匿名化分科会報告書

（分科会報告・提言書案）

平成 29 年 1 月 20 日
匿名化分科会

【匿名化分科会報告・提言書案】

メディカル IT セキュリティフォーラム代表理事
愛知医科大学医療情報部長・特任教授
深津　博

1. 医療機関における患者個人情報の匿名化について

医療機関における患者個人情報の取扱いについては、大きく二つの観点から論じる必要性があると思われる。すなわち個人情報保護の観点からの匿名化と、外部・内部不正による情報漏洩対策としての匿名化である。

これらの二つの要件は相互に密接に関連するが、その取扱いや運用、ポリシーは本来別個のものであり、それぞれ別々に検討すべき性質のものである。しかしながらこれらの観点がしばしば混在して整理されないまま議論されている現状があると感じられる。

本提言は、上記のような視点から医療機関における患者個人情報の取扱いについて、改正個人情報保護法および関連するガイドライン等を順守することを前提として、医療機関において検討すべき事項、最低限求められるルール策定と運用上の検討事項について検討し、医療機関およびその運用責任者に対して提言を取りまとめたものである。

2. 個人情報保護の観点からの匿名化

1）個人情報保護法改正

2015 年 9 月に成立した改正個人情報保護法では、2005 年以降施行されて来た従来の個人情報保護法と比較して、医療分野においてもいくつかの点が大きく変更となっている。

具体的には、死者の個人情報も保護対象となったこと（個人情報等と記載）、病歴を含む個人方法は要配慮個人情報として特段配慮すべき情報として分類され、収集および第三者提供に際して、原則個別同意（オプトイン）が必要となった点である。

また同改正法では匿名加工情報の定義もなされ、個人を特定できないような加工をされた情報は個人情報ではない、とされた。具体的にどのような処理を行うかについては、個人情報保護委員会からのガイドライン（匿名加工情報編）によって詳細が規定されている。

すなわち匿名加工情報とするためには、

1. 個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること
2. 個人識別符号の全部を削除すること
3. 個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号
4. 特異な記述等を削除すること（希少性の高い情報：例えば年齢が 116 歳、日本に

数人しか存在しない疾患名等）

5.前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。

の条件を満たす必要がある、とされている。

しばしば誤解されるのは、匿名化と匿名加工情報の関係性である。匿名化は情報の個人識別性を低減させる情報に対する処理・加工の総称であり、一般に匿名化を行っても、非個人情報化できるとは限らない。特に個人識別符号（後述）をデータ自体に含む場合は、一般的な匿名化処理により氏名、性別、生年月日、住所等を削除しても非個人情報化にならない点に留意すべきと思われる。

2)「人を対象とした医学系研究に関する倫理指針」(2015/12)

2015 年 12 月に文科省と厚労省の合同で、「人を対象とした医学系研究に関する倫理指針」が公表された。

この中で匿名化については、「連結不可能匿名化」と「連結可能匿名化」の概念を提唱し、個人を特定できないように個人識別情報である名前や ID 等を削除する匿名化＝「連結不可能匿名化」は個人情報ではなく、また名前や ID 等を別符号に置換えた場合＝「連結可能匿名化」でも、復元するための「対応表」を第三者機関が保有する場合も個人情報ではない、とした。

一方で「連結可能匿名化」で対応表を自ら保有する場合は個人情報を取り扱っているとみなし、保護措置を講じる必要がある、との立場である。

2016 年3月に一部が修正されたが、上記の連結不可能・可能匿名化の考え方は継続されており、現時点ではこの考えに沿った運用が求められている。

3)三省合同会議による検討と、人を対象とした医学系研究に関する研究指針改正案
(2016/8 公開・2016/10/20 一部修正)

2016年4月以降、文部科学省、厚生労働省及び経済産業省で合同開催の「医学研究等における個人情報の取扱い等に関する合同会議」において、関連する複数の法令「個人情報保護法」、「行政機関個人情報保護法」、「独立行政法人等個人情報保護法」および「地方公共団体および効率医療機関等における個人情報保護条例」の整合性を図るべく、検討が行われてきた。

その経過中に、個人情報保護委員会から2016年8月に個人識別符号として、「特定個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの」との定義が公表され、パブコメを経て政令として実施された。

個人識別符号の具体例として、医療分野においては、

（ア）DNAを構成する塩基の配列

（イ）顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌

（ウ）虹彩の表面の起伏により形成される線状の模様

（エ）発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化

（オ）歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様

（カ）手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状

（キ）指紋又は掌紋

が挙げられている。

これらの個人識別符号を含む医療情報は個人情報として扱うべきである、との認識から“氏名等の個人識別情報のみを削除ないし置換したのみでは非個人情報化したことにならない”という考え方であり、合理的帰結と言える。

その結果、新しい三省合同倫理指針には「連結不可能匿名化」、「連結可能匿名化」といった表現は不採用となっており、従来の指針に沿った運用との変更が要求されることとなる。

但しその後の三省合同委員会の検討では、再び連結不可能匿名化を以って非個人情報化とみなし、オプトアウトでの運用を認めるように再修正する動きもあり、今後の展開を注視する必要がある。

4）改正個人情報保護法と三省合同研究指針により必要とされる運用について

改正法では、病歴情報は要配慮個人情報に当たるため、その取得および第三者提供にはオプトインが原則となる。取得に際してはICを含む個別同意について、書式や手続きについてなるべく個別性を確保した形での同意を得るべく、変更・最適化が求められる。

問題は第三者提供の場合である。

改正個人情報保護法によれば、提供する病歴情報に個人識別符号（遺伝子情報等）を含む場合、氏名等の個人識別情報を匿名化したのみでは、非個人情報化したことにはならない。従ってデータから個人識別符号を削除するか、オプトインを取得するかの二者択一となる。

ただ例えば遺伝子情報を研究している第三者にとって、遺伝子情報を削除されては、そのデータの価値はほぼゼロとなってしまう。

従って研究推進を阻害しない形で第三者提供を合法的に行うためには、オプトインを随時取得できる必要性が発生する。

オプトイン取得時の前提としては、初回の個人情報取得時に第三者提供の対象となり

得る施設名や個人名等をできるだけ特定して列挙しておくことになるが、研究の遂行中に新たな第三者提供先が発生した場合には、その都度患者本人のオプトインを取得する必要があり、ここに具体的なソリューションが必要とされる。

利用目的の変更については、同一医療施設・研究機関が利用する場合で、新たな利用目的が合理的に十分な関連性があると認められる場合は通知または公開での対応を、関連性がなくとも特に公衆衛生上必要であると思われる場合はオプトアウトでの対応が例外的に認められているが、十分な関連性がない場合や公衆衛生上特に必要があるとは言えない場合には、やはり随時オプトインが必要となることになる。

5）統計的希少性発現について

希少な病名等は他の情報（居住地や性別、年齢等）と組み合わせることによる個人を特定できる情報となる可能性があるものであり、その状況は個別の状況によりダイナミックに変化しうる。

これを仮に「統計的希少性発現」と名付けるとすれば、一定の統計的な範囲で希少性があると認められた段階で、個人識別符号に準じる形で保護対象とすべきであろう。これについても、希少性発現の閾値を設定して、必要時に個人識別符号として取り扱えるようなシステム的な対応が必要となろう。

3. 外部・内部不正による情報漏洩対策としての匿名化

現行の個人情報保護法では、個人の氏名等を削除ないし符号化すれば匿名化が成立し、非個人情報化が実現できた。従って匿名化により当該情報が万が一流出しても個人情報の漏洩には当たらず、情報を管理する側としてはリスクをヘッジする有力な手段と言えた。

しかるに改正法や新研究指針においては、従来の考え方の匿名化を行っても個人情報のままであるため、漏洩したら依然個人情報の漏洩に該当する。

従って個人情報漏洩のリスクヘッジとしての意味付けは、改正法施行後はほぼ皆無となるであろう。逆に匿名化を以て漏洩対策を行ってきた機関は、運用も含め全面的に見直さざるを得ない状況となることが考えられる。

個人情報保護委員会からは、「高度に暗号化した個人情報」の場合は、漏えいしても届け出は不要であるとの見解を公表しており、本目的に関しては匿名化より暗号化を主たる対策として位置づけるべきであろう。

4. 匿名化と仮名化について

上記のように個人情報から氏名等を削除もしくは符号化したのみでは、個人情報のままであることが考えられるため、従来一般的に受け入れられてきた「匿名化」自体の定義が事実上変更されることになる。

すなわち“匿名加工情報”とは「個人を特定できない状態に加工された情報」ことであり、氏

名・住所等の「個人識別情報」に加え、「個人識別符号」をも削除・別符号化することが必要条件となるからである。

医療で扱う病歴等の要配慮個人情報ではない場合、上記の新しい厳密な匿名化を行い本人の許可なく別目的利用や第三者提供を自由に行う方法が確保されたことになるが（個人情報保護委員会への届け出が必要）、医療系の場合は上述の事情から厳密な匿名化は利用目的自体をスポイルする可能性があり、現実的な選択肢となりにくい。

従来の匿名化は「仮名化」等の呼称での再定義が必要と思われるが、この処理には引き続き一定の意味があると考えられる。

即ち、学会発表や論文発表等の場合、医学部・看護学部等で学生教育に教材として患者データを用いる場合などである。

また将来的に研究・教育目的以外の目的として、製薬会社や化粧品会社、保険会社、マーケッティング会社等にデータを提供する場合、仮名化することを条件にオプトインを取得しておくことにより、患者にとっての情報提供に関するハードルを一段階引き下げる効果も期待できる。

5. 国際標準への適合：「欧州統一個人情報保護法（GDPR）」

2018年5月から開始されるEUにおける個人情報の取扱いの統一ルールであり、違反した場合EU域外の企業等に対しても最低で1000万ユーロの罰金を課す、という厳しい強制力を有するものである。

特にGDPRでは、従来の「匿名化情報」であっても「個人情報」とみなすため、EUの住民の個人情報を取扱う場合には、他地域の企業・法人に対しても同様の取扱いを要求する。

また「十分な情報保護の仕組みが担保されていない第三国への、欧州内の個人情報を移転することを禁ずる」との条項もあり、今後医学分野においても国際共同研究等において、国際的な標準企画への適合が必須となってくる可能性が高い。

既に米国においては、2015年10月の欧州司法裁判所による「セーフハーバー協定無効判決」と、その後に発覚したいわゆる「スノーデン事件」により、EUのルールへの適合を進めている状況がある。

このような状況の中で、我が国においてもEU、米国等世界的な潮流に適合する必要性は高い。

特に遺伝子研究等においては国際共同研究が標準的な枠組みとなっており、個人情報の取扱いに関する見解の相違で、国際的な枠組みからはずされるような事態は避けるべきであると考えられるからである。

我が国の複数の学会や大学等の研究機関から、三省合同委員会の研究指針案について、個人情報の定義や匿名化のあり様、オプトインとの関係性について、上述のような厳格化に対して否定的な意見が相次いでいるが、世界標準への対応と、現場の研究遂行における運用変更やシステム的な対応に要する手間暇・費用等を比較した場合、どちらが重要であるかは論

を待たない。

6. 以上の状況把握と分析から、当フォーラムとしては以下の提言を行う。

① 医療分野における患者個人情報は要配慮個人情報として、取得・第三者提供においては個別同意（オプトイン）を取得すべき対象であることを明確に認識し、各組織において運用方法を適合させるべきである。

② 個人識別符号を有するデータは、氏名等を削除しても依然個人情報であることを明確に認識し、従来の匿名化処理では、本来の意味での匿名化とはならず、個人情報として取り扱うべく、運用方法を適合させるべきである。

③ EU、米国等を含め個人情報の取扱いに対する考え方が厳格化・個人の権利保護の方向に変化する潮流を認識し、研究者の目先の利便性の追求を優先して、世界的な標準への適合を怠ってはならない。