

「医療情報取扱制度調整ワーキンググループとりまとめ」 に対する意見

一般財団法人情報法制研究所 個人情報保護法タスクフォース
板倉陽一郎, 加藤尚徳, 鈴木正朝, 高木浩光

2017 年 1 月 26 日

意見 1

【該当箇所】 p.8

【意見】

本制度が法制化を目指している、匿名加工情報に加工して希望する匿名加工情報取扱事業者に提供する事業（以下、「加工提供事業」と言う。）と、本人のためのサービスである EHR 事業とは、情報管理が混同されることのないよう、明確に区別する必要がある。

【理由】

医療情報匿名加工・提供機関（仮称）が、加工提供事業を行うために、医療機関等から人々の医療等情報を取得し、複数の医療機関等から集めた情報を突合して分析する（匿名加工情報への加工の過程で必要となる分析を言う。）ことが、本人の同意を得ることなく許され得るのは、提供される情報の本人を再識別することが改正個人情報保護法により禁止されており、かつ、分析の結果（分析の過程で得られる情報を含む。）が最終的に統計量に集計されて利用されることのみを目的としていてこそであろう。

これに対し、本件「とりまとめ」p.8 に記載されている、「また、医療情報匿名加工・提供機関（仮称）は、個人別の医療等情報の管理に資するよう、本人の同意に基づき、各個人に最適な医療や健康管理を実現するために医療等情報を個人別にまとめて提供できることとする。」とある EHR 事業は、本人を識別して情報を扱う点で、加工提供事業とは性質が根本的に異なるものである。

p.8 のこの記載は、加工提供事業と EHR 事業とを同時に行ってよいとする旨であると理解したが、この 2 つが区別なく混同して行われることにはリスクがあり、そのような危うい状況では、加工提供事業は安易に許されるべきでない。

性質の根本的な違いとは、具体的には、一つには、加工提供事業においては、収集する情報に対して「正確性の確保」（個人情報保護法 19 条 1 項）はさほど厳格には求められない（なぜなら、加工提供事業で取り扱う情報は本人に対して何ら影響を及ぼさないことを前提としていることから、本人に権利利益侵害

をもたらさないからである。)のに対し、EHR 事業では、本人に医療等情報をフィードバックすることになるため、言うまでもなく厳格な正確性の確保が求められるという点が異なる。

本件「とりまとめ」では、加工提供事業において、分析の過程で、個人ごとの何らかの属性情報が推定されたとき、例えば、特定の重大疾患に罹患するリスクが極めて高いと判明したときに、本人（又は本人が受診している医療機関等）に当該情報をフィードバックすることが、この制度において許されるのか許されないのかが明らかにされていない。この点が曖昧なままでは、最終的に統計量に集計することのみを目的としているからこそ本人同意なく収集・突合・分析することが許されるという、前提が崩れることになる。

他方、分析結果を本人にフィードバックして、「各個人に最適な医療や健康管理を実現する」ことは、EHR 事業として行えばよいことであり、加工提供事業の中で行う必要がない。

以上の理由から、まず、加工提供事業と EHR 事業とを明確に区別するべきである。前掲の p.8 の記載は、これらを混同して一体的に行うことを許すかのような書き振りであり、看過できない。両事業を同じ機関が同一システムを共有して行うことは認められてしかるべきと考えられるが、ルールの異なる 2 つの事業を同時に行うものとして整理し直すべきである。その上で、加工提供事業においては、本人へのフィードバックは行わないことをルールとして定めるべきである。

また、前掲の p.8 の記載は、医療情報匿名加工・提供機関（仮称）が、EHR 事業も同時に必ず行わなければならないことを意味したものではないことを確認したい。

意見 2

【該当箇所】 p.20

【意見】

医療情報匿名加工・提供機関（仮称）は、安全管理措置として、氏名・生年月日・住所等を削除した仮名化データのみを保有するべきであり、また、「医療情報等の破棄」を実現するために、情報の提供元である医療機関等で対応表を管理する連結可能匿名化の仕組みを用いるべきである。

【理由】

本件「とりまとめ」は、p.20 において、「本人が、医療情報匿名加工・提供

機関（仮称）に対して、医療情報等の破棄（データベースからの消去）を求めることを可能とする。」としているが、削除の要求を受けたとき、どうやって当該本人のデータを特定するのか。氏名・生年月日・住所等の情報を用いるということか。また、本人確認はどのように行うのか。

医療情報匿名加工・提供機関が、氏名・生年月日・住所等の情報を保有するのとも明らかでない。この機関は、健康医療に係る個人のあらゆる情報を突合して蓄積することになるから、情報漏洩は重大な権利利益侵害を引き起こすという大きなリスクを孕むものであるから、安全管理措置の一つとして、氏名・生年月日・住所等の情報を保有せず、仮名化した個人データで扱うべきである。

仮名化した個人データで扱う場合にも、本人からの削除の要求に応じるべきであり、要求された個人データがどれであるかを特定するために、情報の提供元となった医療機関等に協力を求めることができるようにするべきである。

また、本人はどこに削除の要求をすることになるのか。本人にとって医療情報匿名加工・提供機関（仮称）は遠い存在であって、削除をどこに求めればよいかかわからず、制度に対する不信感を持たれてしまうことが懸念される。本人に近い存在は本人が診療等を受けている医療機関等であるから、そうした医療機関等に求めることができる体制とするべきである。また、そのようにすれば、必要な本人確認は自然な形で行われることになる。

要求を受けた医療機関等は、その要求を医療情報匿名加工・提供機関（仮称）に伝達して、これを受けて削除を実施することになるが、どの仮名化データの削除が要求されているのかを特定するためには、提供元の医療機関等で氏名等と仮名（識別子）との対応表を管理する必要があるだろう。すなわち、従前「連結可能匿名化」と呼ばれてきた方法を用いることができるのではないか。

なお、この場合、医療情報匿名加工・提供機関（仮称）が保有するデータが、仮名化データとなり、当該機関においては個人情報保護法の（保有）個人データ（個人情報）に該当しないものとなり得るかもしれないが、提供元で個人データに該当するものの提供を、本制度の下で受けたものであることを理由に、当該機関においても（保有）個人データに該当するものとみなして、本人からの開示等の請求等への対応を含み、個人情報保護法の義務を適用する制度とするべきである。

意見 3

【該当箇所】 p.20 脚注 11

【意見】

脚注 11 で、医療情報匿名加工・提供機関（仮称）が匿名加工情報ではない医療等情報の提供を可能としている理由は、個人情報保護法の適用除外の考え方を逸脱しているのではないか。

【理由】

本件「とりまとめ」は、p.20 において、「医療情報匿名加工・提供機関（仮称）は、「原則として利活用者に対して匿名加工情報を提供することを想定しているが」としつつ、「第三者との関係において、個情法における本人の同意を不要とする例外規定や適用除外に関する規定等に該当する場合には、当該第三者に対して本人の同意なしに匿名加工情報ではなく医療等情報を提供することが可能である」としていることについて、脚注 11 は、「大学その他の学術研究を目的とする機関等（中略）に対して医療等情報を提供する場合には、個人情報保護委員会はその権限を行使しないこととなる」と、現行法 35 条 2 項の規定を示している。

しかし、委員会が権限を行使しないことは違法性の有無とは無関係である。委員会が権限を行使しないことをもって、違法行為を推奨してよいものではない。現行法 35 条 2 項は、違法だが個人情報保護委員会が執行しない、ということのを奇貨として、事業として日常的に違法な提供を行うような状況を想定していない。脚注 11 の記述は、個人情報保護法の理解を誤ったものではないか。

意見 4

【該当箇所】 p.8

【意見】

医療情報匿名加工・提供機関（仮称）は匿名加工情報に該当しない統計情報の提供を可能としているのか、明らかにされたい。

【理由】

医療情報匿名加工・提供機関（仮称）は、匿名加工情報に加工して提供し、提供先に匿名加工情報取扱事業者としての義務（識別行為の禁止）が課されることを前提として、そのための情報の取得・蓄積・突合等が認められているものと理解している。では、匿名加工情報に該当しない統計情報に加工して提供することは、認められるのか、認められないのか、明らかにされたい。

瓜生和久編著「一問一答 平成 27 年改正個人情報保護法」（商事法務）によれば、「統計情報については、『個人に関する情報』とはいえないことから」とし

て、匿名加工情報には当たらないとしている。統計情報に加工されると、提供先に匿名加工情報取扱事業者としての義務がかからないことになるが、医療情報匿名加工・提供機関（仮称）にそのような提供を認めてよいのか。

意見 5

【該当箇所】全体

【意見】

医療情報匿名加工・提供機関（仮称）に集中するリスクを低減するため、将来は、暗号を用いたプライバシー保護データマイニング技術を導入することや、集中型ではない分散型の医療 ICT 基盤を目指していくべき。

【理由】

本件「とりまとめ」が提案する構想では、医療情報匿名加工・提供機関（仮称）にあらゆる人々のあらゆる情報が集められ、突合され、継続的に蓄積されることになる。大量のデータ流出といった事故が起これば、重大な権利利益侵害が発生することになるから、そのような事態を完璧に防ぐ万全の安全管理措置が計画されているのであろう。しかし、本来は、そうした事故を防ぎ切れなくとも、被害が最小化されるような仕組みの構築を検討するべきではないか。

例えば、複数の医療機関等に跨って保有されている同一人の医療情報等を突合して分析することは、準同型暗号を用いたプライバシー保護データマイニング（Privacy-Preserving Data Mining、PPDM）技術を用いれば、本件「とりまとめ」が提案するような、データを実際に一箇所に集める必要がない。現時点では、そのような技術が実用化されていないので、その実用化を待たずに、医療情報匿名加工・提供機関（仮称）を先に実現していく必要性は理解できるが、将来には、リスクを低減するため、こうした高度な技術を導入して、情報の集中を避けることも計画していくべきではないか。

また、そうした技術をまだ用いることができないにしても、データを分散させて管理する別案もあり得たのではないか。医療情報匿名加工・提供機関（仮称）は、データが必要とされる前から、あらゆる人のあらゆる分野の情報を集めて準備しておく方式であるがゆえにリスクが高いが、分野ごとに蓄積されているデータを、必要に応じて医学研究者等が必要最小限のデータを集めて突合し、分析を終えたらデータを返却するといった仕組みも考えられ、そちらの方がリスクが低いと言えるのではないか。そうした別案も検討していくべきではないか。