที่มีประเด็นทางกฎหมาย

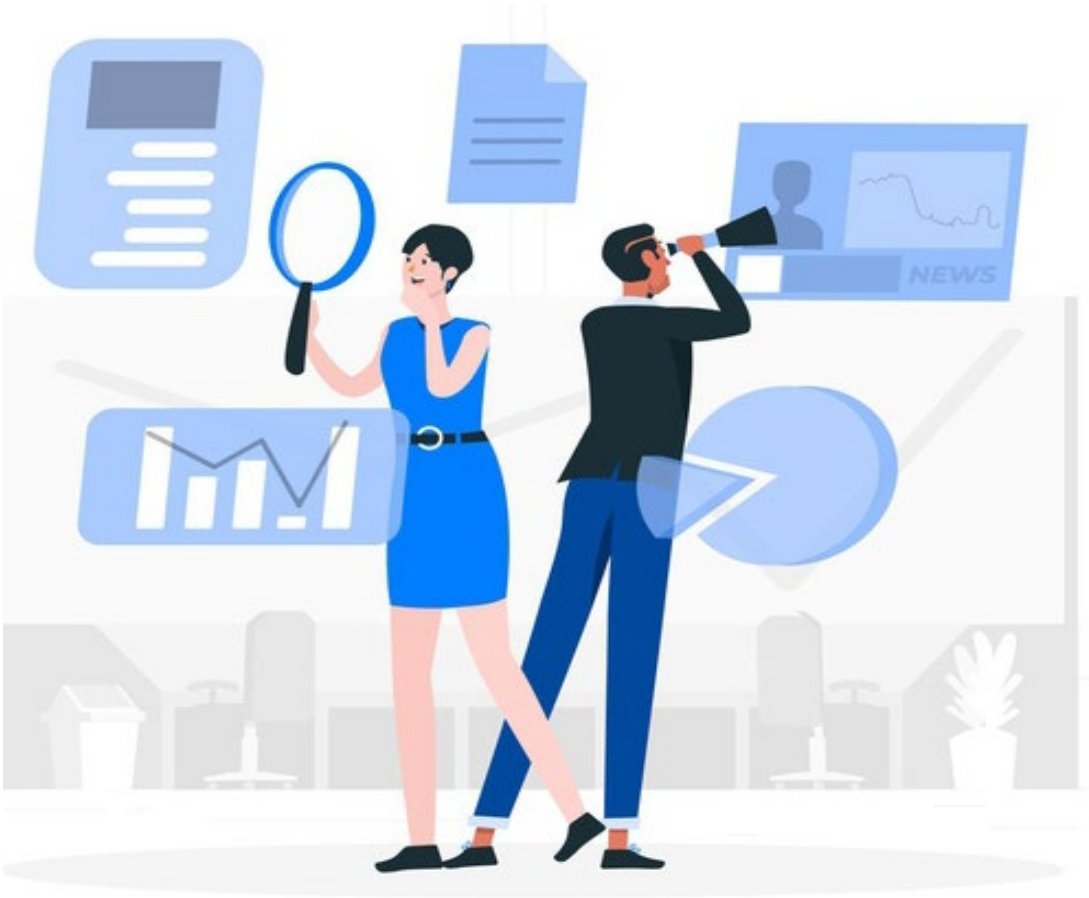
การเก็บใช้ข้อมูล ที่ได้จากการเปิดเผย/แบ่งปัน

- นักวิจัย ผู้เปิดเผย/แบ่งปันข้อมูล
  - ต้องควบคุมว่าจะแบ่งปัน
    - กับใคร
    - ภายใต้เงื่อนไขอะไร

CIOMS Guidelines 11, 12 & 24

การเก็บใช้ข้อมูล ที่ได้จากการเปิดเผย/แบ่งปัน

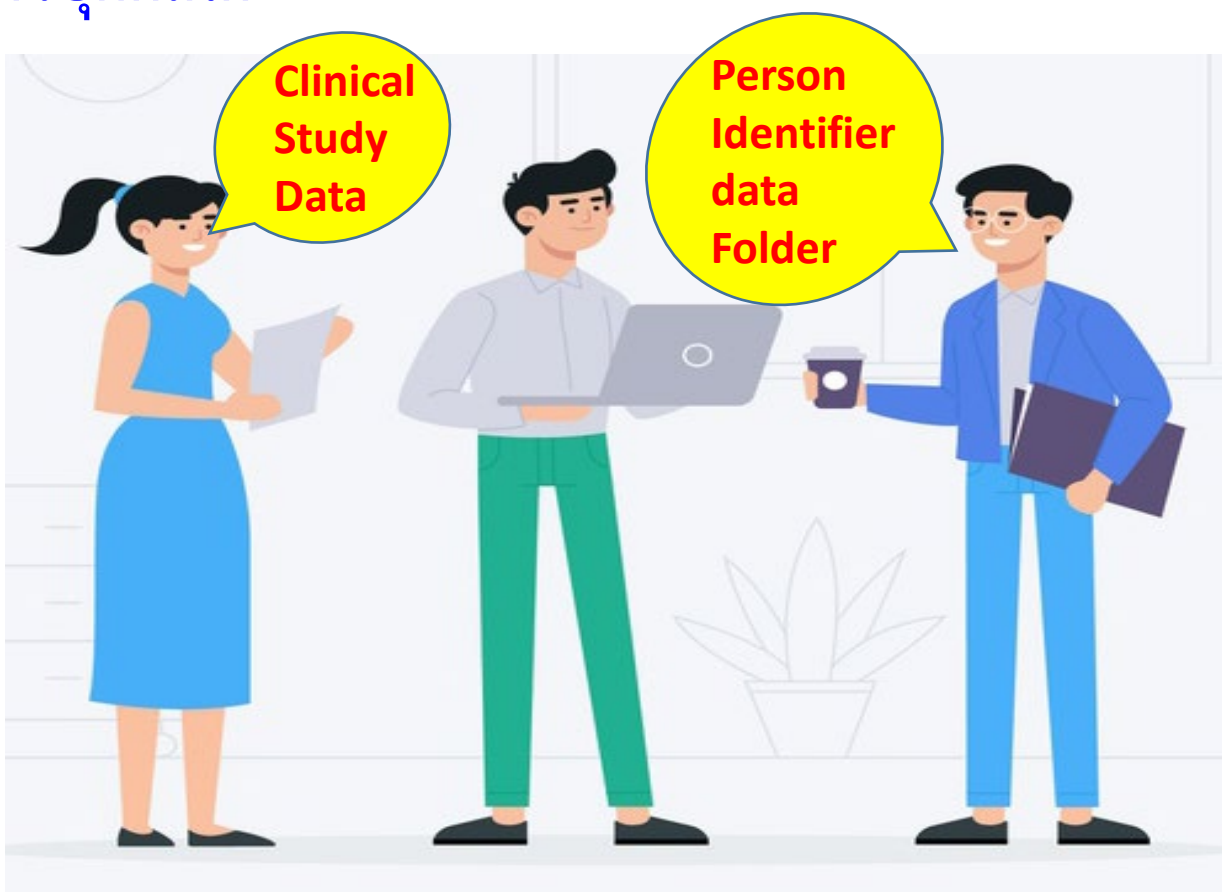
- นักวิจัย ผู้ใช้ข้อมูล
  - ใช้ข้อมูลที่เป็นรหัสที่ไม่อาจระบุตัวบุคคลได้ (Anonymized/ Coded data) ตามที่ได้รับจากแหล่งข้อมูล
  - ไม่ใช้ข้อมูลจากหลายแหล่งข้อมูล หรือ นำเอาข้อมูลหลายๆตัว มาประกอบกัน สร้างเป็นตัวแปรใหม่ที่อาจระบุตัวบุคคลได้



CIOMS Guidelines 11, 12 & 24

การเก็บใช้ข้อมูล ที่ได้จากการเปิดเผย/แบ่งปัน

- หากมีความจำเป็นต้องใช้ข้อมูลที่สามารถระบุตัวบุคคลได้
  - ต้องชี้แจงต่อกรรมการจริยธรรม
    - เหตุผลความจำเป็น
    - มาตรการปกป้องรักษาความลับ



CIOMS Guidelines 11, 12 & 24

สรุป กฎหมาย และ แนวปฏิบัติ เกี่ยวกับ การปกป้องรักษาความลับส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล

- ตรวจสอบความถูกต้อง เป็นปัจจุบัน สมบูรณ์ ของข้อมูล
- มีระบบ และมาตรการคุ้มครองข้อมูล
- จัดเก็บ ใช้ และเผยแพร่ตามวัตถุประสงค์ที่ตกลง

เจ้าของข้อมูล

- ให้ หรือ เพิกถอน คำยินยอม
- เข้าถึง หรือ คัดค้าน
- ทำลาย หรือ ระงับการใช้

ผู้ประมวลผลข้อมูลส่วนบุคคล

- ใช้ข้อมูลที่เป็นรหัสที่ไม่อาจระบุตัวบุคคล
- ไม่สร้างตัวแปรใหม่ที่อาจระบุตัวบุคคลได้
- จัดเก็บ ใช้ และเผยแพร่ตามวัตถุประสงค์ที่ตกลง