カナダのブリティッシュ・コロンビア州における電子診療データの二次利用

British Columbian's population based Data Base for Medical Study in Canada.

増成　直美
Naomi MASUNARI

要旨

更新のたびに繰り返しデータリンケージが行われる行政データへのアクセス権を研究者に提供することには、多くの利点がある。たとえば、開示リスク、個人の時間の使用、研究のコストを最小限に抑えることができる、氏名や他の識別データが含まれる一次データの収集が減少する等々である 。これらのデータの研究利用は、住民の医療と福祉を向上させうる政策立案のためのエビデンスを提供する大きな可能性を秘めている。しかしながら、これらの使用は、利用可能なデータセットが増加するので、特に、慎重なコントロールが要求される。PopData は、法律やデータ管理者のプライバシー関連要件だけでなく、情報が研究のために使用されている住民の期待に応えるために、PbD を採用している。継続的な技術開発は、物理的および技術的なインフラストラクチャの洗練を求めている。そして PopData は、常に人間の誤りやすさに対して警戒する。個人レベルの情報を再利用する研究は、公共政策や住民の福祉の向上に貢献する。

Abstract

There are many advantages to providing researchers with access to administrative data that data linkage is repeatedly performed on each update. For example, disclosure risk, use of personal time, research cost can be minimized, collection of primary data including name and other identification data decreases, and so on. Research and use of these data holds great potential to provide evidence for policy planning that can improve the medical care and welfare of residents. However, these uses require careful control, especially as the number of available data sets increases. PopData employs Privacy by Design not only for privacy related requirements of laws and data administrators, but also to respond to the expectations of residents whose information used for research. Continued technical development calls for sophistication of physical and technical infrastructure. And PopData always warns against human error susceptibility. Research that reuses individual level information contributes to public policy and improving the welfare of residents.

キーワード：自己情報コントロール権、診療情報、個人情報保護法、プライバシー・バイ・デザイン、データ共有契約

Key words：individuals' self-information control rights, medical record, Personal Data Protection Act, Privacy by design, data sharing agreement.

Ⅰ　はじめに

世界中で、国民の電子健康記録（Electric Health Record：EHR、以下「EHR」という。）を整備することは、医療領域、特に公衆衛生分野においては根本的な改善をもたらす機会とみなされている。疫学研究とは、疾病の罹患をはじめ健康に関する事象の頻度や分布を調査し、その要因を明らかにする科学研究である[1)]。疾病の成因を探り、疾病の予防法や治療法の有効性を検証し、または環境や生活習慣と健康とのかかわりを明らかにするために、疫学研究は欠くことができず、医学の発展や国民の健康の保持増進に多大な役割を果たしている[1)]。疫学研究は、個人のさまざまな診療データを利用して進められる。診療情報等の疫学研究への利用により、効率的で効果的な医療の提供が可能となる。

しかし、EHR プログラムは、数年という期間を要し巨額な投資を含む複雑なプロジェクトであることから、世界中が試行錯誤の中にある。統合された情報技術の確立に加えて、プログラムは、医療政策における目標の付随措置、金融、法律や協力の促進といった医療システムとのアライメント、すべての医療機関と国民のために必要な臨床組織と文化の改変などを必要とする[2、3)]。

また、EHR データの研究への二次的な利用は、個人の研究プロジェクトにとって第一義的には、データ収集への費用対効果的で効率的な代替手段となる[4)]。さらに、二次的なデータ利用は、調査結果の偏りを削減することができる[5)]。

ビッグデータとの対峙が待ち受けているこれからの時代」においては、「データ収集と保有を制限する」これまでのやり方から、「データ使用の管理」へと法と規制の焦点をシフトさせることが、ビッグデータ時代のプライバシーを守る対策の第一歩になる[6)]、ともいわれている。現行の個人情報保護法やプライバシー保護法は、「個人情報の収集・処理する手続きは、『告知と同意』方式がプライバシー保護の基本となっている[7)]」ので、ビッグデータ時代になり、「告知に基づく同意」という個人情報の収集・処理によるプライバシー保護の仕方は根底から揺らいでいく可能性が大きい、ともいわれる[8)]。

欧米においても、医療情報の活用と患者のプライバシー保護の調整については議論が尽きない状況ではあるが、近時、幾多の批判にもかかわらず、医療分野における個人情報の利用を一層推し進める方向性が打ち出されている[9、10)]。診療情報を活用しなければ、より有効で安全な、費用対効果に優れた医療の実現が不可能だと考えられるからである。

そこで、本稿では、プライバシー保護策としてプライバシー・バイ・デザイン等と先進的に取り組んでいる、プライバシー保護先進国といわれている、カナダのブリティッシュ・コロンビア州の状況を調査・検討することにしたい。

Ⅱ　カナダの状況

1　カナダにおけるプライバシー保護

連邦制を採用するカナダでは、立法権が連邦と州に分属するが、保健・衛生に関する立法権は、州が有する[11)]。カナダにおいては，連邦法としての「プライバシー法（Privacy Act）[12)]」と「個人情報保護及び電子文書法（PIPED 法：Personal Information Protection and Electronic Documents Act）[13)]」）が、それぞれ公的部門と民間部門とを別の法律で対象とするセグメント方式（分離方式）が用意されている。プライバシー保護の運用面において、プライバシー・コミッショナーは、カナダにおいても中核となる役割を果たしてきている。

2　プライバシー・バイ・デザイン

プライバシー・バイ・デザイン（Privacy by Design：以下「PbD」という。）は、1990 年代にカナダのオンタリオ州のプライバシー・コミッショナーであるアン・カプキアン博士が提唱したものである[14、15)]。PbD は、プライバシー対策を設計段階で事前に埋め込むという概念である。カプキアン博士は、PbD について、「さまざまな技術の設計仕様の中にプライバシーを織り込むフィロソフィーでありアプローチである[16)]」と述べている。

PbDの特徴は、サービスやアプリケーション等の新しいシステムの企画・設計段階からプライバシー対策を織り込んでいく考え方であり、設計から保守までのライフサイクル全般において、体系的かつ継続的にプライバシー保護の一貫した取り組みを行うことである。すなわち、①事後的ではなく事前的（Proactive）、救済的でなく予防的（Preventative）、②初期設定（Default Setting）としてのプライバシー、③デザインに組み込まれる（Embedded）プライバシー、④全機能的：ゼロサムではなく、ポジティブサム、⑤最初から最後ま

でのライフサイクルすべてにわたってのセキュリティ保護、⑥可視性と透明性：公開の維持、⑦利用者のプライバシーの尊重：利用者中心主義を維持する、という7つの基本原理を持つ[17]。

カプキアン博士は、これらの原則の適用について、「PbDの原則は、あらゆる種類の個人情報に適用され得るが、医療情報や財務データといった機微なデータには、特に強力に適用されなければならない。プライバシー対策の強度は、データの機微性の高さに相応する傾向がある[17]」と述べている。

カナダの公的資金による社会的セーフティネットは、個人のレベルの行政保健・社会サービスの豊富なデータとともに、州および準州のガバメントを提供する。これらのデータは、研究者が住民の医療と福祉の需要と供給を調査し、公共政策の開発のためのエビデンスを提供する、豊富な資源となっている。前述のように、データの二次的な研究への利用は、個人の研究プロジェクトにとって第一義的にはデータ収集への費用対効果的で効率的な代替手段である[4]。また、二次的データ利用は、調査結果の偏りを取り去ることができる[5]。すなわち、データを研究のために二次的に利用することは、医療と福祉の展望を改善することにつながる故に公共の利益に該る、と考えられている。同時に、適切なセーフガードは、多くの場合、機密情報の開示や利用を管理するために必須である、というのがカナダの基本的なスタンスのようである。

Ⅲ　ブリティッシュ・コロンビア州

1　BC州住民データベース（PopData）

ブリティッシュ・コロンビア州の住民データベース（Population Data BC：以下、「PopData」という。）は、ブリティッシュ･コロンビア（以下、「BC」という。）州の約460万人の住民の個人レベルの匿名化された経時的データを保持している。これらのデータは、データプロバイダによって相互に承認された外部データセットに連結可能な状況にある。PopDataの医療、教育、職場や環境などのさまざまな分野にまたがるデータの連結は、ヒトの医療、福祉の展開への影響の複雑な相互作用を理解するために非常に有益である。PopDataは、また全国的なリアルタイムのデータリンケージ、アクセス、およびヒトの健康に関する研究・開発を支援するために、数々のトレーニングを提供する教育研究資源という位置づけもある。PopDataから支援を受ける研究は、健康な地域社会のために、関連する政策立案や投資決定に役立つ。

PopDataは、それ自身は研究活動を行わないという決定の下、BC州の健康データベース（The British Columbia Linked Health Databae）[18]のデータを受け継ぎ、医療サービスの視点からデータの保持を拡大する目的のために、2009年に設立された。PopDataは、BC大学の一組織という位置づけである。

PopDataは、医学研究者から研究申請書が提出されると、その申請を調整することで、研究者を支援する。承認された研究プロジェクトに対しては、データセットを抽出・作製し、安全なサーバ上でこれらの抽出されたデータセットの利用を可能にする等、データに関する研究要請面をも支援する。すなわち、後述のように、法的な基盤の上で、公的機関として、データを受領し、連結し、保管する。当該データ管理は、プロジェクト単位で行われる。

PopDataは、統合レベルのデータだけを提供する組織とは異なり、個人レベルの非識別データを提供する。PopDataの保有するデータの大半は、サービスの提供や支払いのために収集された行政データである。データセットには、医師への支払い、病院の分類、労働災害などに関するものがある。直接識別子が存在しない場合でも、データの再識別が可能な詳細で多様な十分な情報が含まれる。そのため、PopDataはリンク作業にユニークIDを有しないが､そのリンク率は95%を超えるものとなっている[19]。

PopDataは、主に研究目的のために、BC保健省、BC人口動態統計庁、BCがん登録機関、BC労働安全庁等からのデータを、二次的な研究利用目的のために保持している。したがって、PopDataの支援を受ける研究者は、医療費の支払い、処方箋、退院サマリ、介護、精神保健、がん、周産期、収入、職業、幼年期、および出生・死産・婚姻・死亡といった人口動態等に関するデータにまでアクセスすることも可能となる。

データ資源の追加更新は、継続的に行われる。データリンケージや研究面での最高の柔軟性を可能にするために、これらのデータは、多くの場合、個人レベルで可能な限り最も詳細なレベルで保存されている。PopDataは、承認された研究プロジェ

クトのために、申請の承認を受けた研究者に、承認されたデータセットを提供するために、これらのデータを保持している。

PopData は、BC 州のすべての住民の個人情報または識別子を保持する可能性がある。これらの個人情報または識別子は、記録された情報の機密性の大きいコンテンツデータ（研究契約書の下で許可された通りに使用もしくは開示される個人固有の情報を含む PopData が保有するデータ）[20] とは別に、保持される。すなわち、診断コード、労働者補償請求、または死亡日などの項目を含むコンテンツデータと、氏名、住所、生年月日などの個人レベルの識別子とは、別々に保管されている。識別子は、唯一、データリンケージのためにだけ使用される。このように、PopData は、データリンケージのための信頼できる第三者として機能している。

2　立法上の枠組み

PopData は、BC 州の情報の自由とプライバシー保護法（Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.：以下、「FIPPA」という。）を中心に、個人情報に関するすべての関連法規に準拠している。

（1）FIPPA

FIPPA は、BC 州における公的機関によって収集、使用、開示または保持される情報に関して、個人にプライバシーの権利と情報アクセス権を保証する。

PopData は、個人情報の収集、使用と開示に関して、BC 州の立法上の必要条件を満たす方針と手順を開発し、実装している。FIPPA 付則 1 は、「個人情報」を「身元を確認し得る個人に関する記録された情報」で、氏名、年齢、性別、人種などの属性データ、個人に割り当てられる識別番号、シンボルまたは他の詳細、個人の指紋、血液型または遺伝上の特徴、身体的もしくは精神的な障害を含む個人の健康管理履歴に関する情報等を含むものと定義する。

BC 州では、個人を識別できる情報の開示に関しては、FIPPA が適用される。PopData は、FIPPA の付則 1 の下で公的機関と定義される。政府の機関やその他の州の機関も、同様に公的機関と定義されている。

PopData とさまざまなデータ管理者間のデータ共有協定は、FIPPA33 条の下で可能となる。情報が義務の遂行もしくは公的機関の活動のために、または 35 条に基づく研究または統計目的のために必要であるとき、「公的機関は、33.1 条、33.2 条または 33.3 条で許可されている場合に限り、個人情報をその監視下または管理下で開示することができる。」と規定する 33 条の下で、公的機関は情報を開示することができる。

FIPPA35 条 1 項は、以下の条件が満たされる場合に限り、公的機関がその監督下でまたはそのコントロール下で、研究または統計目的のために、個人を識別できる情報を開示することができると規定する。すなわち、(a) 情報が提供されなければ研究の目的を合理的に達成することができず、または研究の目的が情報・プライバシー監督官によって承認されている場合で、(a.1) 研究参加を要請するためにその情報主体に連絡しないという条件の下で情報が開示されるとき、(b) 記録の連結が情報主体にとって有害でなく、かつ連結によってもたらされる利益が公共の利益になることが明らかであり、(c) 関係する公的機関の長が個人情報の保護に関する条件（(i) セキュリティと機密性、(ii) 早期の妥当な時点での個人の識別子の除去または破棄、(iii) 当該公的機関の明示的な許可なしに識別可能な形で情報のその後の使用または開示の禁止）を承認し、(d) 情報の開示を受ける者が個人情報の機密保持に関する承認された条件、FIPPA および個人情報の保護に関係する公的機関の方針と手続に従うという合意書に署名する場合に限られる。

FIPPA に基づいて、情報主体は、登録された自己の情報へのアクセス権を有し（4 条）、情報の複写・閲覧を請求することができる（5 条）。関係する公的機関は、FIPPA の例外規定（12 条から 22.1 条）によって定められた一定の理由がある場合には、請求を拒絶することができる。

登録された自己の情報に誤りまたは脱落があると考える者は、関係する公的機関の長に対して訂正を請求することができる（29 条 1 項）。公的機関の長は、訂正請求に応じない場合には、請求の内容を登録情報に注記しなければならない（同法 29 条 2 項）。

PopData は、データプロバイダの情報を収集することができ（26 条 1 項、27 条 1 項）、承認を得てそれらをデータリンケージ目的で使用することができる（32 条、33.1 条、33.2 条）。PopData は、研究契約書に基づいて、研究者にデータプロバイダの情

報を開示することができる（33.1 条、35 条）。

(2) データ共有協定

PopData は、合法的に、BC 州保健省などのさまざまなデータプロバイダとデータ共有協定[21]を締結している。本協定は、FIPPA に準拠したプロバイダ情報の開示の枠組みを提示する（協定書 2 条）。これらの協定契約により、PopData は所内にデータファイルの保持を実現することができる。データプロバイダの支援、FIPPA を基盤にしたデータ共有契約の厳格なガイドラインの下で、PopData は、経年的にさまざまなデータ資源とデータセット間で、個人を参照する記録を連結する権限を有する。

PopData とデータプロバイダは、互いに共有するデータの正確性を維持・向上させるために努力することを約する（6 条）。PopData は、本契約に基づいてデータプロバイダによって提供された情報が、本契約、大学法、FIPPA、その他の適用される法律および適用される裁判所命令で許容される場合に限り、PopData によって収集、保持および使用されることを約する。本契約が FIPPA の規定に加えて義務を課す場合は、本契約が適用される（8.1 条）。PopData は、データプロバイダが研究協定契約書に基づいてその研究者によるデータプロバイダ情報の使用を承認した後にのみ、研究用抽出データセットを研究者に開示することができる（8.4 条）。

情報共有協定書の 8.6 条によれば、PopData は、以下の義務を負う。すなわち、a）データプロバイダの識別子データを他のデータ管理者が提供する識別子データにリンクする、b）データプロバイダと協力して、データアクセス要求書（Data Access Request: DAR、以下「DAR」という。）の審査と修正を調整する、c）該当する研究契約書に基づき研究者に研究用抽出データセットを準備し提供する、d）データプロバイダ情報のアーカイブとして機能する、e）安全に保護された研究環境（Secure Research Environment：SRE、以下「SRE」という。）上のプロジェクトについては、研究契約書の期限が切れた場合やデータ管理者が勧告した場合に、研究者のデータプロバイダ情報へのアクセスの終了を可能にする、f）SRE をオンオフにするプロジェクトについては、PopData は、研究契約書が期限切れになった場合、またはデータ管理者が勧告した場合、データプロバイダ情報のプロジェクトの閉鎖を監督する。プロジェクト閉鎖手続きは、資金調達機関、研究倫理委員会および研究契約の要件に従う。PopData は、承認された期間（最低 7 年）の間、研究用抽出データセットを安全に保管し、アーカイブ保存期間の満了時に研究用抽出データセットを破棄する。g）SRE 内の資格のあるスタッフは、就任時および年間の定期プライバシー・トレーニングを受けなければならない。

データプロバイダの義務は、以下のものである（9 条）。すなわち、a）適用、修正および審査のための共通基準の作成のために、データ管理者の作業部会に他のデータ管理者とともに参加する、b）データ管理者のワーキンググループの責任を、任期に定められた活動レベルで達成する、c）データ管理者のワーキンググループの期間ごとに DAR を審査する、d）本共有協定に基づく PopData の運営に影響を与えるデータプロバイダ情報の重要な変更または更新について PopData に通知する。および、e）PopData がサービスを提供するために必要な場合には、フィードバックと承認を適宜に提供する、f）必要に応じて、年 1 回のデータ更新と更新された情報を提供する、というものである。

データプロバイダ情報は、本契約期間の開始時、およびデータプロバイダと PopData の契約両当事者が相互同意を得た暫定的で追加的な更新時に PopData に送信される。さらに本契約の期間中はいつでも、データプロバイダと PopData は、相互書面による合意により、リストされているデータセットを追加または変更したり、データ送信スケジュールを変更することができる（10.5 条）。

PopData は、本情報共有協定に基づいて、データプロバイダから収集された個人情報の保護および機密保持を、不正アクセス、収集、使用、保存、変更、開示または破棄などのリスクから保護するために、合理的な取り決めを行う。これらの取り決めは、BC 州が示す方針および基準によって提供される保護レベルを満たすか、上回るものでなければならない（11.1 条）。

PopData は、データプロバイダ情報の誤用防止対策を含むデータの適切かつ安全な保管を保証するため、付則 D に詳述されているすべてのセキュリティ対策を実施する（11.2 条）。PopData は、データプロバイダ情報を保管および使用する情報システムが付則 D に記載されているように物理的に安

全な環境に配置され、これらの情報システムへのアクセスが許可を受けた個人により、管理、監視、および制限されることを保証する（11.3 条）。

PopData は、データプロバイダ情報を、BC 大学に保管するとともに（11.4 条）、災害復旧の目的で、当該情報の暗号化されたバックアップコピーを、バンクーバーのアイアンマウンテンに保管する（11.5 条）。PopData は、許可なしに 11.5 条にいうオフサイト保管施設を変更することはできない（11.6 条）。

本情報共有協定に基づいて提供されたデータプロバイダ情報への無断のアクセス、使用、改変、使用の変更、転載もしくは破棄、または開示は、本契約の違反とみなされる可能性があり、データプロバイダからの契約解約に至ることがある（16.1 条）。

PopData は、本協定の違反があると思われる合理的な根拠があるときは、直ちに状況を調査しなければならない（16.2 条）。PopData は、本協定の 16.1 条に記載されているような情報の誤用が疑われる事象については、データプロバイダに直ちに通知し、当該事象の発生後合理的に可能な限り速やかに、状況および是正措置の詳細な報告書を提出しなければならない（16.3 条）。本協定の 16.3 条に基づき、情報の誤用の事例について通知を受けたデータプロバイダは、以下のいずれかの措置をとることができる。すなわち、a）誤用再発に対処するために PopData が提案する手続きを審査する、b）誤用の再発を防ぐために、PopData にデータプロバイダが指定した措置を講じるよう指示し、PopData はこの指示に従うものとする、c）BC 州情報・プライバシー局の事務所に通知し、書類の写しを提出する、d）調査の必要があるときは、監査を開始し、監査人または調査官が PopData 施設への入退を調査し、誤用に関する記録を作成する、e）データプロバイダ情報の開示を PopData に直ちに停止させる等、である（16.4 条）。

（3）研究契約書

さらに、PopData は、研究者との間の法的拘束力のある研究契約書[22]において指定、承認された研究プロジェクトの研究者に、自らが保持するデータを利用可能にすることが許可されている。PopData は、研究者とデータ管理者との間の署名された研究契約書に従って研究用の抽出データセットを準備し、提供する（研究契約書 1.1 条）。研究用の抽出データセットは、ASCII フラットファイルとして提供される。この形式は、分析用のさまざまなソフトウェアプログラムに読み込むことができる（1.2 条）。

研究者は、受領したデータセットを分析する責任があり、研究者が独自の分析を実行するための能力と必要な資源を持つことが期待される。PopData の研究者担当係は、データ分析サービスを提供することはできない（1.3 条）。担当のデータ管理者との秘密保持契約を締結し、PopData の研究のプライバシー・トレーニングを完了した、承認された DAR で特定されたプロジェクトメンバー、研究者およびその他の個人だけが、抽出データセットへのアクセスを保証される（1.4 条）。チームメンバーが SRE へのアクセスを許可される前に、主任研究員は、最新の研究者用プライバシー・トレーニングを当該チームメンバーに完了させなければならない。プロジェクトメンバーは、抽出データセットにアクセスしている間、PopData のプライバシー・トレーニングを 3 年毎に更新しなければならない（1.5 条）。学生が抽出データセットを自らの学術研究のために使用しようとする場合、担当のデータ管理者による検討と承認のために、PopData を介して学生 DAR を提出しなければならない。a）学生は、担当のデータ管理者の承認を得た場合に限り、抽出データセットを自分の学術研究のために使用することができる。b）学生は、DAR による論文／プロジェクトの承認を得た目的を超えて、抽出データセットを使用することはできない（1.6 条）。研究契約書に則って、抽出データセットは、a）PopData を通じて BC 州の SRE に、または b）PopData の安全なファイル転送サイトを通じて、c）パスワードで保護され暗号化された CD によって、提供される（1.7 条）。データ管理者によって明示的に許可されているように、安全なファイル転送サイトまたは暗号化された CD を使用して抽出データセットが提供された場合、研究者は受領時から抽出データセットのセキュリティについてすべての責任を負い、研究契約書に定められた使用期間および条件を遵守する（1.8 条）。SRE に抽出データセットが提供されているときは、すべてのプロジェクトメンバーに責任を認識させ、安全な研究環境を遵守することに同意させることは、署名者の責任である（1.9 条）。

研究者は、研究課題、要求したデータフィールド、資金調達、新たなデータリンケージ、研究契約期間

の延長等のプロジェクトの変更が生じたときは、当該変更を通知しなければならない。その際、担当のデータ管理者による審査と承認が必要な場合がある（2 条）。

研究プロジェクトが完了したとき、もしくは研究契約期間が満了したとき、研究倫理委員会証明書が失効したとき、研究契約書または研究倫理委員会証明書が早期に終了したとき、またはデータ管理者の書面による請求により、PopData は研究者に連絡してプロジェクトを終了させる（3.1 条）。

SRE 上でアクセスされるプロジェクトは、a）プロジェクト終了時に、PopData はすべてのプロジェクトメンバーの YubiKey トークンとパスワードアクセスを直ちに無効にする、b）プロジェクトメンバーは、アクセスしたすべてのプロジェクトが終了してから 90 日以内に、YubiKey トークンを PopData に返却しなければならない、c）プロジェクトの期間終了または閉鎖に先立って、プロジェクトメンバーは SRE から持出しを希望する支援文書または研究成果を転送しなければならない。閉鎖または期間終了後にファイルをダウンロードすることはできない。d）プロジェクト終了後、プロジェクトは 7 年間、またはデータ管理者の指示に従って保存される、e）保存期間中、データ管理者の承認を得て、PopData に費用を支払うことにより、研究者は保管プロジェクトへのアクセスを要求することができる。データ管理者は、新しい DAR と研究契約書、または保管プロジェクトへのアクセスのための新たな要求書が必要かどうかを、ケースバイケースで判断する、f）保管プロジェクトへの部分的なアクセスは、できない。研究者は、保管プロジェクト全体へのアクセスのみを要求することができる（3.2 条）。

各研究プロジェクトメンバーは、割り当てられた YubiKey トークンのセキュリティと安全性について責任を負い、本契約のサービス料金表に則って、紛失または破損したトークンに対する料金を請求される（5.1 条）。研究プロジェクトメンバーは、同じプロジェクト内または関連するプロジェクトの他のメンバーと共有しないなど、いかなる状況下でも、YubiKey トークンとパスワードを機密に保たなければならない（5.2 条）。全ての研究プロジェクトメンバーは、YubiKey トークンを紛失したときは直ちに PopData に報告しなければならない。PopData は、紛失または破損した YubiKey トークンに関連する認証を速やかに中断しなければならない（5.3 条）。

PopData は、研究申請が承認された研究者に対して、カナダ内で、仮想プライベートネットワーク（VPN：Virtual Private Network、以下「VPN」という。）を介して、研究用の抽出データセットへのアクセスを提供することができる。研究者は、臨床評価科学研究所やカナダ統計局の調査データセンター等の他のモデルによって利用されるような指定されたオフィスや端末の制約といったものなしに、直接データにリモートアクセスすることができる。

研究者は、自分の研究のために必要な最小限のデータセットの匿名化されたデータを受領する。研究者は、研究倫理委員会の承認証明書と研究契約書の両方を通して、研究成果物の非識別性を確保することを保証する。

研究者は、研究契約書に則り、研究プロジェクトの成果としての出版または公表を意図した紙媒体のすべての資料に関して、公表前に審査を受け意見を求めるために、PopData を経由してデータ管理者に提出しなければならない（4.1 条）。

PopData は、資格のある研究者に対して、①保健サービスや住民の健康データを研究申請する際の指針、サポートやアドバイスといった研究申請の補助、②中央メタデータ、オンラインデータ文書システムへのアクセスという方法の支援、③ PopData を介してのデータ使用のための調整、アクセス手順、④ PopData のプロジェクト管理システム、⑤ PopData の SRE へのリモートアクセス、⑥ BC 州の研究者の養成と教育ニーズを満たすための教育課程の提供、といったサービスを用意している。

カナダ全土の学術機関からの研究者は、独自の研究・収集したデータを持っていてもいなくても、連結された行政データ含むプロジェクト用のデータへのアクセスを行うために、PopData で作業することができる。

ここでいう研究者とは、研究契約書に基づいて研究に従事しており、a）大学法（R.S.B.C. 1996、c.468）に定められている大学、b）大学および研究所法（R.S.B.C. 1996、c.52）に規定されている単科大学、総合大学または地方の研究所、c）公開学習局法（R.S.B.C. 1996、c.341）の下の公開学習局、d）ロ

イヤル・ローズ大学法（R.S.B.C. 1996、c.409）の下のロイヤル・ローズ大学、e）上記の法令に記載されている公立の中等後教育サービスを提供するその他の機関、および f）世界中にある他の同等の機関、のいずれかの機関に在籍している学生、教員または研究者である者、と定義されている。

3　PopDataのPbD

PopDataは、住民ベースの医学研究のために、連結されたデータへのアクセスを支援する革新的なリーダーであり、これにより住民に公的利益、精度の高い研究、経費削減をもたらすことができる。PopDataは、データリンケージのための「信頼できる第三者」として機能し[23]、データプロバイダの承認されたすべてのデータを連結するために必要な機密データに対して、利害関係を持っていない中立体としての地位を設定するために、研究機能を見送ることにしている[24]。PopDataは、データリンケージ目的のために個人を特定する情報を受け取ることで、一般住民ベースのデータ分析において潜在的なバイアスを制限する95%の以上の割合でのデータ連結を実現している[19]。

PopDataは、住民の健康問題の広いスペクトルを分析する350以上の研究プロジェクトをすでに支援した[25]。PopDataは、その運営のあらゆる面において、プライバシー対策を埋め込んでいる（PbD）。PopDataは、公共の利益のために、研究のための個人レベルのデータへのアクセスを支援しながら、プライバシーを保護するデザインモデルによってプライバシー保護を実装している。PopDataは、法律、行政、および一般住民の認識によって提示された課題を検討し、業務の効率化と適正な配慮の双方を実現する方法を模索し続けてきた。

PopDataは、個人情報の保護のためのカナダ規格協会のモデルコードとオンタリオ州情報・プライバシー・コミッショナーであるアン・カブキアンによって開発されたPbDの枠組みを採用している[14,15]。これは、プライバシー保護の包括的で先進的な取組みの一つとして行われている。PopDataがPbDの原理に対応することによって、その戦略目標を達成する方法は、表1のとおりである[25]。

表1は、PbDの7原則に対応するPopDataでのコントロール状況を示している。PopDataの最初のプライバシーを保護するための予防的コントロール（原則1）に関して、オフィスは、物理的に紫、赤、黄色という3つのゾーンに分けられている。各ゾーンは、異なるアクセス・コントロールを持つ。すなわち、イエローゾーンは、ロックはされているが、PopDataスタッフ全員がアクセス権を持つ。レッドゾーンは、別々のロックとアラームを持っており、生の、識別されたデータへのアクセス権を持つ従業員のゾーンである。ここでは、ドアにはビデオ監視があり、壁は侵入を防ぐために鉄鋼で強化されている。データ・サーバを収容するパープルゾーンは、壁や個別のアラームで要塞化されている。そこには、3人の特定のスタッフのみがアクセス可能となっている。

このような帯状のアプローチは、PopDataに適用される技術的なセキュリティ構造であり、ファイアウォールおよび侵入検出ソフトウェアによって保護されるが、イエローゾーンのコンピュータは、外部通信に使用することができる。レッドゾーンのコンピュータは、物理的なレッドゾーン内域にめぐらされているネットワーク上でパープルゾーンに格納された暗号化データにアクセスするために使用される端末となる。プログラマーは、これらのコンピュータにログインするために2段階認証を使用する。

通常は年1回のプロバイダからのデータの安全な転送は、リムーバブルメディアや宅配便の利用者の個人情報の記憶を回避する、安全なファイル転送プロトコルを使用して暗号化されたデータを転送することによって達成される。

コンテンツの識別子の分離は、新しいデータセットとして行われ、年次更新されたものがインポートされる。研究のために要求することができるすべてのコンテンツ変数は、識別子とは別に保存される。

データ更新毎の積極的な結合は、プロジェクトに関係なく、情報がデータプロバイダから到着したときに、行われる。このような積極的な結合は、PopDataがリンケージ率を向上させることができ、住民のデータベースを維持することを可能にする。

コンテンツと識別子の分離などのネットワークシステムの技術的なコントロールは、侵害のリスクとその結果の被害を最小限に抑える（原則2：デフォルトによるプライバシー）。物理的なコントロールは、権限のないユーザへの偶発的な暴露を防止する。機密保持契約およびプライバシー研修での誓約のような管理上のコントロールは、スタッフや研究者がその責任とプライバシー保護のベストプラク

表 1　ブリティッシュ・コロンビア州の住民データベースにおけるプライバシー・バイ・デザインの 7 原則

	BC 州住民データベースでの実装		
原　則	**物理的なコントロール**	**技術的なコントロール**	**管理上のコントロール**
1. プライバシー保護のための予防的コントロール（反応ではなく、事前対策；救済的対処ではなく、予防）	・強化されている位置的な境界 ・アラームコードを使用した、物理領域への役割ベースのアクセス ・入口/出口のビデオ監視	・ファイアウォールのあるネットワーク ・識別子とコンテンツデータの分離 ・ダミーコンピュータ ・ID を使用した 2 要素認証 ・転送からバックアップのためのストレージへの全ての点におけるデータの暗号化	・スタッフ雇用時の犯罪歴のチェック ・スタッフおよび研究者の機密保持契約 ・年間訓練を含むスタッフの包括的なプライバシー教育プログラム ・研究者のための必須プライバシー研修
2. デフォルト設定としてのプライバシー	役割に基づいた物理的なアクセス	識別子と、コンテンツデータの暗号化ストレージのネットワーク分離	スタッフと研究者のための機密保持誓約プライバシー・トレーニング
3. 設計に埋め込まれたプライバシー	作業とサーバ施設の建設の事前に計画された物理的なコントロール	アクセスとネットワークのコントロールは、国内および国際的なベストプラクティスに基づく	情報共有協定で概説認証、アクセス、およびその他の管理コントロール
4. 十分な機能性―ポジティブサムであり、ゼロサムでない。プライバシーコントロールは、ポジティブサム「ウィンウィン」の方法で、すべての利害と目的を収容する。プライバシー機能を失うことなく、保護されている。		・ソフトウェア、技術サポート、および（暗号化されたバックアップを含む）システムを研究者に提供 ・データ管理者に提供するログ、監査、追跡、およびその他のコントロール	データ管理者のすべてのセキュリティとプライバシー要件を満たしつつ提供される個人レベルのデータ、政府の政策、および法律
5. 全ライフサイクルを通じた最初から最後までのセキュリティ保護		抽出、使用、保管、バックアップ、そして最終的に破棄を通じて、暗号化されたデータ	
6. 可視性と透明性	ビデオ監視の公告	ログ記録と定期的な監査とアクセス制御	プライバシー影響評価、プライバシーポリシー、および使用文書の利用規約などの文書の入手可能性；すべての研究プロジェクトのリストはウェブサイト上で公表
7. ユーザのプライバシーの尊重：ユーザ中心			現在の基準や要件に照らした政策の年次レビューと年次プライバシー訓練

BC：ブリティッシュ・コロンビア；SFTP：安全なファイル転送プロトコル；
SRE (Secure Research Environment)：保護された研究環境

ティスに関して教育されていることに基づく。これは、エラーによる事故のリスクを低減する。これらのコントロールは、プライバシー保護がデフォルト設定であるため、継続的な作業を必要とせずに機能している。

PopData は、最初からデータの安全性確保のために施設の設計時にプライバシー保護を埋め込んでいる。また、アクセスシステムは、主要な目的として、プライバシー保護を考慮している。PopData は、同様に管理構造の設計に埋め込まれたプライバシーを確保するために、研究活動が開始可能な状態になる前に、データ共有契約、ポリシー、手続きを確定する（原則 3：デザインに埋め込まれたプライバシー）。

PbD は、ポジティブサムの方法で、すべての利害と目的を収容しようとする[25]（原則 4：ポジティブサム・アプローチ）。PopData は、統合レベルのデータ使用よりも多くの利益とリスクを有する[26]、個人レベルのデータの使用促進により、データ管理者と一般住民の期待に応える方法で、この原理を具現化する。

慣習的に行われている非識別化された研究用に抽出されたデータセットへのアクセスは、データ管理者および PopData との協定を締結した正規の研究者に限られている。プロジェクトの大半において、データは、研究者に開示され、その後、PopData の SRE、ストレージ、処理、暗号化、バックアップ、および研究者に分析用ソフトウェアの広い領域を提供する VPN を介して研究者によって分析される。研究者は、自らが特定の物理的な場所に移動する必要なくプライバシー保護を保証する革新的な装置である VPN や、2 要素認証を使用して、カナダの任意の場所から SRE にアクセスすることができる。

電子メディア上の研究者に直接データを配布するとき、SRE は研究者をコントロール不能にすることができる。例えば、これは倫理の承認の有効期限が切れた場合、もしくは不正使用が疑われる場合に、アクセスを一時停止する。SRE は、ファイルサイズ、タイプ、および名前をスクリーニングすることにより、システムのオンとオフに関して個人レベルのデータの転送を妨げることができる。SRE のスタッフは、転送されたファイルを手動で監視する。システムは、分析された出力のダウンロードのような許容転送を含み、すべての転送やアクセスをログに記録する。

SRE の利点は、研究者およびデータ管理者の双方がともに満足できるプライバシーコントロールを可能にすることであるが、個人レベルのデータへのアクセスは、プライバシー法の下で許容されるものの、開示リスクの絶対的な解決策が存在しないことに注意することが重要であり、PopData はこの点をしっかり認識している。SRE のセキュリティ措置、研究者の厳格な要件、および研究者の署名のある機密保持契約および非識別化は、このプライバシーのリスクに対処するために、PopData によってすべての作業が行われる。このアプローチは、技術の組み合わせが最高の軽減戦略を提供するデータに固有のリスクをカスタマイズすることを勧める、ベストプラクティスと一致している[27、28]。

PopData は、転送、保管、使用、開示、バックアップ、および破棄の間、すべてのデータを暗号化する（原則 5: ライフサイクル全体の保護）。データのライフサイクルは、データ管理者と適用される法律から求められる要件を満たし、もしくはそれ以上に設計されたポリシーに則って管理される。これにより、データが PopData 所内にもたらされた瞬間から、それらが破棄されるまで、徹底したセキュリティを提供する。

SRE は、コアシステムのアクセス・コントロールだけでなく、データにアクセスしたり、データを転送している者の個別の検証とデータ管理者によるビデオ監視が提供するログの監査を可能にする。PopData は、作業中のプロセスとポリシーを検証するために定期的なレビューや監査を実施することで、データ管理者と協同する。これは、可視性と透明性の重要な構成要素となる。PopData は、そのプライバシー影響評価、プライバシーポリシー、および公衆に利用可能な使用文書の利用規約を作成し、公開する（原則 6：独立した検証による透明性）。

プライバシーの尊重は、PopData の方針と実務の中心にある（原則 7：個人のプライバシーの尊重）。FIPPA35 条は、研究者に以下のことを要請する：すなわち、①識別データの必要性の正当化、②研究が公共の利益になることを示すこと、③セキュリティ、破棄、その後の使用や開示に対処される方法についての説明、および④使用条件に関する承諾への署名である[29]。

プライバシー関連の施策は、研究データへのアクセスの枠組み、プライバシーポリシー、データ管理ポリシー、アクセスポリシー、インシデント対応手順等を含む。PopData は、新しいスタッフを雇用する前に、犯罪歴のチェックを行い、スタッフにプライバシー関連のトレーニングを提供する。研究者は、研究倫理委員会の承認を得、データへのアクセス権を受領する前に、オンラインプライバシーのトレーニングを完了する必要がある。これらのポリシーと実務は、PopData が常に優先課題として、個人の情報の機密性を確保するために意図されている。

更新のたびに繰り返しデータリンケージが行われる BC 州行政データへのアクセス権を研究者に提供することには、多くの利点がある。たとえば、開示リスク、個人の時間の使用、研究のコストを最小限に抑えることができる、氏名や他の識別データが含まれる一次データの収集が減少する等々である [30]。これらのデータの研究利用は、住民の医療と福祉を向上させうる政策立案のためのエビデンスを提供する大きな可能性を秘めている。しかしながら、これらの使用は、利用可能なデータセットが増加するので、特に、慎重なコントロールが要求される。PopData は、法律やデータ管理者のプライバシー関連要件だけでなく、情報が研究のために使用されている住民の期待に応えるために、PbD を採用している。継続的な技術開発は、物理的および技術的なインフラストラクチャの洗練を求めている。そして PopData は、常に人間の誤りやすさに対して警戒する。個人レベルの情報を再利用する研究は、公共政策や住民の福祉の向上に貢献する。それで、PopData は、プライバシーコントロールを改善するために、PbD の原則に則ってプライバシー対策を改善し続けている。

Ⅳ　わが国への示唆

わが国においても、2017 年 5 月 11 日の改正個人情報保護法の全面施行においては、罰則強化や遺伝子情報を個人識別情報と明記した点で評価されている。さらに、わが国においても、「個人情報保護委員会」がやっと設置された。当該委員会が、プライバシー・コミッショナーとして効果的運用を担当することになろう。しかしながら他方で、医学研究における手続きが煩雑になるという結果を生んでしまった、との批判もある [31]。彼らは、公的保険を使った医療に関する個人情報を医学研究に二次的に利用するのは当然である、と主張する。その利用を拒む者は、医療サービスの対価として診療情報の提供を承認することなく、医療サービスという便益のみを享受するフリーライダーである、というのである。しかし、医療領域においては、医療に従事する医療有資格者に対して、刑法、その他医療従事者の資格を定める法律によって守秘義務が課されており、患者の自己情報コントロール権は人格権の一つにも相当するものと評価されていることから、特別の配慮が求められるように思われる [32]。

「法には法で」ということで、改正個人情報保護法による医学研究上の煩雑な手続きに対抗すべく、2017 年 4 月 28 日に医療分野の研究開発に資するための匿名加工医療情報に関する法律（次世代医療基盤法：平成 29 年法律第 28 号）が国会で可決・成立し、同年 5 月 12 日に公布された [33, 34]。2018 年 5 月までに施行される予定である本法は、医学・医療研究目的のために医療情報を利活用することで、健康長寿社会の形成をすることを目指すものである（1 条）。すなわち、改正個人情報保護法の特例を定めるものとなる。各医療機関における医療情報の収集のしくみ、および「認定匿名加工情報作成事業者」（以下、「認定事業者」という。）を認定するしくみを確立することで、患者本人には本法律に基づいて、匿名加工した医療情報をさまざまな研究開発に利活用することを明文化して告知する。そのような状況下で患者本人が個人情報の提供を拒否しなければ、認定事業者に対して個人の医療情報を提供できるようにする、という構想である。

わが国においては認定事業者として大学等が予定されているようだが、PopData にように、認定事業者自体は研究活動を回避し、中立な第三者として作業する必要があるように思われる。PopData は、データプロバイダのすべての情報を連結する立場上、必要な機密データを扱う他の利害関係のない中立体としての地位を確立するために研究機能を放棄しており [24]、それによってはじめてデータリンケージのための「信頼できる第三者」として役割を果たすことに成功している [23]。PopData は、リンケージ目的のために個人を特定する情報を受領し、一般住民ベースの分析では潜在的なバイアスを制限する 95% の以上のデータ連結率を実現してい

る[19]。

最もセンシティブな個人情報である患者の診療情報の保護と医学研究の発展という公益という2つの相反する利益の調整問題が存在する[32]。プライバシー保護のためのルールやガイドラインは、診療情報を収集・蓄積し適正に利活用することとプライバシー保護との調整を図ることを目的とするが、ビッグデータの時代には、情報主体の知り得ぬところでも個人情報が流通する可能性があることから、ルールやガイドラインだけではプライバシー保護に限界が生じてくる。そこで、事前にプライバシー保護を作りこむ PbD に大いなる期待がよせられる。

法益の対峙に対して、HER の二次利用による医学研究の公益性に着目して、無条件に住民の健康情報の使用を訴えるのは、問題の解決に至らない。オーストラリアの PCEHR[35]や英国の care.data[36]の事例がそのことを示している。

プライバシー保護に対する考え方は各国で様々であり、大きく EU 型と米国型に分けられる[37]。EU 型は、個人の尊厳としてプライバシーの保護を考える。それに対し，米国型はどちらかというとビッグデータの利活用に積極的な傾向である。33 か国のプライバシー法について比較検討したグラハム・グリーンリーフの論文[38]によれば、日本はベトナム、チリとともにデータ・プライバシー法のヨーロッパ的要素が十分備わっていない最下位のグループに位置づけられており、「日本はアジアの法の中で最もヨーロッパ的な要素が少ない」と評価されている[8]。

BC 州では、厳格なデータの二次利用システムを構築しつつ、同時に積極的に医学研究を行い始めている。そこには、PbD の原則に則った強化されたプライバシー対策と透明性が物理的、技術的、管理上も、住民視点で高度に維持される努力があった。PopData のプライバシー保護は、データ保護とプライバシーのためのすべての関連した法的、倫理的、運用上のガイドラインの要件を満たし、上回っている[39]。住民の信頼という基盤の上でのシステム運営こそが、研究支援の鍵である。

PopData は、公共の利益のために、研究用の個人レベルのデータへのアクセスをサポートしながら、プライバシーを保護するシステムモデルにおいてプライバシーを実装する方法に焦点を当てている。PopData は、法律、行政、および一般住民の認識によって提示された課題に正面から向かい合い、業務の効率化および適正な配慮の双方を実現する方法を示している[25]。

個人のプライバシーを尊重して、秘密の情報を保護し、セキュリティを確保することは、PopData の責務においてきわめて重大である。このために、PopData は秘密保持契約、プライバシー・トレーニング、プライバシー影響評価、物理的なセキュリティ、ネットワーク・セキュリティ、およびプライバシー部門担当者の存在を含む人的資源コントロールによる公的なウェブサイトを含む多くの構成要素からなるプライバシーリスク管理の枠組みを実施する。

わが国においても、住民にその EHR の医学研究への二次利用により実現可能な利益について説明し、プライバシー保護に関してもその時点での最高の対策が打たれているとなれば、賢明な住民は HER の医学研究への二次利用を支援するにちがいない。カナダ BC 州の PopData がその好例である。わが国においても、適切な監視、監督下で、行政データを疫学研究に利用できる可能性をも検討する時機が到来しているのではないだろうか。得られる利益は、相当大きなものに思われる。

謝辞

2016 年 9 月に実施したカナダでの現地調査においては、ブリティッシュ・コロンビア大学のキム・マクグレイユ准教授、カナダ･ヘルス･インフォウェイのジョーン・ロクプライバシー対策部長には、多くのご配慮を賜り、貴重な資料の提供もいただき、大変お世話になったことを特記して、感謝の意を表したい。

本研究は、MEXT 科研費 26380158「診療情報の保護と有効活用 ―処方箋データベースの構築と利活用に着目して」の助成を受けたものの一部である。

参考文献

1）厚生労働省：疫学研究に関する倫理指針 平成14年6月17日（平成16年12月28日全部改正、平成20年12月1日一部改正）、2004.

2）Deutsch E, Duftschmid G, Dorda W: Critical areas of national electronic health record programs-is our focus correct? Int J Med Inform, 79(3), 211-22, 2010.

3）出口弘：保健医療情報の利活用に向けた高度データ処理およびIoTの利活用と課題、日本公衆衛生雑誌,64（10）、112、2017.

4）Roos LL, Brownell MD, Lix L, et al.: From health research to social research: Privacy, methods, approaches, Soc Sci Med, 66, 117–129, 2008.

5）Gershon AS, Tu JV: The effect of privacy legislation on observational research, CMAJ, 178: 871–873, 2008.

6）クレイグ・マンティ：オンライン個人情報とプライバシー、フォーリン・アフェアーズ・リポート2014　No. 3　フォーリン・アフェアーズ・ジャパン、2014.

7）ビクター・マイヤー=ショーンベルガー、ケネス・クキエ：ビッグデータの正体 情報の産業革命が世界のすべてを変える、講談社、2013.

8）竹井潔：ビッグデータ時代におけるプライバシー：カナダを中心として、聖学院大学論叢、28（1）、33 -52、2015.

9）中山健夫：医療の未来を創るビッグデータ、週刊医学界新聞、3107号、1–9、2015.

10）中山健夫：医療ビッグデータがもたらす社会変革、日経BP社、2014.

11）日本貿易振興機構「カナダ法制の概要」www.jetro.go.jp/jfile/report/07000369/canada_hosei2010.pdf (2017.11.12参照).

12）the Minister of Justice, Privacy act, http://laws-lois.justice.gc.ca/eng/acts/P—21/ (2017.11.12参照).

13）the Minister of Justice, Personal Information Protection and Electronic Documents Act, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (2017.11.12参照).

14）Ann Cavoukian, Ph D.「PRIVACY BY DESIGN」堀部政男監修、一般財団法人日本情報経済社会推進協会編訳、https://www.coneps.jp/contents/product_001.pdf（2017.11.12参照）.

15）Cavoukian A. Privacy by Design: Strong Privacy Protection –Now, and Well into the Future. Information and Privacy Commissioner of Ontario, 2011.

16）IPC: Privacy by Design, https://www.ipc.on.ca/privacy/protecting-personal -information/privacy-by-design/（2017.11.12参照）.

17）Ann Cavoukian: Privacy by Design The 7 Foundational Principles, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (2017.11.12参照).

18）Chamberlayne R, Green B, Barer ML, et al: Creating a population-based linked health database: a new resource for health services research, Can J Public Health, 89, 270–3, 1998.

19）Jutte DP, Roos LL, Brownell MD: Administrative Record Linkage as a tool for Public Health Research, Annu Rev Public Health, 32, 91–108, 2011.

20）情報共有協定書1条1項c）。

21）Information sharing agreement (PopData Data Provider Core Holding Information Sharing Agreement) format.

22）PopData Researcher Services Agreement format.

23）populationdataBC: About PopData, http://www.popdata.bc.ca/aboutus (2017.11.12参照).

24）Canadian Institutes of Health Research: CIHR best practices for protecting privacy in health research, Canadian Institutes of Health Research, 2005.

25）Pencarrick Hertzman C, Meagher N, McGrail KM: Privacy by Design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest, J Am Med Inform Assoc, 20(1), 25-8, 2013.

26）El Emam K, Cavoukian A: A positive-sum paradigm in action in the health sector, Information and Privacy Commissioner of

Ontario, 2010.
27）Sparks R, Carter C, Donnelly John B, et al: Remote access methods for exploratory data analysis and statistical modelling: privacy-preserving analytics, CMPB, 91, 208–22, 2008.
28）O'Keefe CM: Privacy and the use of health data—reducing disclosure risk, EJHI, 3:1–9, 2008.
29）Freedom of Information and Protection of Privacy Act [RSBC 1996] Chapter 165, 2012.
30）Trutwein B, Holman CD, Rosman DL: Health data linkage conserves privacy in a research-rich environment, Ann Epidemiol, 16, 279–280, 2006.
31）樋口範雄：医学研究と改正個人情報保護法の微妙な関係、日本臨床疫学会第1回年次学術大会プログラム・抄録集、55、2017.
32）増成直美：診療情報の法的保護の研究、成文堂、2004.
33）増田克善＝日経デジタルヘルス：内閣官房が語る「次世代医療基盤法」の狙い、2017/06/14 http://techon.nikkeibp.co.jp/atcl/event/15/052600126/0613000　06/?ST=health (2017.11.12参照).
34）岡本利休：次世代医療基盤法について、日本臨床疫学会第1回年次学術大会プログラム・抄録集、56、2017.
35）増成直美：患者の自己情報コントロール権を尊重したオーストラリアの電子診療録システム、山口県立大学高等教育センター紀要、1、33-45、2017.
36）増成直美：患者の同意なく患者識別データを処理することの法的・倫理的検討　―英国の状況を手がかりとして―、山口県立大学共通教育機構紀要、7、45-56、2016.
37）宮下紘：ビッグデータの支配とプライバシー危機、集英社新書、2017.
38）Graham Greenleaf: The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, Edinburgh School of Law Research paper series, No 2012/12, 2012
39）PopulationdataBC: PRIVACY. https://www.popdata.bc.ca/privacy/policies (2017.11.12参照).