Ⅲ．データエコノミー時代における データ立法政策の課題

――偽名情報の活用，医療情報の安全な処理，情報集合物の結合等を中心に――

全　應睃*
金　知萬**（訳）

Ⅰ．本稿の射程と基本的な考え方

「データ」という用語は個人情報の性格のデータを包括する概念であり，個人情報の範囲が広いため，データ政策は，常に個人情報やプライバシーを念頭に置くべきである。このような観点から，本稿は「データ」と個人情報を同じ意味で使用し，「データ」の意味には常に個人情報が含まれているものとする。

本稿は，韓国の状況を念頭に置き，日本・EU の法制を比較しながらデータの立法政策の争点を論議しようとする。

反対意見はあるものの，韓国の個人情報保護法は，データの収集や第三者提供の要件が日本・EU の GDPR よりも制限的であるため，他の国の場合と比べ，データの偽名化ないし非識別化措置をとって，データを流通する必要性が高いといえる。

韓国は国民健康保険公団，健康保険審査評価院等の公共機関が，医療情報ないし健康情報を膨大な規模で体系的に管理している国の一つである。このような大規模の医療情報を学術的に利用することが重要であるが，敏感情報である医療情報に対するデータ・ガバナンスが未だに（全世界的に）確立されていない状況であり，医療情報をどのような手続によって利用できるかについて議論がある。そこで，医療情報の利用関する紛争事例を紹介し，解決すべきものに

*韓国弁護士。
**韓国大邱広域市議会議員，韓国寿城大学講師，比較法研究所招聘研究員。

ついて議論する。

企業や研究所は，情報集合物（データ・セット）の結合に関心が高い。様々な情報集合物（データ・セット）を特定のキー（識別者）を基準で結合できる場合，データの価値は高くなるが，その過程で特定個人の性向や形態が識別され，プライバシー侵害の問題が生じうる。韓国では，情報集合物の結合ないしデータ連携の問題が多く発生しており，この主題は，偽名情報の活用範囲とともに議論されている。

Ⅱ．データの収集や提供等のデータ取引において発生する問題

１．データ処理の要件

データ処理について，韓国の個人情報法は，opt-out 方式の同意を認めていない点が重要な特徴である。また，韓国の個人情報法は，データの収集，提供，再提供の要件が相違している。データの第三者提供要件は，データの収集要件よりも制限的であって，データの再提供は情報主体の特別の同意あるいは他の法律の特別な規定がある場合にのみ許容され，第三者提供よりも制限されている。

医療情報等の敏感情報の処理もまた，情報主体の特別の同意や，法令において特にデータ処理を要求し，または許容できる場合にのみ可能である。したがって，データ処理に関して個人情報処理者ないし第三者の利益が情報主体の利益より顕著に優れた場合であっても，その事実だけでは，データの再提供ないし医療情報等の敏感情報の処理は，許可されない。

このように，データの収集，提供を処理（processing）という概念によって統一的に規定する EU の GDPR と韓国の個人情報保護法とは多くの違いがあり，「要配慮個人情報」に対する制限的な処理を考慮しても，日本の個人情報保護法よりも厳格な立法例であると考えられる。

２．公開されたデータの収集

（１）情報主体の黙示的，抽象的同意によるデータ処理の可能性

ウェブページ，ブログ等において公開されたテキスト，資料等を情報主体（アカウント所有者）の同意なく収集できるかが問題となる。ウェブページ等のインターネットにおいて公開された情報は，情報主体が少なくとも一定の範

囲で第三者によるアクセスを許容しているから，情報主体の同意なく収集できるという主張が一見すると可能である。しかし，情報主体の意思が単純な閲覧のほか，営利的目的の収集または情報の変形・加工まで許容されていると断定するには困難がある。

一般に，ウェブクローラー等の機械によってインターネット上のデータを大規模で貯蔵する場合には，情報主体にデータ収集の利用目的を告知しないため，情報主体の立場からは，自分の情報がどのように利用されるか全くわからない状況に直面する。このような状況を重要視する見解はウェブページ，ブログ等に公開された情報を情報主体の同意なく大希望として収集する行為がいつまでも適法であると言えないから原則的に情報主体に告知ないし情報主体の同意を得てデータ処理をしなければならないとみている。

（2）著作権侵害の可能性

著作権法では公正利用条項によって解決されるべきである。日本の場合，日本の著作権法の第30条の 4 の第 2 号（情報解釈のための利用）（営利目的である場合でも適用されると解釈される。），日本著作権法第47条の 4 （電子計算機における著作物利用に付随する利用）等が適用される。韓国では，一般的な公正利用（著作権法第35条の 3 ）以外に特別な規定はないから，テキストマイニングやデータマイニングを可能とする公正利用条項を規定しようとする立法的努力が進められている。

（3）個人情報保護法違反の可能性が問題となった事例

韓国大法院は，法律情報の提供サイトを運営しているＹ株式会社がＡ大学の法科大学法学科の教授として在職しているＸの写真，氏名，性別，生年月日，職業，職場，学歴，経歴等の個人情報を上記法学科のホームページ等を通じて収集し，上記法律情報提供サイト内の「法曹人」の項目において有料で提供した事案で，Ｙ社の行為をＸの個人情報自己決定権を侵害する違法な行為とは評価できず，Ｙ社が個人情報保護法第15条ないし第17条に違反したとはいえないと判示した（韓国大法院2016. 8.17. 宣告2014ダ235080判決）。

この事案では，ＹがＸの異議申立てを受けてＸの関連情報を法律提供サイトから削除したため，ＸはＹに対し，過去の行為に対する損害賠償請求のみを提起している。

データ処理の観点から，上記判決の積極的な側面は，個人情報処理者に営利目的があるという事情だけでは，直ちに個人情報処理行為を違法とすることはできないという立場をとった点である。また，既に公開されている個人情報を

情報主体の同意があったと客観的に認められる範囲内で収集，利用，提供等の処理をするときは，情報主体の特別の同意は不必要であると判示して，公開されたデータの処理を一定の場合においては可能であるとした。

しかし，上記判決の消極的な側面も存在する。韓国の個人情報保護法は，利益衡量によって個人情報を第三者に提供できる規定を持っていないため（cf. GDPR 6(1)(f)），大法院はやむを得ず「同意」の枠組みによって判断するしかなかった。情報主体が同意を撤回すると，個人情報処理者はそれ以上データを処理できず，情報主体が要求する場合にはデータを破棄すべきであるから，このような類型の情報提供サービスは持続可能ではないといえる。上記事案も，情報主体が異議申立て，すなわち同意を撤回したため，当該情報主体の情報はそれ以上公開されなかった。

3．個人情報の第三者への提供

（1）データの取引のために個人情報を第三者へ提供することを許容する要件

データの第三者への提供は，国毎に許容要件が相違する。

EU の GDPR は，収集，提供，利用等を処理（Processing）概念にまとめ，第 6 条第 1 項（a）～（f）によって統一的に規定している。

日本の個人情報保護法は，第三者提供時に原則として情報主体の同意を要求しているが，要配慮個人情報を除き，opt-out による第三者提供を許容している。

日本の「AI・データの利用に関する契約のガイドライン」は，データ契約を①データ提供型契約，②データ創出型契約，③データ共用型（プラットフォーム型）の契約に分類し，それによる法律分析を試みている。私見では，上記ガイドラインで提示された契約類型の分類のうち，プラットフォーム型の契約の場合，一般的に考えられるマーケットプレイスの形をプラットフォーム型の契約から除外して，あたかも同業で行われる組合のような形のデータ共用を「プラットフォーム」として定義した点に特徴があるように思われる。

韓国の個人情報保護法は，収集段階よりも第三者提供時のデータ処理要件を厳格に制限しており，たとえば，収集段階で許容できる「利益衡量によるデータ処理」を，第三者提供段階では許容していない。ただし，公共機関の必要による第三者への提供は大幅に許容されている。

収集段階では，「個人情報処理者の正当な利益を達成するために必要な場

合であって，明らかに情報主体の権利よりも優先する場合」に，個人情報処理者が情報主体の同意なく個人情報を収集することができるが（韓国の個人情報保護法第15条），第三者提供の段階では，このような規定がない（韓国の個人情報保護法第17条，第18条）

したがって，韓国の場合，データの第三者への提供要件が厳格であるため，個人情報的性格を帯びたデータを取引するのは非常に難しい状況にある。

（2）データ取引（提供）の不法性が問題となった事例

韓国の場合，個人情報の第三者への提供要件が厳格であるため，データ取引が裏で行われる場合が発生しており，公開の場で取引が行われる場合にも法律要件を満たさないという批判を受けている。

これに関連する最初の事例としては，いわゆる「景品応募券 1 mm 告知」事件に対する大法院判決が挙げられる。（大法院2017.4. 7. 宣告2016ド13263判決）

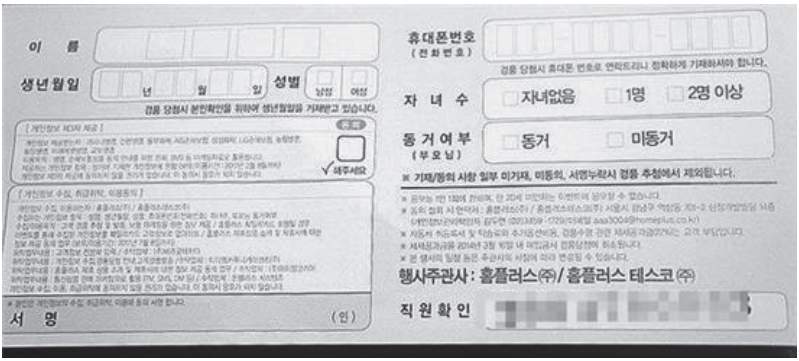
この事案では，大規模流通会社が，景品行事を通じて，顧客の個人情報（氏名，生年月日，携帯番号，子女数，親との同居可否）を収集し，保険会社に 1 件当たり1,980ウォンで販売する事業を企画し，11回の景品行事を通じて約712万件の顧客情報を収集し，第三者提供に関する同意を受け，そのうち約600万件を保険会社に販売して，約119億ウォンの支払いを受けた。

上記流通会社は，第三者（保険会社）への提供の同意に関する文言を景品の応募券の裏面で約 1 mm の大きで記載して景品応募者から同意を受けていたが，これが適法であるかが問題となった。

大法院は，上記流通会社が景品行事の主な目的を隠して，謝恩行事を行うかのように消費者らを誤認させた後，景品行事とは無関係な顧客らの個人情報まで収集し，これを保険会社に提供した点を挙げ，「虚偽やその他の不正な手段や方法で個人情報を取得したり，個人情報処理に関する同意を受けたりする行為」をしたと判示した。

この事案では，保険会社が子女数及び親との同居可否に関する情報の価値を，1 件当たり1,980ウォンと見積もったことが，法経済学的には興味深い点であると考えられる。

実際の経費の応募券の裏面は，以下の通りである。



第二の事例として，ソウル高等法院2019. 5. 3. 宣告2017ナ2074963，2017ナ2074970判決（韓国 IMS ヘルス事件）が挙げられる。

この事案では，薬局の処方箋の管理プログラムを運営している業者（薬学情報院）が，米国 IMS Health Inc の韓国子会社である韓国 IMS ヘルスに対し，2011年から2014年まで韓国国民4,399万人の処方箋関連情報約47億件を約20億ウォンで販売した。

上記処方箋関連の情報には，患者の住民登録番号，性別，生年月日，処方箋の発給機関，医療人の異名及び免許番号，疾病分類記号，処方医薬品の名称，分量及び用法，処方箋発給の年月日等の情報が含まれていた。

米国 IMS Health Inc は，韓国 IMS ヘルスから上記情報の提供を受け，それらは調剤医薬品の市場の推定分析のための統計資料作成に活用された。

薬学情報院は，上記処方箋関連情報に対して，偽名処理水準の単純な両方向暗号化（一種のデータ・マスキング方式であった）をし，また，一般的に信頼できると評価される SHA-512方式の一方向 Hash function を利用した暗号化をして，韓国 IMS ヘルスに提供していた。

このように暗号化された情報が，個人情報保護法上の個人情報に該当するか，それとも匿名情報に該当するかが問題となった。

ソウル高等法院は，単純な方式で両方向暗号化された偽名情報は，容易に復元でき，匿名情報とはいい難く，SHA-512方式の一方向 Hash function と暗号化された場合でも，被告が患者らの住民登録番号を記載し

たマッチングテーブルを保有しており，このようなマッチングテーブルを活用して復元が可能であるとして，なお個人情報とみることができると判示した。

被告らは，情報主体の同意なく個人情報を第三者へ提供するために一定の水準の非識別措置をとっていたが，法院は，上記事案の程度での非識別措置の水準では個人識別の可能性が依然として存在すると判断した。

第三の事例として，政府の「個人情報の非識別措置のガイドライン」発表（2016. 6. 30. 関係組織合同），及びこれに対して市民団体が刑事告発した事案が挙げられる。

韓国政府は，2016年 6 月30日に関係省庁と合同で「個人情報の非識別措置のガイドライン」を発表した。政府は，上記ガイドラインに従い，情報主体を識別できないように非識別措置を適正に行なった非識別情報は，個人情報ではないと推定されるので，ビックデータ分析に活用することができると説明した。

個人情報の非識別措置のガイドラインは，大きく分けて①事前の検討，②非識別措置，③適正性の評価，及び④事後管理で構成されている。上記ガイドラインの核心は，非識別措置と適正性の評価である。

政府が勧告した非識別措置とは，米国の HIPPA プライバシー規則等を参考に，識別者および準識別者を全部もしくは一部削除・代替して，偽名処理，総計処理，データ・マスキング，範疇化等の技法を活用してデータを非識別することである。

このように技術的な非識別措置を取った後で，外部専門家が参加する専門家パネルが，K-匿名性基準を適用して当該非識別措置の適正性を評価する（必要に応じて L-多様性，T-近接性の基準も適用する）。また上記ガイドラインは，中立的な公共機関の性格をもつ専門機関が，他の企業間の情報集対物（データ・セット）を結合することを許容する。

上記ガイドラインは個人情報保護法の委任根拠がないという批判を受けて，これに反対する市民団体は，2017年11月に上記ガイドラインに従い情報集合物を結合した 4 つの専門機関と20個の企業を，個人情報保護法違反として刑事告発した。

検察は，2019年 3 月22日に嫌疑なしとして処理した。検察は，被疑者ら

が政府から提示されたガイドラインに従って非識別措置を取っており，その内容をみても，非識別化された情報は「再識別が顕著に難しい方法」によるものであるから，特定個人が分からないため個人情報に該当せず，さらに，政府のガイドラインによって行為をした以上，少なくとも法律の錯誤として正当化の事由があると判断した。

また，通信社や信用カード会社は，通信記録やカード売上記録を非識別化して第三者に販売しているが，このような営利活動に対しては批判的な世論がある。

４．問題点及び検討方向

（１）解決すべき課題

たとえ個人情報性が薄い，または一定水準の非識別化されたデータであっても，追加情報と結合して特定個人が識別できる可能性があるため，情報主体のプライバシー侵害の恐れは存在するとみるべきであろう。

また，通信社の通信記録や信用カード社のカード売上記録等（派生データを含む）を商業的に販売する行為について，該当情報の価値に実質的に寄与をした情報主体（企業の加入者）に何ら告知もなく，企業がその販売利益を独占することに対しては，不満も存在する状況である。

（２）発表者の意見

法令やガイドラインで厳格に非識別化の基準を設定しても，データ環境（Data circumstance）や文脈（Context）によって情報主体が識別できる可能性は存在するから，このような抽象的な可能性だけを考慮してデータの利用を許さないとはいえないと考えられる。

個人情報保護政策は，絶対的基準の非識別化措置では達成できず，リスク・ベースのアプローチ（risk based approach）によって具体的，個別的に行われるべきであろう。

このような観点からは，匿名化ないし非識別化は，データの物理的性質ではなく，データをどのように利用するかによって決定できる性質のものである（Anonymity is not a property of a data set, but is a property of how you use it(1)）。

（１）“Your Data Were ‘Anonymized’? These Scientist Can Still Identify You”, https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html（2019. 7.27. 접속）

データ販売等によって生じる利益の分配については，当該データの財産権的性格の程度や該当データの敏感度，企業データ加工の水準等を考慮して，さらなる議論がなされるべきであろう。

法律的改善事項としては，韓国の場合，偽名情報の利用ついて明確な規定が必要であり，第三者への提供の際，情報主体とデータ・コントローラー間の利益衡量にもとづいてデータを処理することができる，GDPR6(1)(f)と同じ規定が必要であると考えられる。

Ⅲ．データの安全な利用のための偽名処理等の非識別措置の必要性

１．EU の GDPR の規定

EU の GDPR は，偽名処理等の適切な安全措置を備える場合，公益のための記録保存，学術研究，歴史研究，統計的目的でデータを処理する行為を最初の収集目的と両立するものとみなす（Art. 5(1)(b), Art89(1), Art.6(4)(e)）。

２．韓国個人情報保護法

現行の韓国個人情報保護法は，統計作成及び学術研究棟の目的のために必要な場合，「特定個人を識別できない形」で個人情報を「提供」することができる（第18条第 2 項第 4 号）。上記条項は，データ処理のうち，「第三者への提供」についてのみ規定しているから，データ処理行為全般に関する特例条項はない状況である。

このような状況を改善しようとして，2018年11月15日に偽名情報に対する特例等を規定した法律改正案が国会に提出されたが，市民団体の反対と，国家人権委員会の修正勧告の意見表明があった。

現行法第18条第 2 項第 4 号の「特定個人を識別できない形の個人情報」が，解釈上，匿名情報なのか偽名情報なのか議論がある。

目的の範囲では，「統計作成」の範囲には商業的性格の統計作成も含まれるかが論議されている。統計処理は，集合的データ（aggregate data）の性格を有し，特定の個人の行動や判断に使用されるものではないから，偽名化措置，個人に対する再識別禁止措置などの技術的・組織的安定性の確保措置をとるという前提であれば，商業的性格の統計作成も，上記の「統計作成」の範囲に含まれると考えられる（EU の WP29意見も，統計目的には商業的目的も含まれ

るとする）。

「学術研究」目的の範囲について，産業的ないし営利的目的の研究をも含むかに対しては，強い反対意見が存在する。EU の GDPR は，この学術研究の目的は広く解釈されるべきで（should be interpreted in a broad manner），民間が後援した研究（privately funded research）も含まれると説明しているが，このような説明により，企業が商品開発のための営利目的で情報主体の同意ないしその他の適法要件なしにデータを処理することができるとみるべきではないと考えられる。最終的には，営利目的でデータを処理しようとする企業が，情報主体の同意なくデータを処理できる別途の適法要件を揃えているか否か，換言すれば，データ処理に関する個人情報処理者ないし第三者の利益（公益を含む）が情報主体の利益よりも顕著に優越しているかどうかにより，個別的に決定される問題である。

3．日本の個人情報保護法の匿名加工情報

個人情報保護委員会の規則で定められた基準に従って加工された匿名加工情報は，「特定個人を識別できないように個人情報を加工して得られる個人に関する情報」を意味する。

これは，韓国法の「偽名情報」と類似した概念として理解できる。

匿名加工情報の場合，利用目的の制限がないから，匿名加工情報は営利目的で処理できると考えられる。

匿名加工情報の作成時に削除されたデータや加工方法については，安全管理措置を講じなければならず，再識別するために，匿名加工情報を他の情報と照合してはならない義務が課されている。

日本の匿名加工情報で注目される点は，一種の手続の透明性原則が反映されている点である。日本の個人情報保護法は，匿名加工情報を作成したり，第三者に提供したりするときは，当該匿名加工情報に含まれる個人に関する情報の項目は，その提供方法を事前にインターネット等を利用して公表しなければならず，E メールや書面等を利用して当該第三者にその情報が匿名加工情報であることを明示しなければならないと規定するところ，匿名加工情報のデータ処理を一定程度の公開することで，透明性を確保し，当該データを扱う第三者に再識別防止に対する注意義務を喚起させることができるよい制度であると考えられる。

4．発表者の意見

偽名情報ないし非識別化の基準を法令やガイドラインとして客観化することも意味があるけれども，このような基準を絶対化して，いかなる状況であっても機械的に適用することは，リスク・ベースのアプローチや文脈的アプローチ（context based approach）に反すると考えられる。

日本の個人情報保護法の態度と同じく，手続の透明性を強化して情報主体が自身の情報が偽名処理できるという事実を認知できるようにし，必要に応じて監督機関から外部専門家の監査（audit）や個人情報の影響評価（privacy impact assessment）をすることができる制度的措置を備えることが必要であるように思われる。

英国の個人情報監督機関（Information Commissioner's Office；ICO）も，care data 事業が2016年に中断された事例に言及し，ビッグデータ処理の透明性の不足が大衆の信頼不足と結び付き，公共データの共有においても障害となりうると指摘したことがある。

Ⅳ．敏感情報の医療情報の処理

1．法的根拠の明確化

日本は，医療ビッグデータに関する次世代医療基盤法を制定し，認定事業者による匿名加工された医療情報の適正な活用を図っている。

一方，韓国は一般個人情報や信用情報の領域において偽名情報の活用を導入しようとしたが，医療情報の領域では，特殊な立法措置を取っていない状況である。

しかし韓国では，国民健康保険公団や健康保険審査評価院等が非常に体系的で膨大な医療情報を保有しており，公共データ法に基づき制限的に医療ビックデータ事業を展開している。ただし，健康保険審査評価院による保険医療ビックデータの提供事業に対しては，法的根拠の不備やプライバシーの侵害を理由とした批判的な見方も存在する。

医療情報は非常に敏感な個人情報であるから，医療情報に適合したデータ・ガバナンス原則を樹立することが求められる。このような観点で，OECD の Health Data Governace の 8 つの原則（2015），及びそれに基づく法制の枠組み

の主要な考慮事項を参考にする必要がある(2)。

2．一般の個人情報保護法に基づいた医療情報処理の可能性

（1）英国の NHS Royal Free London – Google DeepMind 事例

NHS Royal Free London は，2015年に Google 子会社である DeepMind と，急性腎臓損傷（Acute Kidney Injury；AKI）を探知して警告できる医療サービス「Stream」プロジェクトを進めた。

Stream サービスは，２つの機能を提供する。①患者の12ヵ月間の血液検査を分析して AKI の徴候があったと判断されると，医療陣にリアルタイムで iphone にインストールされた Stream アプリ（app）に警告をする。② DeepMind が管理する Stream サーバーは，患者の過去診療記録を保存して，アプリを介してこれを照会できるようする。

AKI の徴候判断は，DeepMind の AI アルゴリズムを利用するのではなく，NHS が開発した意思決定ツリー（decision tree）のアルゴリズムを利用する。

上記プロジェクトが個人情報保護法に違反したとする批判が起き，英国 ICO は，2016年に上記プロジェクトに対する調査に着手し，結論的には上記プロジェクトが個人情報保護法に重大に違反するものではでないと判断したものの，最初のプロジェクトの開始時に個人情報の影響評価をしておらず，患者に対し，患者の医療情報が DeepMind に伝達されるという事実を十分に告知していなかった点を指摘した。ICO は，Royal Free が上記指摘事項を是正した後で，第三者による監査を受けることを要求した。

それにもとづき，法律事務所 Linklaters が，Royal Free London に対する監査を行い，2018年５月17日に監査報告書を提出した。

上記監査報告書では，上記プロジェクトにはいくつかの補完が必要な事項があるが，①個人情報保護法上，Royal Free は data controller，DeepMind は data processor にあたるところ，② DeepMind は，Royal Free の厳格な統制のもとで患者情報を Stream 事業の目的のみに利用し，③ Stream サービスは，DeepMind の AI アルゴリズムを採用せず，もっぱら NHS が開発した意思決定ツリーのアルゴリズムに従っており，④

（２） OECD, “Health Data governance：Privacy, Monitoring and Research”, 2015

Royal Free 及び DeepMind の関連者らは，患者情報の秘密性や敏感性を明確に理解しつつ適法に行動しているから，Stream サービスは患者情報を安全に保護している，とした。

ただし，Royal Free と DeepMind は，GDPR art. 6(1)(d), 6(1)(e), 9(2)(h), 9(2)(g)で許容された，患者の重大な利益保護，医療目的のために必須の事項，及び Royal Free の法的義務の履行という条件に基づき上記プロジェクトを実施したため，患者に対して，具体的に患者情報の第三者への提供の事実を告知したり，同意を受けたりはしていなかった(3)。しかし，患者には opt-out をすることができる権利を保障していた。

上記事例は，情報主体の事前同意がなければ，このようなサービスを提供できない例と考えられる。

（2）2019年 6 月に米国で提起された，患者の電子医療記録（EHR）の不正利用の疑いに対する class action（Dinerstein v. Google, University of Chicago Medical Center, University of Chicago）

この事案では，シカゴ大学が電子医療記録（Electronic Health Record）を分析するために Google へ患者情報を提供した行為に対し，原告は，state consumer protection law 及び common law 上のプライバシー権が侵害されたと主張した。

原告は，EHR データは IPAA にもとづく非識別措置がされたうえで Google に提供されたといわれているけれども，Google が獲得できる検索結果ないし決済情報等の追加情報を利用すれば，患者が再識別できると主張した。

この事案では，HIPAA の定める非識別化方法の適正性が問題となった。

私見では，原告の論理を拡張すると，患者情報を大手 IT 企業に提供して分析することは全て違法と解される余地があると考えられる。

（3） 厳密には，GDPR の施行前であったため，上記 GDPR 条項に対応する英国の1988年データ保護法の条項に基づいてプロジェクトが実施された。

3．発表者の意見

医療データに関するデータ・ガバナンスは未だに確立されているとはいいがたく，試行錯誤を経ながら段階的に進行されている状況である。

米国の HIPAA のプライバシー規則が客観的に設定した非識別化基準（18個の識別子の除去等）も，具体的，文脈的な状況次第では，再識別の危険を完全には排除できないと考えられる。

最近の論文によると，性別・郵便番号・結婚可否等の人口統計学的な15個の属性が分かれば，99.98パーセントのアメリカ人を識別できるコンピューターのアルゴリズムが考案されたという(4)。

情報集合物（データ・セット）の結合時には，特定のレコードに対するプロパティの数が増加するため，特定個人を識別することができる可能性が高くなるという点についての具体的な研究が必要である。

医療データ活用の必要性は高いが，その逆のプライバシー侵害に対する懸念も高い状況である。英国の NHS-Deepmind 事例は，いくつかのリスク要因にもかかわらず，内外の監査，ログ記録保管等の適切な技術措置や相互運用性が可能なインフラの構築によって，信頼性と透明性を確保しようとする試みとして，参考に値する事例であると考えられる。

（4） Luc Rocher, Julien M. Hendrickx, Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", Nature Communications, 2019