（一社）日本画像医療システム工業会規格

ＪＥＳＲＡ　ＴＲ－００４５－2018

制定　2018年 11月 15日

画像医療システムにおける匿名化技術ガイド

Anonymization Technique Guide for Image Medical Systems

（一社）日本画像医療システム工業会

目次

１．はじめに

医療の進歩のためには医療情報の利活用は不可欠である。現在の医療水準が達成されているのは、過去の医療情報の蓄積と分析、すなわち利活用が行われてきた成果である。もし医療情報の利活用が制限されるようなことがあれば、それは今後の医療の進歩を妨げるものであり、社会的利益の喪失を意味する。

他方、患者のプライバシーを守ることは、医師に課せられた守秘義務に代表されるように、医療情報管理の必須要件である。誰しも自身の不利益になる情報の公開は望まないし、場合によってはその患者の家族にまで影響が及ぶ可能性がある。したがって、医療情報管理には高度な安全性が要求される。

これら利活用と安全管理を両立させる対策として情報の「匿名化」がある。平成 29 年 5 月 30 日全面施行された改正個人情報保護法において「匿名加工情報」が規定され、医療情報のみならずパーソナルデータを含むビッグデータの利活用の推進の上で、「匿名化」の重要性が高まっている。

本書では、医療情報の「匿名化」に関しての社会的背景や技術的内容について解説する。

２．目的と適用範囲

本書は、JIRA 会員企業に対し、医療情報の利活用における匿名化についての社会的な要求と技術的な内容について解説するものである。JIRA 会員企業向けということで、医療情報の内、画像医療システムが取り扱う DICOM 画像データ、読影レポートを主な対象としている。JIRA 会員企業が製造・販売している機器から出力される画像データやレポートデータなどを、医療機関が何らかの目的のために匿名化を行う際に、医療機関から JIRA 会員企業に対して情報の匿名化の技術的対応要求、あるいは業務委託がある場合に、それに対応するための情報提供を目的としている。また、医療機関から匿名加工情報や非個人情報の提供を受ける場合の取り扱い方についても解説している。

JIRA 会員企業になじみの深い利活用ユースケース例には、

- 臨床画像・レポートの症例データベースへの提供
- 臨床画像・レポートの学会での発表
- 臨床画像・レポートの教育への利用

が考えられる。

利活用にあたって、匿名加工情報を提供する時のリスク分析は、情報提供者（医療機関）が用途・提供先組織・利用形態で判断することであるが、医療情報システム事業者として関与する場合には、本章末に記載している資料等により理解を進めておくことを推奨する。

さらに、JIRA 会員企業が「医療機器・システム機能のテストデータとして診療情報の提供を受ける」場合は、JIRA 会員企業側が当事者になることから、手法や制度的体制につい

ての理解が必須である。すなわち、改正個人情報保護法の内容に従うこととなる。このケースは民間事業者による事業用途であるが、市場への機能提供によって最終的には社会的利益＝公益が発生することを提供側に理解してもらうことが望まれる。

本書においては、医療施設からデータ提供を受ける JIRA 会員企業は、「匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者」に該当し、JIRA 会員企業にデータを提供する医療施設は、「匿名加工情報を作成する個人情報取扱事業者」に該当する。

なお、本書は医用画像情報の基礎知識と、以下の法令、政令、ガイドラインに関する基礎知識を持っている方を対象とする。

1) 個人情報の保護に関する法律（平成 15 年法律第 57 号)、以下「法」と記す。（平成 27 年 9 月改正）
2) 個人情報の保護に関する法律施行令（平成 15 年 12 月 10 日政令第 507 号）（平成 28 年 10 月改正）
3) 個人情報の保護に関する法律施行規則（平成 28 年 10 月 5 日個人情報保護委員会規則第 3 号)、以下「規則」と記す。
4) ガイドライン・QA 等
   4-1) 個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年 11 月）（平成 29 年 3 月一部改正）
   4-2) 個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編）（平成 28 年 11 月）
   4-3) 個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）（平成 28 年 11 月）
   4-4) 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）（平成 28 年 11 月）（平成 29 年 3 月一部改正）
   4-5) 個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）
   4-6) 「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ（平成 29 年 2 月）（平成 29 年 5 月更新）
5) 厚生労働省発行
   5-1) 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（平成 29 年 4 月）
   5-2) 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に関するＱ＆Ａ（事例集）（平成 29 年 5 月）

6) 内閣官房発行

6-1) 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についてのガイドライン　Ⅲ．匿名加工医療情報編 2018 年 5 月

３．医療情報の適切な取り扱いについて

3.1 改正個人情報保護法における医療情報の取り扱い

3.1.1 医療情報は要配慮情報

改正個人情報保護法においては、“要配慮個人情報”が「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの」として定義され、本人同意を得ない取得を原則として禁止されている。さらに、オプトアウト手続きによる第三者提供も認めていない。

法律施行令によって、要配慮個人情報は、以下のように記されているので、所謂「医療情報」は要配慮個人情報として扱われる。

（ア） 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会で定める心身の機能の障害があること

（イ） 本人に対して医師その他医療に関連する職務に従事する者により行われた健康診断その他の検査の結果。

（ウ） 健康診断その他の検査の結果に基づき、又は疾病、負傷その他の心身の変化を理由として医師その他の医療に関連する職務に従事する者により心身の状態の改善のために指導又は診療若しくは調剤が行われたこと

（エ） 犯罪関連（省略）

（オ） 非行関連（省略）

3.1.2 医療情報の第三者提供について

医療情報の第三者への提供は、原則として本人同意のもとで行わなければならない。明示的に同意行為を伴わなくても“同意がなされている場合”は、「医療・介護関係事業者における個人情報の適切な取り扱いのためのガイダンス」に第三者提供の特例（黙示の同意）として、“（３）本人の同意が得られていると考えられる場合” “別表２” が挙げられているが、あくまでも医療サービスの提供に限定されている。

医療情報の匿名化、匿名性の判断、責任はデータ提供元である医療機関にある。今回の法改正において“提供者基準”が明確化された。

医療情報の匿名化の処理を外部事業者に委託することは、適切な委託契約の元で可能である。

3.1.3 匿名化処理の業務受託について

匿名加工情報への加工あるいは、非個人情報への匿名化処理は、医療施設等が実施し、事業者等に提供する。医療施設等での匿名化処理は、事業者等に委託することも認められている。この場合、加工を受託した事業者と加工された情報の提供を受け利用する事業者が同一の場合もありえる。このため、別契約等にして、同一の事業者でも別なものとして、管理することが必要になる。

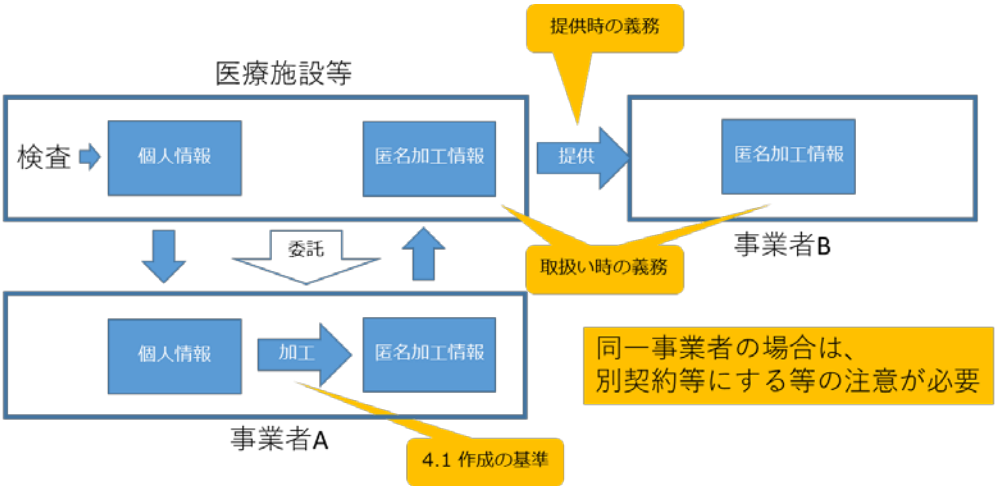


図 3.1　匿名加工の業務委託と匿名加工情報の提供

3.1.4 商業利用についての医機連 Q&A

一般社団法人 日本医療機器産業連合会 法制委員会から、医療機関から医療機器・システムベンダが医療情報の提供を受ける際の要点が公表された（平成29年7月24日）。以下に、そのままの形で掲載する。

Q：医療機器のカタログへの画像等の掲載について、
・個人を特定する氏名やIDを削除していますが、個人情報に該当しますか。
・また、施行前に入手した情報について、改めて、同意を取る必要があるでしょうか。
A：医療機関において、個人が特定できないように処理され、特定の個人を識別できない情報は、個人情報に該当しないと考えられます。
なお、氏名やＩＤを削除しても、個人が特定されるような情報が含まれる画像や症例、年齢等が含まれる場合は、要配慮個人情報に該当しますので、これらは使わないようにする必要があります。
　また、施行前に取得した個人情報であって、施行後に要配慮個人情報に該当するものでも、施行前に適法に取得された個人情報であれば、改めて同意を取る必要はありません。

Q：機器メーカー（医療機器製造販売業者等）が展示会や製品カタログで用いるために

用いる診断画像等を医療機関から提供を受けるためには、どのような手続きを行えばよいでしょうか。 Ａ：医療機関より、個人が特定できないように処理された情報として提供を受けることにより、個人情報に該当しないものとして扱うことができます。

3.1.5 外国への第三者提供について

外国における第三者への提供の制限については、今回の改正で新設された内容である。以下、個人情報保護委員会ガイドライン（外国にある第三者提供編）に従って説明する。

個人情報取扱事業者は、外国にある第三者に個人データを提供する場合には、法第 23 条第 1 項各号に該当する本人同意不要の場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。

「委託」、「事業承継」、「共同利用」に当たっては、本人同意を得る、あるいは以下に該当する場合においては認められている。

①当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則で定める国にある場合

②当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則で定める基準に適合する体制を整備している場合

医療情報は要配慮情報であり、国内と同様にオプトアウトによる第三者提供は認められていない。

外国にある第三者とは、例えば、外資系企業の日本法人の外国にある親会社、日本企業の外国法人格を取得している現地子会社　などである。

外国にある第三者に業務委託（例、個人情報の匿名化などの作業委託）を本人同意なく行う場合は、上記の①または②の条件を満たす事業者であることが求められる。業務委託であるので、委託側が管理・監督することも必要である。

この条件に照らせば、海外に拠点のあるクラウドサービスも利用可能に見える。しかし、この条件は“個人情報保護に関しての条件”であり、「医療・介護関係事業者における個人情報の適切な取り扱いのためのガイダンス」の外部保存の項には「医療情報システムの安全管理に関するガイドラインによること」を求めており、当該ガイドラインが準拠を求めている総務省と経済産業省のガイドラインではどちらも「保存義務のある情報は国内法のおよぶ範囲に限定」している。これは、セキュリティの為では無く“行政権”の問題であり、条約締結による解決が待たれる。

3.2 匿名加工情報と非個人情報

「匿名加工情報」と「非個人情報」に関して説明を記す。

改正個人情報保護法の制定にあたり、ビッグデータビジネスの事業者に対して、匿名化処

理されたデータの扱いがグレーであった部分をより明確化し、個人情報の利活用を促進するために「匿名加工情報」が設けられた。

法第 2 条第 9 項において、「匿名加工情報」とは、特定の個人を識別することが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であって、当該個人情報を復元することができないようにしたものをいう。

(1) 第 1 項第 1 号に該当する個人情報

当該個人情報に含まれる記述等の一部を削除すること。

(2) 第 1 項第 2 号に該当する個人情報

当該個人情報に含まれる個人識別符号の全部を削除すること。

つまり、当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることであり、個人情報を加工し、個人を識別できないようにした情報である。

このように「匿名加工情報」を明確に定義し、その作成方法、匿名加工情報取扱事業者の責務も明確にされた。

「匿名加工情報」を作成する個人情報取扱事業者及び匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者が、「匿名加工情報」を取り扱う場合等に遵守すべき義務（法第 36 条～第 39 条）がある。

個人情報取扱事業者は、「匿名加工情報」（匿名加工情報データベース等を構成するものに限る（※1）。）を作成するときは、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、規則第 19 条各号に定める基準に従って、当該個人情報を加工しなければならない。

（※1）匿名加工情報の取扱いに係る義務（法第 36 条～第 39 条）は、匿名加工情報データベース等を構成する匿名加工情報に課されるものであり、いわゆる散在情報となる、匿名加工情報データベース等を構成しない匿名加工情報の取扱いに係る義務は課されていない。

ちなみに、「匿名加工情報」と「匿名化された情報」とは異なる概念である。「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に関するＱ＆Ａ（事例集）に以下のように明記されているように「匿名化」とは手段の一つであり、結果を保障するものではない。「個人情報に該当することもあり得ます。」と明記されている。

「匿名化」は、個人情報から、氏名、生年月日、住所、個人識別符号等、個人を識別することができる情報を取り除くことですが、症例や事例により、匿名化を行ってもなお特定の個人が識別できる場合には個人情報に該当することもあり得ます。他方、「匿名加工情報」については、個人情報を個人情報の区分に応じて定められた措置を講じて特定の個人を識別することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものであり、個人情報保護委員会規則で定める基準に従って加工する必要があります。（「個人情報の保護

に関する法律についてのガイドライン（匿名加工情報編）」（平成２８年個人情報保護委員会告示第９号）参照）

「非個人情報」とは、法的には定義は存在しないが個人を識別できない情報であり、通常は統計処理情報で安全性を確認したものか、極めて少数の項目のみ抜き出し、かつ特異値を除いたものを示し、外部情報を参照しても「容易」に個人を識別出来ない情報のことである。利用にあたり、本人を特定できない“非個人情報”にすれば、その扱いは法の適用範囲外になる。　「匿名加工情報」と「非個人情報」とは、その定義、取扱い等に違いがある。「匿名加工情報」に関しては、法で定義され、その加工情報の作成方法、「匿名加工情報」を作成する個人情報取扱事業者の責務に関して明確になっている。詳細を 4 章に示す。「非個人情報」に関しては、明確な作成方法、責務等は明記されていない。匿名化処理に関しては、DICOM 画像等では本書を参考に個人が識別できない方法で実施する必要がある。

「匿名加工情報」と「非個人情報」との取扱いの関係をまとめると図 3.2 のようになる。

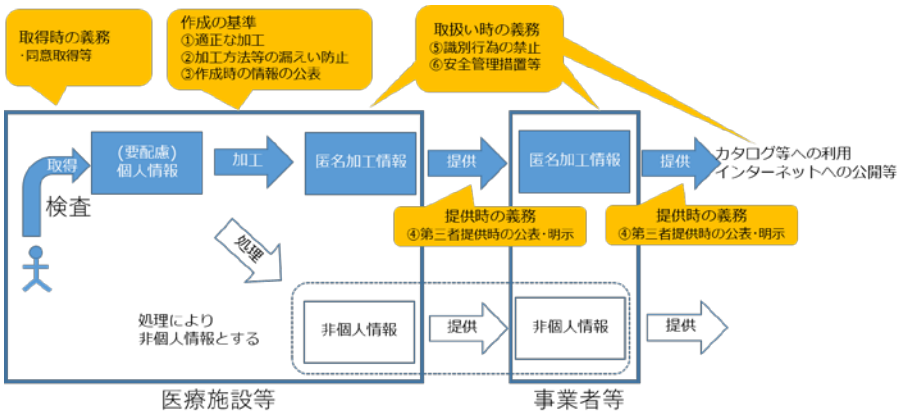


図 3.2　匿名加工情報と非個人情報の取扱い

4. 匿名加工情報に関して

4.1 匿名加工情報の作成の方法に関する基準

法 36 条では、個人情報取扱事業者の匿名加工情報を作成する時の義務を以下のとおり規定している。

> 第 36 条　個人情報取扱事業者は、匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、当該個人情報を加工しなければならない。

この条文の「個人情報保護委員会規則にて定める基準」は、規則第 19 条に該当し、次の（1）から（5）のとおりに定められている。個人情報取扱事業者が匿名加工情報を作成する時は、以下の各号に定める基準に従い、当該個人情報を加工しなければならない。

> （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（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
> （2）　個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
> （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（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）。
> （4）特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
> （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。

なお、加工する情報の性質に応じて、規則第 19 条各号に定める加工基準を満たす必要があるが、こちらの具体的な考え方については、下記文書を参照されたい。

[1] 個人情報保護委員会：「3-2 匿名加工情報の適正な加工（法第 36 条第 1 項関係）」『個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）』2016 年 11 月（2017 年 3 月一部改正）

[2] 個人情報保護委員会事務局：「4. 匿名加工情報の作成に当たって求められる加工」『個人情報保護委員会事務局レポート：匿名加工情報―パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて』2017 年 2 月
[3] 経済産業省：『事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（「匿名加工情報作成マニュアル」）Ver1.0』2016 年 8 月
[4] 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についてのガイドライン　Ⅲ．匿名加工医療情報編　2018 年 5 月

4.2 匿名加工情報取扱事業者等の責務

4.2.1 匿名加工情報取扱事業者とは

匿名加工情報データベース等を事業の用に供している者のうち、国の機関、地方公共団体、独立行政法人の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）で定める独立行政法人等及び地方独立行政法人法（平成 15 年法律第 118 号）で定める地方独立行政法人を除いた者をいう。

4.2.2 匿名加工情報取扱事業者等の義務

「法第 4 章第 2 節」では、匿名加工情報の取り扱いに係る義務について、「匿名加工情報を作成する個人情報取扱事業者」と、「匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者」に分け、遵守すべき義務を規定している。

1) 匿名加工情報を作成する個人情報取扱事業者が遵守する義務等

① 基準に従った適正な加工（法第 36 条第 1 項）
匿名加工情報を作成するときは、4.1 章に記載する方法にて、適正な加工を行わなければならない。

② 加工方法等情報の漏えい防止（法第 36 条第 2 項）
匿名加工情報の作成に用いた個人情報から削除した記述等や個人識別符号、加工の方法に関する情報の漏えいを防ぐため、個人情報保護委員会が定めた基準に従って、安全管理措置を行わなければいけない。

③ 作成時の情報の項目の公表（法第 36 条第 3 項）
匿名加工情報を作成した後、遅滞なく、インターネット等を利用して、作成した匿名加工情報に含まれる個人に関する情報の項目を公表しなければいけない。

④ 第三者提供時の公表・明示（法第 36 条第 4 項）
匿名加工情報を第三者提供するときには、あらかじめ、インターネット等を利用して、提供する匿名加工情報に含まれる個人に関する情報の項目を公表するとともに、提供先に対して匿名加工情報である旨を明示しなければいけない。
個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）により、“匿名加工情報をインターネット等で公開する行為についても不特定多数への第三

者提供に当たるため、上記義務を履行する必要がある”。

⑤ 識別行為の禁止（法第 36 条第 5 項）

匿名加工情報を取り扱う際に、本人を識別する目的で、匿名加工情報を他の情報と照合してはいけない。

⑥ 安全管理措置等（努力義務・法第 36 条第 6 項）

匿名加工情報の安全管理措置や苦情の処理等について、必要な措置を講じ、これら措置の内容を公表するよう努めなければいけない。

2) 匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者が遵守する義務等

① 第三者提供時の公表・明示（法第 37 条）

匿名加工情報を第三者提供するときには、あらかじめ、インターネット等を利用して、提供する匿名加工情報に含まれる個人に関する情報の項目を公表するとともに、提供先に対して匿名加工情報である旨を明示しなければいけない。

個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）により、“匿名加工情報をインターネット等で公開する行為についても不特定多数への第三者提供に当たるため、上記義務を履行する必要がある。”

② 識別行為の禁止（法第 38 条）

匿名加工情報を取り扱う際に、本人を識別する目的で、匿名加工情報を他の情報と照合してはいけない。

③ 安全管理措置等（努力義務・法第 39 条）

匿名加工情報の安全管理措置や苦情の処理等について、必要な措置を講じ、これら措置の内容を公表するよう努めなければいけない。

5 JIRA に関係する医療情報の匿名化について

5.1 DICOM における匿名化

5.1.1 DICOM データの構造と匿名化処理の基本的な考え方

DICOM データは、図 5.1 のように、患者や検査に関する属性情報の値（Value）が、タグ（Tag）、値の形式（Value Representation、以下 VR）とデータの長さ（Value Length）が付帯したデータ要素(Data Element）として記録されている。タグの値（グループ値、エレメント値）は情報の項目ごとに決められており、例えば、患者の ID は(0010,0020)、検査日付は(0008,0020)である。項目ごとのタグ値は、DICOM 規格書 6 巻の「データ辞書（Data Dictionary）」に規定されている。

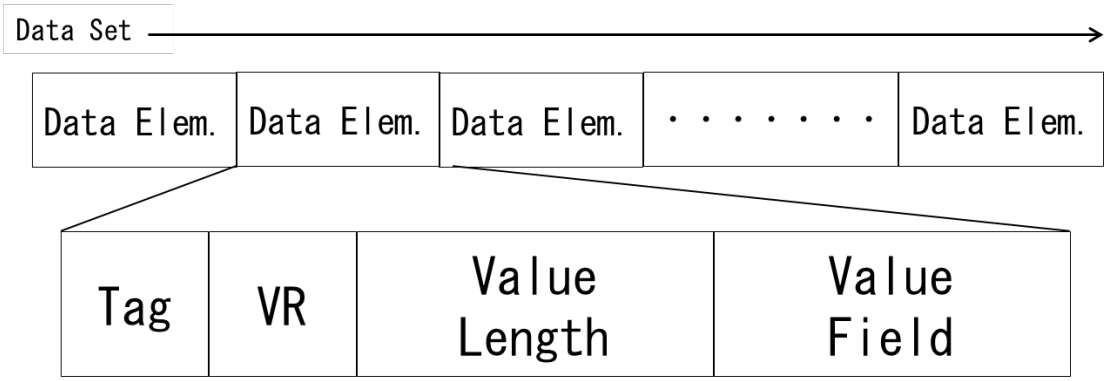


図 5.1 DICOM データ構造

DICOM データ内の患者に関する識別情報を匿名化するということは、単純にその識別情報のタグのデータ要素を取り除けば良いわけではない。DICOM 規格は、タグごとにタイプや値の形式を決めており、単に削除すると DICOM 規格違反のデータになってしまい、その後の処理に使えないデータになってしまうので注意が必要である。

タイプ（Type）に関しては、タイプ 1（Type 1）は必須のデータ要素であり、長さがゼロでなく何らかの値が入っていること、タイプ 2（Type 2）は必須のデータ要素であるが、値が不明ならば長さゼロで値なしにすること、タイプ 3（Type 3）は任意であり、値が不明ならばデータ要素を削除すること等と決められている。したがって、匿名化する際は、これらの条件を満たすように、長さがゼロでないダミー値をセットや値の削除、データ要素の削除など行う必要がある。

値の形式（VR）に関しては、例えば検査日付(0008,0020)は、VR が DA（Date）と定義されており、8 文字固定の文字列で、使える文字は数字のみである。したがって、検査日を匿名化したいということで、"20140101"と入っている値を、"XXXXXXXX"といった数字以外の値に置き換えると DICOM 規格違反となってしまう。

また、VR が SQ（シーケンス）のデータ要素の値は、階層構造がとられていて、複数の

データ要素からなるサブセットを 1～複数含んでいる。匿名化処理の対象となるタグ値のデータ要素がシーケンスに含まれている場合は、そのタグ値のデータ要素全てに対し、処理が必要である。

匿名化の処理の際にセットするダミー値の内容は、本ガイドで規定はしない。その値が患者を識別不能であることは、ダミー値を生成する匿名化ソフトウェアか、それを入力する操作者の責任である。

5.1.2 DICOM の属性の機密性プロファイル

匿名化の際、どのデータ要素を処理するかは、匿名化したデータの利用目的に関連するため、ケースごとに匿名化処理者の責任で判断しなければならない。

DICOM 規格[1][2]における匿名化については、DICOM 規格書 15 巻「セキュリティおよびシステム管理のプロファイル（Security and System Management Profiles）」の付属書 E「属性の機密性プロファイル（Attribute Confidentiality Profiles）」には、教育データ作成等を目的とした匿名化処理として推奨している基本アプリケーションレベル機密性プロファイル（E.2 Basic Application Level Confidentiality Profile　以下 Basic Profile）と、この Basic Profile をベースにして、更に画像の加工や利用目的を考慮して特定の情報削除（Clean）、あるいは、利用目的を考慮して特定の情報を保持（Retain）する 12 の基本アプリケーションレベル機密性オプション（E.3 Basic Application Level Confidentiality Options　以下 機密性オプション）を定義しており、匿名化を行う際の参考になる。

機密性オプション	概要
① Clean Pixel Data Option	画像に埋め込まれた個人情報の削除
② Clean Recognizable Visual Features Option	画像に埋め込まれた個人情報の削除（顔写真，高精細データ）
③ Clean Graphics Option	画像に埋め込まれた個人情報の削除（文字や GSPS）
④ Clean Structured Content Option	レポート構造からの個人情報の削除
⑤ Clean Descriptors Option	検査指示情報からの個人情報の削除
⑥ Retain Longitudinal Temporal Info. with Full Dates Option	日付と日時を保持する（⑦とは排他の関係）
⑦ Retain Longitudinal Temporal Info. With Modified Dates Option	修正した日時を保持する（⑥とは排他の関係）
⑧ Retain Patient Characteristics Option	患者特有の情報を保持する
⑨ Retain Device Identity Option	装置情報を保持する
⑩ Retain Institution Identity Option	医療機関情報を保持する

⑪ Retain UIDs Option	UID 群を保持する
⑫ Retain Safe Private Option	個人情報以外のデータをプライベートデータに保持する

表 5.2 機密性オプション

以下、幾つかのオプションに関して補足する。

① Clean Pixel Data Option

超音波や内視鏡、血管造影、透視といった検査の画像やその他のモダリティを含むセカンダリキャプチャ画像等では、画像データに識別情報が埋め込まれている場合がある。

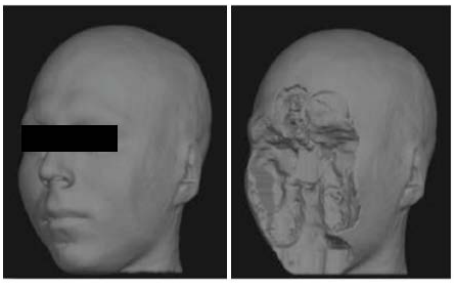
DICOM Conference 2010 David Clunie氏
"De-identification Revisited DICOM Supplement 142" より

識別情報が含まれるかどうかは、Burned In Annotation（0028,0301）の値が参考になるが、このタグは任意であり、基本的に処理者は画像を表示して目視で確認する必要がある。

識別情報が埋め込まれていた場合の画像の加工方法について、DICOM 規格としての規定はなく、識別情報が埋め込まれた周辺部を塗りつぶす（画素値を特定の値に書き換える）ことを推奨する。

② Clean Recognizable Visual Features Option

顔画像は一般に個人を識別するのに十分な情報として考えられ、匿名化の処理が必要である。画像の加工方法について、DICOM 規格としての規定はなく、目線を入れる（目の周辺部の画素値を特定の値に書き換える）ことを推奨する。


DICOM Conference 2010 David Clunie氏
"De-identification Revisited DICOM Supplement 142" より

CT や MR の頭部シンスライスの画像セットは、再構成により顔の輪郭画像の生成が可能であり、患者を識別するに十分な認識可能視覚的特徴を有する場合があると言われている。認識可能な視覚的特徴を有するかどうかは、Recognizable Visual Features(0028,0302) の値が参考になるが、このタグは任意であり、処理者の責任で判断しなくてはならない。

再構成された顔の輪郭画像が含まれる場合は、顔画像の場合と同様に目線を入れることを推奨する。また、シンスライス画像から顔の輪郭画像の生成が可能であり、その画像は患者を識別するに十分と判断した場合は、顔領域にノイズを加

えるようなシンスライスの画像への加工を推奨する。ただし、この処理により、匿名化したデータの利用目的に適さなくなる可能性があり、その場合は、別の加工方法を考える必要がある。

③　Clean Graphics Option

オーバレイデータ(60xx,3000)に識別情報がビットマップデータとして含まれている可能性があるため、原則削除すべきである。

④　Clean Structured Content Option

レポートコンテンツには、施設情報や装置情報、患者特有の情報、検査に関わった医師等スタッフの情報を含む場合があり、処理者はコンテンツの内容を確認し、削除やダミー値への書き換えを行う必要がある。

⑤～⑪は補足事項なし。

⑫ Retain Safe Private Option

装置ベンダが独自に定義したプライベート属性については、その中に識別情報が含まれるかどうかは不明のため、原則削除すべきである。ただし、プライベート属性の中には画像処理等で必要とし、匿名化の際にも保持することが望ましいものもあり、こうした配慮が必要と事前にわかっている場合は、DICOM 規格書 15 巻付属書 E の表 E.3.10-1 Safe Private Attributes を確認して処理を行うべきである。

この Safe Private Attributes にリストアップされたプライベート属性については、下記のいずれかに該当する場合は、識別情報が含まれていないことを装置メーカが保証しており、タグを保持することが望ましい。

- ブロック識別情報ステータス（0008,0303）の値が「SAFE」であるプライベートデータエレメントのブロック内に存在する
- プライベートデータエレメント特性シーケンス（0008、 0300）に含まれる非公開プライベートエレメント（gggg、0004）に含まれる

なお、表 E.3.10-1 Safe Private Attributes は、装置メーカからの要求により継続して更新されているため、常に最新の DICOM 規格書を確認する必要がある。

5.1.3 機密性プロファイルの匿名化処理の詳細

基本アプリケーションレベル機密性プロファイルおよび各オプションにおいて、匿名化を行う際、各データ要素に対してどのように処理するかは、DICOM 規格書 15 巻付属書 E の表 E.1-1. 「アプリケーションレベル機密性プロファイル属性」にて、以下の 6 つのアクションコードで示されている。

D - ゼロでない長さのダミーの値に置換する。値の形式は VR と一致させる。
Z - 長さをゼロにして値をセットしない、あるいは、ゼロでない長さのダミーの値と置換する。値の形式は VR と一致させる。
X - データ要素を削除する。
K - 保持する。（シーケンスでない要素は変更なし。シーケンス要素は消去する）
C - 消去する。識別情報を含まない値に置き換える。値は VR と一致させる。
U - インスタンスとして一貫性のある UID に置き換える。ここでの一貫性とは、例えば同じ検査のデータの場合、Study Instance UID が同じに保つことである。利活用目的によっては一貫性が必須のケースがあるため、注意が必要である。

X/Z/D といった複数の記載のあるものは、匿名化の対象とするデータオブジェクトの種類（IOD）により、タイプが異なることを示しており、X/Z/D は Type 3 であれば X、Type 2 であれば Z、Type 1 であれば D であることを示している。匿名化の際は、いずれのタイプであるかを DICOM 規格書 3 巻で確認する必要がある。

DICOM 規格書 15 巻付属書 E の表 E.1-1 から、Basic Profile における主な属性データ要素の処理方法を表 5.3 に抜粋した。「医療情報の分類」については参考資料[4]を参照のこと。他のデータ要素については DICOM 規格書を参照のこと。

タグ	属性	リタイア	医療情報の分類	処理方法
(0008,0018)	SOP インスタンス UID	N	準識別子	U
(0008,0020)	検査日付	N	準識別子	Z
(0008,0050)	受付番号	N	準識別子	Z
(0008,0080)	施設名	N	準識別子	X/Z/D
(0008,1010)	装置名	N	準識別子	X/Z/D
(0008,1030)	検査内容	N	半静的属性	X
(0008,1070)	操作者名	N	準識別子	X/Z/D
(0010,0010)	患者の名前	N	識別子	Z
(0010,0020)	患者のID	N	識別子	Z
(0010,0030)	患者の生年月日	N	準識別子	Z
(0010,0040)	患者の性別	N	静的属性	Z
(0010,1010)	患者の年齢	N	半静的属性	X
(0010,4000)	患者コメント	N	半静的属性	X
(0018,4000)	収集コメント	Y	半静的属性	X
(0020,000D)	検査インスタンスUID	N	準識別子	U
(0020,0010)	検査ID	N	準識別子	Z

(0032,4000)	検査コメント	N	半静的属性	X
(60xx,3000)	オーバーレイデータ	N	半静的属性	X
グループ番号が奇数	プライベート属性	N	半静的属性	X

表 5.3 主な属性データ要素の処理例

収集コメント(0018,4000)のように、現在はリタイアされているデータ要素にも対応が必要である。 リタイアは、規格書上の記載が抹消されて、規格書のメンテナンスの際に考慮されなくなった状態を示すが、使用を禁止したものではないため、匿名化の対象データに含まれている場合がある。

5.1.4 匿名化の処理内容の記録

DICOM データの匿名化を行った際、そのデータが匿名化処理済みであること、また、その匿名化の際にどのような処理を行ったかを以下のタグを使って記録することができる。この記録は必須ではないが、記録することを推奨する。

タグ	属性	Type	VR	説明
(0012,0062)	Patient Identity Removed	3	CS	匿名化処理が行われたデータかどうかを示す情報 "YES" : 匿名化されたデータ、"NO" : 匿名化されていないデータ タグが存在しない場合は不明として扱われる（匿名化されている可能性もある）
(0012,0063)	De-identification Method	3	LO	匿名化の方法 (0012,0062)が"Yes" かつ (0012,0064)が存在しないか有効値でない場合に必須。 どのような匿名化の処理を行ったかをテキストデータで記述する。
(0012,0064)	De-identification Method Code Sequence	3	SQ	匿名化方法コードシーケンス (0012,0062)が"Yes" かつ (0012,0063)が存在しないか有効値でない場合に必須 5.1.2 で説明した Basic Profile と機密性オプションの組み合わせで匿名化を行った際、その組み合わせをシーケンスデータとして記録する。セットする具体的な値については、DICOM 規格書の PS3.16 CID 7050 "De-identification Method" を参照。

表 5.4 匿名化処理記録タグ

5.1.5 その他の注意事項

1）複数画像からなる 1 検査分の画像データ、画像データと読影レポートなど匿名化する際は、個々のデータ間で匿名化後の各種値（UID、日付に関するデータ、患者に関するデータ等）に整合性をとる必要がある。

2）PDI および DICOM メディアに保存されているデータ一式を匿名化する場合、匿名化の際にセットしたダミー値をもとに、索引ファイルに相当する dicomdir の更新も必要である。 この整合がとれなくなると、メディアからのデータの読み出しが行えなくなる場合がある。

3）DICOM データには、患者以外に、医師やそのほか医療スタッフの識別情報が含まれる場合がある。これらも個人情報であり、患者情報と同様、匿名化する必要がある。

なお、「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についてのガイドライン　Ⅲ．匿名加工医療情報編」[4]の「4-5 医療情報特有の匿名加工」に医療画像の匿名化の説明があるので参考にすること。

【5.1 の参考資料】

[1]NEMA DICOM Standard
http://www.dicomstandard.org/
[2] JIRA「DICOM の世界」
http://www.jira-net.or.jp/dicom/index.html
[3] David Clunie's Medical Image Format Site
http://www.dclunie.com/
[4]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についてのガイドライン　Ⅲ．匿名加工医療情報編 2018 年 5 月

5.2 k-匿名化

米国 HIPAA では個人の同定が不可能なデータとは「個人を同定せず、かつ個人を同定するのに用いることができる情報であると思うような合理的根拠が全くない」データとして定義されるが[1]、この要件を満たすためには公開されたデータが単独あるいは他の公開情報との組み合わせに対しても、個人の同定のリスクが小さいことが要求される。

例えば、次のような例が考えられる[3]。図 5.2-1 では医療データが氏名と住所を削除された状態で公開されている。しかし、氏名および住所が公開されている選挙人リストを利用することで誕生日、性別、ZIP コード（郵便番号）から個人を特定することができ、したがって個人の医療データを特定することが可能となる。

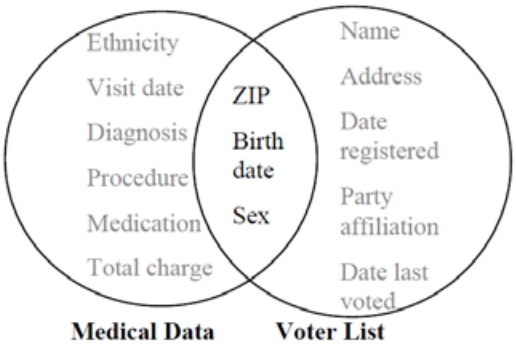


Figure 1 Linking to re-identify data

図 5.2-1

L. Sweeney, “Guaranteeing anonymity when sharing medical data，the Datafly system”

こういった組み合わせによる同定可能を防ぐための技術が k-匿名化(k-ANONYMITY)であり、公開情報から非公開情報の推論を制御するためのプライバシー保護手法の 1 つである。

k-匿名化は上述のようなデータテーブルからレコードが同定されることを防ぐために、同じ保護属性（上記の例では削除した氏名および住所にあたる情報が相当）の組み合わせをもつレコードが、少なくとも k 個存在すること（k-匿名性）を保証するために、レコードの削除・修正方法を提供する技術である。例えば、図 5.2-2 は k-匿名性を保持したテーブルの例である[2]。図 5.2-2 ではそれぞれ t3,t5,t7 の生年, t4,t6 の性別データの一部あるいは全体を削除し、（一般化された）テーブル RT を作成している。このテーブル RT はいずれのデータもすべての項目が一致するレコードを自分も含めて最低 2 個以上はもっており、したがってこのテーブルは 2-匿名性を満たしている。

	Race	BirthDate	Gender	ZIP
t1	Black	1964	f	02138
t2	Black	1964	f	02138
t3	Black	1967	m	02141
t4	White	1971	f	02139
t5	White	1967	m	02141
t6	White	1971	m	02139
t7	White	1965	m	02141

(a) 初期テーブル PT

	Race	BirthDate	Gender	ZIP
t1′	Black	1964	f	02138
t2′	Black	1964	f	02138
t3′	Person	196*	m	02141
t4′	White	1971	*	02139
t5′	Person	196*	m	02141
t6′	White	1971	*	02139
t7′	Person	196*	m	02141

(b) 一般化テーブル RT

図 5.2-2

k-匿名化のアルゴリズムはすでに既存手法の改良版を含めいくつか存在しているが[4]、k-匿名化アルゴリズムは処理時間や過度のデータの変更の回避・低減などの観点から改善が継続されている状況である。

【5.2 の参考資料】

[1] J.ヴィイダヤ, C.W.クリフトン, Y.M.ズー著, 嶋田茂, 清水將吾訳, プライバシー保護データマイニング, 丸善出版株式会社, 2011

[2]村本俊祐, 上土井陽子, 若林真一, k 匿名性を利用したデータ一般化によるプライバシー保護, DEWS2007, A710,2007

[3] L. Sweeney, “Guaranteeing anonymity when sharing medical data，the Datafly system”，Journal of the. American Medical Informatics Association, pp.1-5,. 1997

[4] k-匿名化手法の効率向上に関する一提案. 渡邉奈津美 ,土井洋 ,趙晋輝; 全国大会講演論文集 2013(1), 519-521, 2013.

6.まとめ

JIRA 会員が関係する医療情報の利活用に関しての現状と技術的対応について解説を行った。本書の内容については、今後とも充実させていく方針である。

匿名化処理についての制度的な基準が示された。したがって、匿名化処理についての正しい知識が重要である。

なお、利活用、匿名化処理に関しては、最新の文献などを参照願いたい。

解　　説

１．制定の目的と趣旨

医療の進歩のためには医療情報の利活用は不可欠である。他方、患者のプライバシーを守ることは、医師に課せられた守秘義務に代表されるように、医療情報管理の必須要件である。

これら利活用と安全管理を両立させる対策として情報の「匿名化」がある。平成 29 年 5 月 30 日全面施行された改正個人情報保護法において「匿名加工情報」が規定され、医療情報のみならずパーソナルデータを含むビッグデータの利活用の推進の上で、「匿名化」の重要性が高まっている。

本書は、JIRA 会員企業に対し、医療情報の利活用における匿名化についての社会的な要求と技術的な内容について解説することを目的としている。

２．制定の経緯

医用画像システム部会の新画像医療ＩＴ産業推進 WG の SWG3 にて本文書を作成した。

３．原案作成及び審査

３．１　原案作成：医用画像システム部会　新画像医療ＩＴ産業推進 WG　SWG3

SWG リーダ：	西田　慎一郎	(株)島津製作所
SWG メンバ：	吉澤　哲也	キヤノンメディカルシステムズ(株)
	唐沢　治男	コニカミノルタ(株)
	野津　勤	(株)システム計画研究所
	綾井　環	日本メジフィジックス(株)
	梶山　孝治	(株)日立製作所
	村田　公生	富士フイルム(株)
	大沢　哲	富士フイルム(株)
	上田　智	富士フイルム(株)
オブザーバー	舟橋　毅	JIRA 産業戦略室
事務局	鈴木　真人	JIRA 事務局

３．２ 規格審査：企画･審査委員会

委員長	藤田 直也	キヤノンメディカルシステムズ（株）
副委員長	板谷 英彦	株式会社 日立製作所
	早乙女 滋	富士フイルム（株）
	杉田 浩久	富士フイルム（株）
	飯島 直人	（株）島津製作所
	宮谷 宏	コニカミノルタ（株）
	小田 和幸	（一社）日本画像医療システム工業会

（一社）日本画像医療システム工業会が発行している規格類は、工業所有権（特許、実用新案など）に関する抵触の有無に関係なく制定されています。
（一社）日本画像医療システム工業会は、この規格の内容に関する工業所有権に対して、一切の責任を負いません。

ＪＥＳＲＡ ＴＲ－００４５－2018
２０１８年１１月発行

発行　（一社）日本画像医療システム工業会
〒 112-0004　東京都文京区後楽 2-2-23
住友不動産飯田橋ビル 2 号館 6 階
TEL　03-3816-3450
FAX　03-3818-8920