สมมติฐานทางเทคโนโลยีที่เปลี่ยนแปลงไปกับวิธีคิดถึงการคุ้มครองข้อมูลสุขภาพส่วนบุคคลที่อาจต้องเปลี่ยนแปลงตาม

ข้อสังเกตและข้อเสนอแนะโดย มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง
ถึง คณะอนุกรรมาธิการพิจารณาศึกษาระบบสารสนเทศด้านมาตรฐานและข้อมูลการแพทย์
คณะกรรมาธิการการสาธารณสุข สภานิติบัญญัติแห่งชาติ

บทนำ

วิธีการประมวลผลสารสนเทศที่ก้าวหน้าและซับซ้อนขึ้น ประกอบกับความสามารถของคอมพิวเตอร์ที่ทำงานได้เร็วขึ้นในราคาที่ถูกลง อีกทั้งยังมีความแพร่หลายมากขึ้นจากเดิมเป็นอุปกรณ์ประจำสำนักงานกลายเป็นอุปกรณ์ประจำตัวที่พกพาไปได้ทุกที่ ทำให้สมมติฐานทางเทคโนโลยีที่อาจเคยเป็นจริงเมื่อทศวรรษ 1980 ในคราวที่เริ่มมีการออกแบบมาตรการการคุ้มครองข้อมูลส่วนบุคคล อาจไม่เป็นจริงอีกต่อไปในปัจจุบัน ทำให้มีความจำเป็นต้องปรับเปลี่ยนการคิดเกี่ยวกับการเปิดเผยและคุ้มครองข้อมูลส่วนบุคคลเสียใหม่ เอกสารนี้นำเสนอ 2 ตัวอย่างที่เกี่ยวข้องกับข้อมูลสุขภาพ

Linkability และ Re-identification: การเชื่อมโยงข้อมูลหลายชุดเข้าด้วยกันเพื่อชี้กลับอัตลักษณ์บุคคล

ข้อถกเถียง: ฐานข้อมูลสุขภาพที่ประกอบด้วยได้ข้อมูลส่วนบุคคลนั้น มีประโยชน์ในการศึกษาวิจัยด้านสุขภาพรวมถึงการวางแผนนโยบายซึ่งจะเป็นประโยชน์กับสาธารณะ จึงสมควรให้เปิดเผยได้ เมื่อมีการลบชื่อบุคคลหรือสิ่งที่จะทำให้เชื่อมโยงถึงบุคคลได้ออกไปจากฐานข้อมูลแล้ว (anonymization หรือ de-identification)

ความเห็นของมูลนิธิฯ: เห็นด้วยกับการชั่งน้ำหนักประโยชน์สาธารณะ แต่จะต้องคำนึงถึงความก้าวหน้าทางเทคโนโลยีซึ่งสามารถเชื่อมโยงข้อมูลหลายชุดเข้าด้วยกันและบ่งชี้อัตลักษณ์บุคคลกลับได้อีกครั้ง (re-identification) เพื่อการหาประโยชน์ที่ไม่พึงประสงค์ด้วย การตัดสินใจเปิดเผยข้อมูลควรคำนึงถึงวิธีการ de-identification ว่าสามารถแยกการระบุอัตลักษณ์ออกไปได้ดีเพียงใด เมื่อเทียบกับวิธีการ re-identification ในปัจจุบันและในอนาคตเท่าที่เจ้าของข้อมูลยังจะมีชีวิตอยู่ เพื่อจะชั่งน้ำหนักของความเสี่ยงในการละเมิดสิทธิในความเป็นอยู่ส่วนตัวของบุคคลกับประโยชน์ของสาธารณะได้ตามสภาพความเป็นจริงทางเทคโนโลยี และสนับสนุนให้มีการกำหนดมาตรฐานการ de-identification ที่เหมาะสมและปรับปรุงให้ทันสมัยอยู่เสมอ

ตัวอย่าง: Latanya Sweeney (2000) [1] พบว่า ด้วยข้อมูลเพียง 3 ชนิด คือ เพศ รหัสไปรษณีย์ และ วันเดือนปีเกิด เราสามารถระบุตัวคนอเมริกันได้ถึง 87.1% โดยเฉลี่ย และในบางพื้นที่ที่ประชากรไม่มากนักก็ยิ่งมีโอกาสสูงขึ้น เช่น ในอลาสกา ไอดาโฮ เนแบรสกา สามารถระบุกลับได้ถึง 99-100% ส่วนรัฐที่มีประชากรมาก เช่น ดีซี นิวยอร์ก หรือ แคลิฟอร์เนีย สามารถระบุกลับได้ประมาณ 65-75% (ดูตาราง Figure 13, 14) ทั้งนี้ระดับความสม่ำเสมอของการกระจายตัว (distribution) ของประชากรในชนิดข้อมูลต่างๆ จะส่งผลต่อความสามารถในการระบุกลับด้วย

ตามหลักความน่าจะเป็น เมื่อคำนวณความเป็นไปได้ของการผสมตัวแปร 3 ชนิดคือ เพศ (เป็นไปได้ 2 ค่า ชาย หรือ หญิง) รหัสไปรษณีย์ 5 หลัก และวันเดือนปีเกิดในช่วง 100 ปี รวมกัน จะมีค่าที่ไม่ซ้ำกัน 365,000 ค่า Sweeney ทดลองขอข้อมูลในระดับที่เล็กกว่ารัฐ คือฐานข้อมูลผู้มีสิทธิเลือกตั้งของเขตเลือกตั้ง Cambridge, Massachusett พบว่ามีผู้มีสิทธิลงคะแนนในฐานข้อมูล 54,805 คน ดังนั้นมันเป็นไปได้ที่จะแต่ละคนจะมีข้อมูลสามตัวนี้ไม่ซ้ำกันเลย

ด้วยวิธีการเชื่อมโยงด้วย เพศ รหัสไปรษณีย์ และวันเดือนปีเกิดนี้ เมื่อนำฐานข้อมูลสุขภาพที่มีประวัติการรักษาพยาบาลมาเชื่อมโยงกับฐานข้อมูลผู้มีสิทธิลงคะแนนที่มีชื่อ สกุล และที่อยู่จะทำให้เราสามารถระบุกลับ (re-identify) ได้ว่าระเบียนในฐานข้อมูลไหนเป็นข้อมูลของใคร รวมถึงสามารถเชื่อมโยงกับข้อมูลอ่อนไหวอื่นๆ เช่น ชาติพันธุ์ และพรรคการเมืองที่เป็นสมาชิกในฐานข้อมูลทั้งสองได้ด้วย และวิธีการนี้ยังสามารถนำไปทำซ้ำกับฐานข้อมูลอื่นๆ จนให้ภาพที่ละเอียดมากขึ้นๆ ของเจ้าของข้อมูลได้

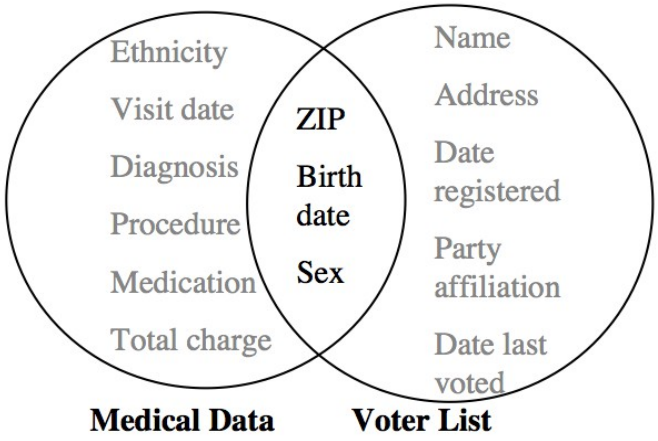

Figure 1 Linking to re-identify data

รูป Figure 1 จาก Sweeney (2000) ชนิดข้อมูลในวงกลมด้านซ้ายมาจากฐานข้อมูลค่าใช้จ่ายการรักษาพยาบาล IHCCCC Research Health Data ในรัฐอิลลินอยส์ ส่วนชนิดข้อมูลในวงกลมด้านขวามาจากรายชื่อผู้มีสิทธิเลือกตั้ง

Data Segmentation: การแบ่งข้อมูลเป็นชิ้นย่อยๆ เพื่อให้ใช้เท่าที่จำเป็นได้

ข้อถกเถียง: ข้อมูลสุขภาพบางชุดจำเป็นต่อการปฏิบัติงานของเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง ดังนั้นจึงจำเป็นต้องอนุญาตให้เก็บ ใช้ และเปิดเผย ระหว่างบุคคลและองค์กรดังกล่าว เพื่อประโยชน์ของเจ้าของข้อมูล

ความเห็นของมูลนิธิฯ: เพื่อประโยชน์ของเจ้าของข้อมูลซึ่งเป็นผู้รับบริการ ข้อมูลจะต้องถูกแบ่งปันและไหลเวียนอย่างรวดเร็ว โดยเฉพาะในภารกิจที่ความแม่นยำและรวดเร็วของข้อมูลส่งผลต่อชีวิตและสวัสดิภาพของเจ้าของข้อมูล อย่างไรก็ตาม ภารกิจจำนวนมากที่ต้องเกี่ยวข้องกับบุคคลและองค์กรที่หลากหลาย ไม่จำเป็นว่าทุกคนในห่วงโซ่ของการทำงานจะต้องได้รับข้อมูลทั้งหมดโดยละเอียดเท่ากัน การออกแบบระบบการไหลเวียนของข้อมูล ที่แบ่งปันชิ้นข้อมูลที่เหมาะสม ให้กับบุคคลที่เหมาะสม ในเวลาที่เหมาะสม เป็นเรื่องสำคัญเพื่อลดความเสี่ยงในการรั่วไหลของข้อมูลหรือการเลือกปฏิบัติต่อเจ้าของข้อมูล ในยุคที่การแบ่งปันข้อมูลยังทำด้วยกระดาษ การซอยข้อมูลเป็นชิ้นย่อยอาจทำได้ยาก แต่ในยุคที่ข้อมูลเกือบทั้งหมดอยู่ในระบบคอมพิวเตอร์ การแบ่งปันข้อมูลเป็นรายชิ้นเป็นเรื่องที่ทำได้ หน่วยงานด้านสุขภาพที่เกี่ยวข้องควรส่งเสริมให้มีมาตรฐานการแลกเปลี่ยนแบ่งปันข้อมูลบนหลักการ “รู้เท่าที่จำเป็น”

ตัวอย่าง: การแบ่งประเภทข้อมูลตามแนวคิดสิทธิในความเป็นอยู่ส่วนตัว แบ่งได้ 3 ประเภทคือ 1) Data ข้อมูลทั่วไป 2) Personal Data ข้อมูลเกี่ยวกับบุคคลที่ระบุตัวตนได้ 3) Sensitive Personal Data ข้อมูลอ่อนไหวเกี่ยวกับบุคคล ซึ่งอาจถูกนำมาใช้เพื่อการเลือกปฏิบัติต่อบุคคลได้ เช่น เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง เป็นสมาชิกสหภาพแรงงานหรือไม่ เพศวิถี ประวัติอาชญากรรม (ทั้งที่เป็นผู้กระทำและถูกกระทำ) ฯลฯ ข้อมูลที่ดูเหมือนเป็น (2) อาจเป็น (3) ได้ด้วย เราจะลองพิจารณาตัวอย่างจากระบบสารสนเทศที่ถูกเสนอให้ใช้กับระบบสุขภาพของเบลเยียม

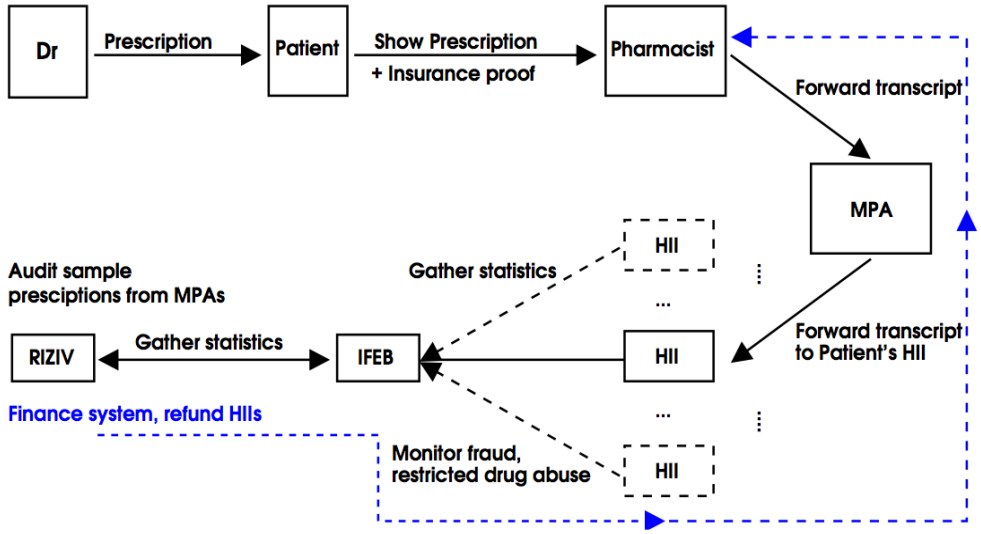

Figure: Belgian Healthcare System

ผังระบบดูแลสุขภาพของเบลเยียม เจาะส่วนที่เกี่ยวกับการจ่ายยา จาก De Decker et al. (2008).

ในระบบสุขภาพของเบลเยียม แพทย์จะเป็นผู้ออกใบสั่งยาให้กับผู้ป่วย จากนั้นผู้ป่วยจะนำใบสั่งยาดังกล่าวพร้อมกับหลักฐานการประกันสุขภาพไปรับยาจากเภสัชกร จากนั้นเภสัชกรจะนำหลักฐานการจ่ายยาไปแสดงต่อหน่วยงานดูแลใบสั่งยากลาง (Medical Prescription Administration – MPA) ซึ่งจะทำงานร่วมกับกองทุนประกันสุขภาพ (Health Insurance Insitutes – HII) ซึ่งมีมากกว่าหนึ่งกองทุนและหน่วยงานประเมินและตรวจสอบคือ IFEB (Belgian Institute for Pharmacoepidemiology) และ RIZIV (National Institute for Health and Disability Insurance) เพื่อจ่ายเงินคืนให้กับเภสัชกร ตามผังการแลกเปลี่ยนข้อมูลข้างต้น จะเห็นได้ว่าข้อมูลของผู้ป่วยจะผ่านมือหน่วยงานจำนวนมาก และข้อมูลจำนวนหนึ่งก็จำเป็นสำหรับการให้บริการผู้ป่วย

ประเด็นคือ กองทุนประกันสุขภาพต่างๆ ในเบลเยียมนั้น ส่วนมากจัดตั้งโดยองค์กรทางศาสนาหรือทางการเมือง เช่น กองทุนของกลุ่มเสรีนิยม กลุ่มสังคมนิยม หรือกลุ่มคริสเตียน [2] ซึ่งหมายความว่า ถ้าผู้ป่วยกรอกหมายเลขประกันสุขภาพลงไปใบสั่งยาเพื่อรับยาจากเภสัชกร เภสัชกรก็พอจะบอกได้ว่าผู้ป่วยมีความเชื่อทางศาสนาหรือความคิดเห็นทางการเมืองอย่างไร ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่เภสัชไม่จำเป็นต้องรู้เพื่อการปฏิบัติหน้าที่ และถ้ารู้ก็มีโอกาสจะเลือกปฏิบัติกับผู้ป่วยได้ ดังนั้นปัญหาคือ ทำอย่างไรที่จะทำให้เภสัชกรสามารถรู้ได้ว่าผู้ป่วยนั้นมีประกันสุขภาพอยู่กับกองทุนใดก็ทุนหนึ่ง (เพื่อที่เภสัชกรจะมั่นใจได้ว่าเขาจะเบิกเงินได้) แต่ไม่รู้อย่างเฉพาะเจาะจงว่าเป็นกองทุนไหน

เพื่อแก้ปัญหาดังกล่าวและปัญหาเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวอื่นๆ จึงมีการเสนอระบบการแลกเปลี่ยนสารสนเทศที่จะทำให้เภสัชกรรู้เฉพาะสิ่งที่จำเป็นในการปฏิบัติหน้าที่ (ตามหลัก need-to-know) คือผู้ป่วยจำเป็นต้องได้ยาอะไรในปริมาณเท่าใด และยืนยันได้ว่าผู้ป่วยมีสิทธิที่จะได้ยาดังกล่าว Medical Prescription Administration (MPA) เป็นกลไกทางสถาบันที่ช่วยเป็นตัวกลางให้เภสัชกรไม่ต้องติดต่อกับกองทุนประกันสุขภาพโดยตรง และเพื่อเพิ่มการคุ้มครองผู้ป่วยจึงมีการพิจารณาอย่างละเอียดว่าใครจะแบ่งปันข้อมูลอะไรให้กับใครอื่นในระบบได้บ้าง ตามหลัก minimum/selective disclosure

ระบบนี้ยังพยายามจะทำให้การสั่งยานั้นสืบย้อนกลับ (trace) ได้เพียงเท่าที่จำเป็นในการตรวจสอบการสั่งยา-เพื่อประโยชน์ในการรักษาพยาบาลของผู้ป่วย และจะทำให้ใบสั่งยาแต่ละอันเอามาเชื่อมโยงกันไม่ได้ เพื่อให้ไม่สามารถเห็นพฤติกรรมการจ่ายยาของหมอแต่ละรายได้ โดยมีจุดประสงค์เพื่อป้องกันไม่ให้บริษัทยาติดสินบนหมอเพื่อจ่ายยายี่ห้อใดเป็นพิเศษ การออกแบบมาตรการทั้งหมดนี้ ใช้แนวคิดที่ว่ามนุษย์นั้นสามารถผิดพลาด (หรืออาจถูกบังคับให้ทำผิดพลาด) ได้ดังนั้นระบบจะส่งข้อมูลเฉพาะเท่าที่จำเป็นให้กับคนที่เกี่ยวข้องเท่านั้น เพื่อลดความเสียหายที่ไม่มีใครอยากให้เกิด

Party\Data	**Patient**	**Presc.**	**Doctor**	**Pharm.**	**MPA**	**HII**
Patient	ID (trivial)	all content	ID	ID	ID	ID
Doctor	nym	PrescID, data (trivial)	ID (trivial)	—	—	—
Pharm.	ss status	data	ID (if anomaly)	ID (trivial)	ID	—
MPA	nym, ss status	PrescID, data	nym	ID	ID (trivial)	ID
HII	ID	PrescID, cost	—	—	ID	ID (trivial)
IFEB	nym, ss status etc.	anon. stat. data	nym	geog. location	—	—

Table: Access control matrix

ตารางการเข้าถึงข้อมูล – ใครจะรู้ข้อมูลส่วนไหนของใครได้บ้าง จาก De Decker et al. (2008) แนวตั้งคือผู้เกี่ยวข้อง แนวนอนคือข้อมูล เช่น คนไข้จะเข้าถึงข้อมูลใบสั่งยาได้ทั้งหมด (รวมทั้งหมายเลขประจำตัวหมอ เภสัชกร MPA และ HII) ในขณะที่หมอจะรู้ชื่อคนไข้และรายละเอียดในใบสั่งยา แต่จะไม่รู้อะไรเลยเกี่ยวกับเภสัชกรและระบบการจ่ายยา ส่วนเภสัชกรนั้นจะรู้เฉพาะสถานะประกันสุขภาพของคนไข้และข้อมูลในใบสั่งยา

ข้อเสนอต่างๆ เหล่านี้ถูกประมวลเป็นข้อกำหนดทางเทคนิคสำหรับโปรโตคอลแลกเปลี่ยนข้อมูล eHealth Protocol (DLVV08) ซึ่งสรุปคุณสมบัติได้ดังนี้ [3]

- **ความลับของข้อมูลผู้ป่วยและหมอ:** ผู้อื่นไม่ควรจะรู้ข้อมูลของผู้ป่วยหรือของหมอ เว้นเสียว่าจะเป็นข้อมูลที่มีเจตนาจะให้รู้ตามโปรโตคอลนี้
- **การยืนยันตัวตน:** ทุกฝ่ายจะต้องยืนยันตัวตนของกันและกันอย่างเหมาะสม (เพื่อให้มั่นใจว่ากำลังจะแบ่งปันข้อมูลกับคนที่เจตนาจะแบ่งปันด้วยจริงๆ)
- **ความเป็นส่วนตัวของข้อมูลการออกใบสั่งยา:** โปรโตคอลจะคุ้มครองพฤติกรรมการจ่ายยาของหมอ
- **การบังคับให้มีความเป็นส่วนตัวของข้อมูลการออกใบสั่งยา:** โปรโตคอลจะต้องป้องกันการติดสินบนระหว่างหมอและบริษัทยา
- **ความเป็นอิสระจากกันของข้อมูลการออกใบสั่งยา:** เภสัชกรจะต้องไม่สามารถแสดงหลักฐานให้กับบริษัทยาได้ถึงใบสั่งยาของหมอ
- **ความเป็นนิรนามของผู้ป่วย:** จะต้องไม่มีฝ่ายไหนสามารถระบุตัวตนของผู้ป่วยได้

- **ความไม่สามารถสืบย้อนกลับไปหาผู้ป่วยได้:** ใบสั่งยาต่างๆ ที่ถูกออกให้กับผู้ป่วยรายเดียวกัน จะต้องไม่สามารถเชื่อมโยงเข้าด้วยกันได้

จะเห็นได้ว่ามาตรการในการคุ้มครองความเป็นส่วนตัวในกรณีนี้นั้น อาจแบ่งได้เป็นสองประเภทซึ่งใช้ควบคู่กัน คือ 1) ความเป็นส่วนตัวที่ได้มาโดยการควบคุมการเข้าถึง (Privacy by access control) และ 2) ความเป็นส่วนตัวที่ได้มาโดยวิธีการทางวิทยาการเข้ารหัส (Privacy by cryptographic approaches) [4] การจัดทำระบบสารสนเทศที่พยายามบังคับใช้มาตรการทั้งสองแบบดังกล่าวอาจทำได้ลำบากด้วยเทคโนโลยีในยุคก่อนหน้านี้ แต่ด้วยเทคโนโลยีการยืนยันตัวตน (authentication) การแบ่งซอยชิ้นข้อมูล (data segmentation) และการเข้ารหัสข้อมูล (encryption) ใหม่ๆ ทำให้มันเป็นไปได้มากขึ้นที่จะมีระบบสุขภาพที่ทั้งอนุญาตให้เจ้าหน้าที่ทำงานได้อย่างมีประสิทธิภาพ รักษาชีวิตผู้ป่วย คุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้เกี่ยวข้อง และป้องกันการทุจริตคอรัปชั่น พร้อมๆ กัน

เมื่อพิจารณาถึงความเป็นไปได้ทางเทคโนโลยีเหล่านี้ ข้อยกเว้นตามกฎหมายจึงควรปรับเปลี่ยนให้เหมาะสมและบังคับให้บุคคลและหน่วยงานที่เกี่ยวข้องแบ่งปันเฉพาะชิ้นส่วนข้อมูลที่จำเป็นเท่านั้น ไม่ใช่ก้อนข้อมูลเหมารวมทั้งหมด ดังเช่นตัวอย่างข้างต้น ที่ระบบจะส่งเฉพาะข้อมูลบางส่วนจากใบสั่งยา ไม่ใช่ส่งใบสั่งยาทั้งฉบับ

บทสรุปและข้อเสนอแนะ

- **การออกแบบระบบการทำงานที่คุ้มครองข้อมูลส่วนบุคคล:** งานด้านสุขภาพเป็นงานที่ซับซ้อนเกี่ยวข้องกับหลายหน่วยงาน ทั้งรัฐและเอกชน ครอบคลุมทั้งงานด้านปฏิบัติการในสถานพยาบาลไปจนถึงงานด้านสิทธิประโยชน์และการเงิน แนวคิดในลักษณะนี้สามารถนำไปประยุกต์กับงานด้านอื่นๆ เช่น รัฐบาลอิเล็กทรอนิกส์ การลงคะแนนเสียงทางอิเล็กทรอนิกส์ หรือการจัดเก็บคลังเอกสารได้ [5]
- **ข้อควรระวังเรื่องการระบุกลับอัตลักษณ์ (re-identification):** การอนุญาตให้เปิดเผยชุดข้อมูลที่สร้างขึ้นมาจากข้อมูลส่วนบุคคล แม้จะมีการลบชื่อหรือสิ่งที่จะทำให้เชื่อมโยงถึงบุคคลไปแล้ว ก็ยังมีโอกาสที่ข้อมูลชุดดังกล่าวจะถูกนำไปเชื่อมโยงกับข้อมูลชุดอื่น เพื่อระบุกลับถึงอัตลักษณ์บุคคลได้ ดังนั้นข้อยกเว้นในการเผยแพร่ข้อมูลจึงควรคำนึงถึงความเสี่ยงดังกล่าวและดำเนินการให้แน่ใจว่าการลบชื่อหรือสิ่งเชื่อมโยงได้ทำอย่างเพียงพอและสุดความสามารถ ในอันที่จะไม่ก่อให้เกิดการละเมิดต่อบุคคลในข้อมูลในภายหลัง
- **การซอยชิ้นส่วนข้อมูล:** การอนุญาตให้แบ่งปันข้อมูลส่วนบุคคลระหว่างหน่วยงานที่เกี่ยวข้อง จะต้องทำให้แน่ใจว่าเป็นการแบ่งปันข้อมูลเฉพาะเท่าที่จำเป็น ให้กับบุคคลที่เหมาะสม ในเวลาที่เหมาะสม เท่าที่จะเป็นประโยชน์กับเจ้าของข้อมูล เพื่อลดความเสี่ยงจากการรั่วไหลของข้อมูลและจากการเลือกปฏิบัติ

- **เทคโนโลยีใหม่ ความเป็นไปได้ใหม่:** เทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองความเป็นส่วนตัวที่ก้าวหน้า ทำให้เป็นไปได้มากขึ้นที่ระบบการทำงานจะคุ้มครองสิทธิของเจ้าของข้อมูลไปพร้อมๆ กับอำนวยความสะดวกให้กับผู้ปฏิบัติงานและเอื้อประโยชน์ให้กับสาธารณะในภาพรวม มาตรการทางเทคโนโลยีที่เดิมในอดีตเคยใช้ได้ อาจใช้ไม่ได้อีกต่อไปในปัจจุบัน เช่นเดียวกับลักษณะของความคุ้มครองที่ก่อนหน้านี้อาจเป็นไปไม่ได้ทางเทคโนโลยี แต่ในปัจจุบันเป็นไปได้แล้ว การออกแบบนโยบายและมาตรการต่างๆ รวมถึงข้อบังคับและข้อยกเว้นในกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงควรตั้งอยู่บนฐานของเทคโนโลยีในปัจจุบันและความเป็นไปได้ทางเทคโนโลยีในอนาคตที่ผู้เกี่ยวข้องยังคงมีส่วนได้ส่วนเสียอยู่

อ้างอิง

[1] Latanya Sweeney. *Simple Demographics Often Identify People Uniquely.* Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. http://dataprivacylab.org/projects/identifiability/

[2] Bart De Decker, Mohamed Layouni, Hans Vangheluwe, and Kristof Verslype, *A Privacy-Preserving eHealth Protocol compliant with the Belgian Healthcare System.* In Proceedings of Public Key Infrastructure, 5th European PKI Workshop: Theory and Practice, (EuroPKI 2008), Springer LNCS 5057, pp. 118-133, 2008. [slides] http://www.item.ntnu.no/europki08/presentations/europki08-layouni.pdf

[3] Naipeng Dong, Hugo Jonker, Jun Pang, *Formal Analysis of an eHealth Protocol.* In Proceedings of 17th European Symposium on Research in Computer Security, (ESORICS 2012), Springer LNCS 7459, pp. 325-342, 2012. http://satoss.uni.lu/members/naipeng/reports/DLV08/DLV08.pdf

[4] Mahmuda Begum, Quazi Mamun, Mohammed Kaosar, *A Privacy-Preserving Framework for Personally Controlled Electronic Health Record (PCEHR) System.* In Proceedings of 2nd Australian eHealth Informatics and Security Conference, pp. 1-10, 2013. http://ro.ecu.edu.au/aeis/9/

[5] adapID – advanced applications for electronic IDentity cards in Flanders https://www.cosic.esat.kuleuven.be/adapid/documents.html