医療等分野における情報の保護と利活用に関する調査研究事業

報告書

2021年3月31日

目次

略語一覧

略語	スペル	説明	対象国
BA	Business Associate	Covered Entitiesの業務をサポートする事業者の総称	米国
CBS	Centraal Bureau voor de Statistiek	中央統計局	オランダ
CE	Covered Entities	医療提供者、保険者等医療関連サービス事業者の総称	米国
CMS	Centers for Medicare ＆ Medicaid Services	メディケア・メディケイドサービスセンター	米国
CPRD	Clinical Practice Research Datalink	医薬品・医療製品規制庁管理の医療データベース	英国
DPA	The Data Protection Act	個人情報保護法	英国
DPO	Data Protection Officer	データ保護オフィサー（データ保護に関する責任者）	共通
EHR	Electronic Health Record	電子健康記録	共通
ENHIS	Estonian National Health Information System	中央健康情報システム	エストニア
HHS	United States Department of Health and Human Services	アメリカ合衆国保健福祉省	米国
HIE	Health Information Exchange	医療情報交換システム	共通
HIPAA	Health Insurance Portability and Accountability Act	医療保険の相互運用性と説明責任に関する法律	米国
HITECH	Health Information Technology for Economic and Clinical Health Act	経済的及び臨床的健全性のための医療情報技術に関する法律	米国
HSCN	Health and Social Care Network	英国独自の医療情報交換システム	英国
HWISC	Health and Welfare Information Systems Centre	健康福祉情報システムセンター	エストニア
ICO	Information Commissioner Office	個人情報保護監督機関	英国
IHiS	Integrated Health Information Systems	公的医療分野のIT化を推進する政府系団体	シンガポール
IRB	Institutional Review Board	倫理審査委員会	共通
LSP	Landelijk Schakelpunt	オランダ独自の医療情報交換システム（ナショナルスイッチポイント）	オランダ
MHRA	Medicines and Healthcare Products Regulatory Agency	医薬品・医療製品規制庁	英国
MOHH	Ministry of Health holdings	公的医療機関の経営サポートを行う保健省直轄組織	シンガポール
MSA	Ministry of Social Affairs	社会省	エストニア
NEHR	National Electronic Health Record	中央電子健康記録システム	シンガポール
NHS	National Health Service	国民保険サービスおよびそれを運営する組織	英国
Nictiz	National ICT Institute in de Zorg	国立医療情報学研究所	オランダ
NIHR	National Institute for Health Research	臨床研究補助金助成機関	英国
OCR	Office of Civil Rights	人権保護局	米国
ONC	Office of the National Coordinator for Health IT	保健福祉省国家医療IT調整室	米国
PDPA	Personal Data Protection Act	個人情報保護法	エストニア、シンガポール
PHI	Protected Health Information	保護対象医療情報	米国
PHR	Personal Health Record	個人健康記録	共通
VWZ	Ministry of Health, Welfare and Sport	保健・福祉・スポーツ省	オランダ
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie	ヘルスケアコミュニケーションのためのプロバイダコミュニケーション協会	オランダ

用語一覧、報告書の記載

用語一覧

本資料では、次の用語を下表の定義にて使用する

用語	定義
（医療情報の）一次利用	患者本人の医療的利益に資する目的での利用
（医療情報の）二次利用	その他の目的での利用
オプトイン	事前の通知・公表を行ったうえで、本人から同意を取得する方式
オプトアウト	事前の通知・公表を行ったうえで、本人から異議が無ければ同意があったものとみなす方式
データ主体	当該個人情報が帰属する本人（患者）のことを示す
医療DB	医療データベース

報告書の記載

- 本報告書に記載されている情報は、調査時点のものであり、公開情報等を基礎としております。これら入手した情報自体の妥当性・正確性については、責任を負いません
- 本報告書のヒアリング調査に記載されている内容は、ヒアリング対象者及びヒアリング対象機関からの回答を基礎としております
- 本報告書における分析手法は、多様なものがありうる中でのひとつを採用したに過ぎず、その達成可能性に関して、いかなる保証を与えるものではありません
- 本報告書が本来の目的以外に利用されたり、第三者がこれに依拠したりしたとしてもその責任を負いません

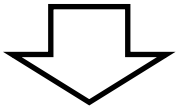
1. 日本の制度の概要

1.1 個人情報保護法

2005年に全面施行となった個人情報保護法は、その後に社会情勢の変化を受けて2度の改正が行われた

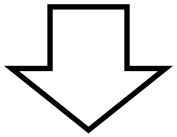
日本における個人情報保護のための法整備の概要

1980年	「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD 理事会勧告」が採択
1988年	「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が公布
2000年	「個人情報保護基本法制に関する大綱」が個人情報保護法制化専門委員会より公表
	「個人情報保護に関する基本法制の整備について」が情報通信技術（ＩＴ）戦略本部にて決定
2003年	**「個人情報の保護に関する法律」（個人情報保護法）が公布**
2005年	**「個人情報の保護に関する法律」が全面施行**



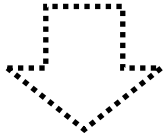
法施行から10年が経過
情報通信技術の発展により、制定当時には想定されなかったパーソナルデータの利活用を可能に

2015年	**「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」（平成27年改正個人情報保護法）が公布**
2017年	**「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」が全面施行**



平成27年改正法には、３年ごとの見直し規定が盛り込まれた
国際的動向、情報通信技術の進展、新産業の創出・発展の状況等を勘案

2020年	**「個人情報の保護に関する法律等の一部を改正する法律」（令和2年改正個人情報保護法）が公布**

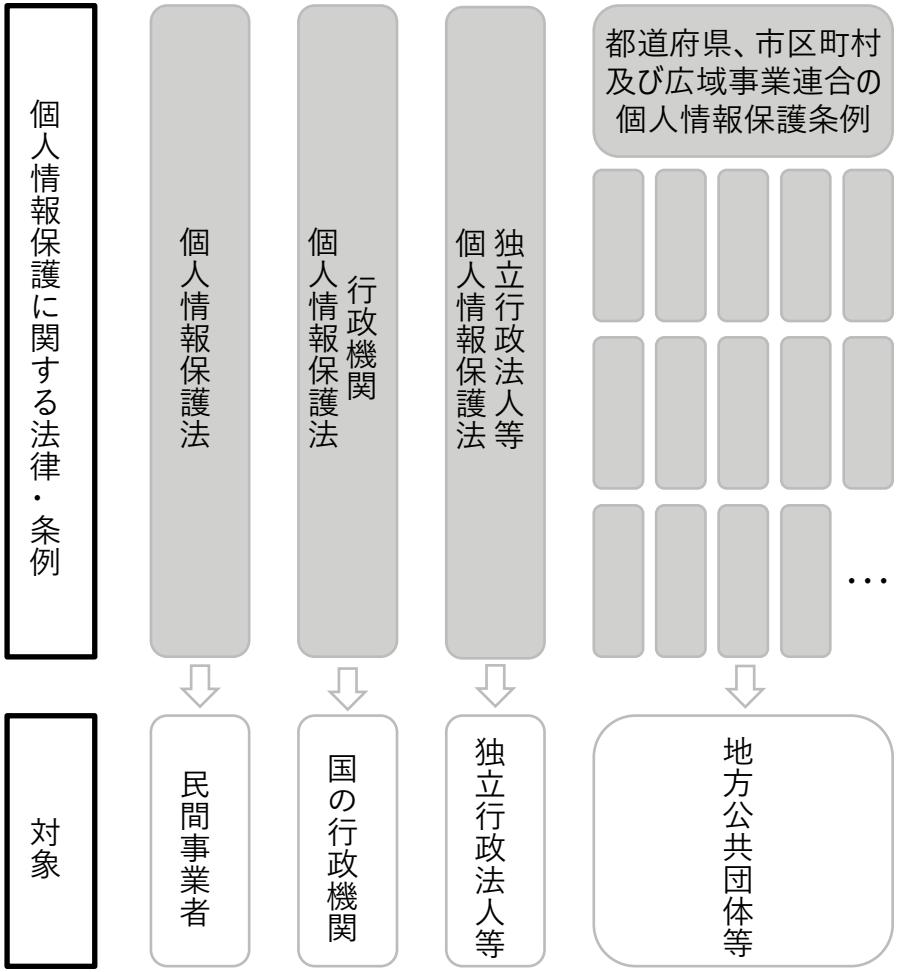


個人情報保護制度の見直しを含む「デジタル社会の形成を図るための関係法律の整備に関する法律案」を令和3年通常国会に提出

出所：https://www.soumu.go.jp/main_content/000720822.pdf、https://www.ppc.go.jp/files/pdf/personal_development.pdf

国内には個人情報保護に関する法律及び条例が多数存在するため、個人情報の利活用に支障が生じることがあり、「2000個問題」と呼ばれている

2000個問題の概要



- 我が国の個人情報保護に関する法律は、民間事業者を対象とした「個人情報保護法」、国の行政機関を対象とした「行政機関個人情報保護法」、独立行政法人等を対象とした「独立行政法人等個人情報保護法」の3法に分かれている。また、地方公共団体等における個人情報の取扱いについては、一部の例外を除き、各地方公共団体が制定した個人情報保護条例により規律されている

- これら法律および条例が制定された理由として、公的部門と民間部門における規律の性格の違いや、我が国の個人情報保護制度の確立に果たしてきた地方公共団体の先導的な役割（地方公共団体等における個人情報の取扱いについては、国の法制化に先立ち、多くの団体において条例が制定され、実務が積み重ねられてきた）がある

- 近年、情報化の進展や個人情報の有用性の高まりを背景として、官民や地域の枠を超えたデータ利活用が活発化しており、現行法制の縦割りに起因する規制の不均衡や不整合（法の所管が分かれていることに起因する解釈上の不均衡や不整合を含む）がデータ利活用の支障となる事例が各所で顕在化しつつある。また医療分野・学術分野では、実質的に同等の立場で個人情報を取得・保有している法人であっても、当該法人が公的部門に属するか（独立行政法人、国立大学法人等）、民間部門に属するか（私立大学、民間病院、民間研究機関等）によって、適用される法律上の規律が大きく異なっており、これが、公的部門と民間部門との垣根を越えた連携医療や共同研究の実施を躊躇させる一因となっているとの指摘もある

（以上、「個人情報保護制度の見直しに関する最終報告案」より）

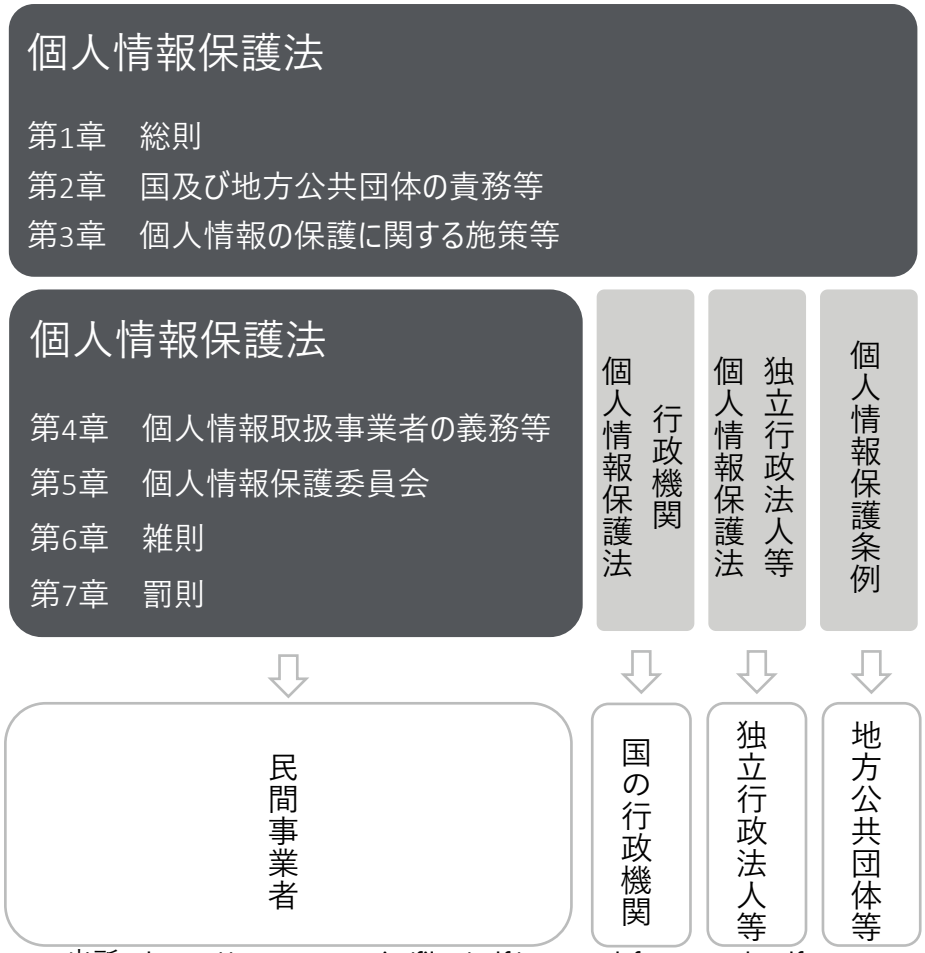
- 個人情報保護に関する法律及び条例の数を合わせると、約2,000個に及ぶ。個人情報保護に関する法律及び条例が多数存在するため、定義や解釈の違いが生じる結果、個人情報の利活用に支障が生じるという問題は、「2000個問題」と呼ばれている

出所：「個人情報保護制度の見直しに関する最終報告案」(令和2年12月 個人情報保護制度の見直しに関する検討会)

個人情報保護法は、基本法部分と一般法部分で構成されている

個人情報保護法の構成

※本ページ以降のスライドでは、日本の個人情報保護制度の中心をなす個人情報保護法に関して記載する



- 個人情報保護法は、第1章～第3章の基本法部分と、第4章～第7章の一般法部分にて構成される
- 基本法部分では、個人情報保護法の目的や用語の定義に加えて、国や地方公共団体の責務や施策方針が記載されている
- 一般法部分では、個人情報を取り扱う民間事業者の義務や罰則に加えて、個人情報の適正な取扱いの確保を目的とする個人情報保護委員会に関する記載が含まれる
- 民間事業者は、個人情報保護法の基本法部分と一般法部分に従い、個人情報の取扱いに関する義務等に従うこととなる
- 行政機関、独立行政法人等および地方公共団体等は、個人情報保護法の基本法部分の規定に従うと共に、個別の法律および条例によって定められた個人情報に関する規定に従うこととなる

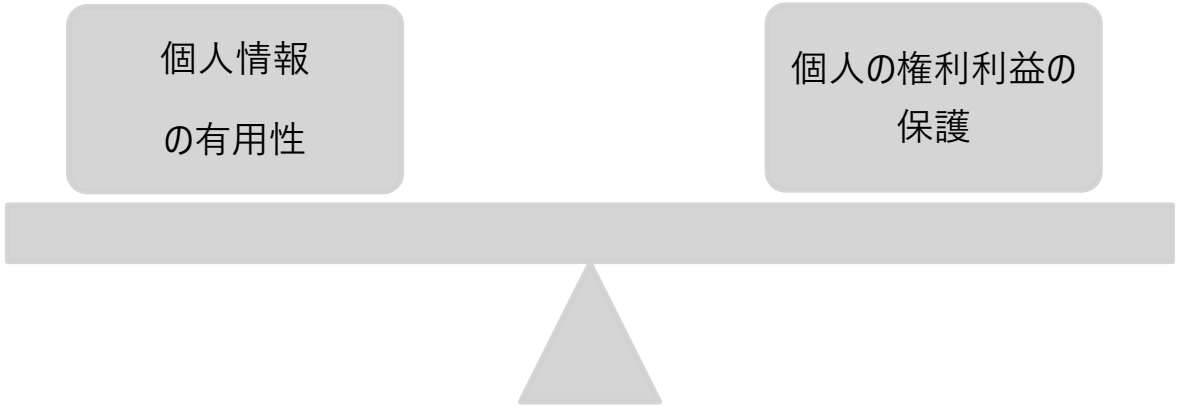
出所：https://www.ppc.go.jp/files/pdf/personal_framework.pdf

個人情報保護法は、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的としている

個人情報保護法の目的

（目的）
第1条

この法律は、**高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み**、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、**個人情報を取り扱う事業者の遵守すべき義務等を定める**ことにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであること**その他の個人情報の有用性に配慮**しつつ、**個人の権利利益を保護することを目的**とする



 出所：個人情報の保護に関する法律

生存する個人に関する情報のうち、特定の個人を識別できるもの又は個人識別符号が含まれるものが、個人情報と定義される

用語の定義（1/3）

（定義）
第2条

個人情報 （第1項）	**生存する個人に関する情報**であって、次の各号のいずれかに該当するものをいう 一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ）で作られる記録をいう。第十八条第二項及び第二十八条第一項において同じ）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く）をいう。以下同じ）により**特定の個人を識別することができるもの**（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む） 二　**個人識別符号が含まれるもの**
個人識別符号 （第2項）	次の各号のいずれかに該当する**文字、番号、記号その他の符号のうち、政令で定めるもの**をいう 一　特定の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** 二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、**特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの**

　出所：個人情報の保護に関する法律

病歴など医療に関する個人情報は、その取扱いに特に配慮を要するものとして、要配慮個人情報と定義される

用語の定義（2/3）

（定義）
第2条

要配慮個人情報 （第3項）	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**として政令で定める記述等が含まれる**個人情報**をいう
個人情報データベース等 （第4項）	個人情報を含む情報の集合物であって、次に掲げるものをいう 一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの 二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
個人情報取扱事業者 （第5項）	個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く 一　国の機関 二　地方公共団体 三　独立行政法人等 四　地方独立行政法人
個人データ （第6項）	個人情報データベース等を構成する個人情報をいう
保有個人データ （第7項）	個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう
本人 （第8項）	個人情報によって識別される特定の個人をいう

　出所：個人情報の保護に関する法律

個人情報を加工して得られるものとして、仮名加工情報と匿名加工情報が定義されている

用語の定義（3/3）

（定義）
第2条

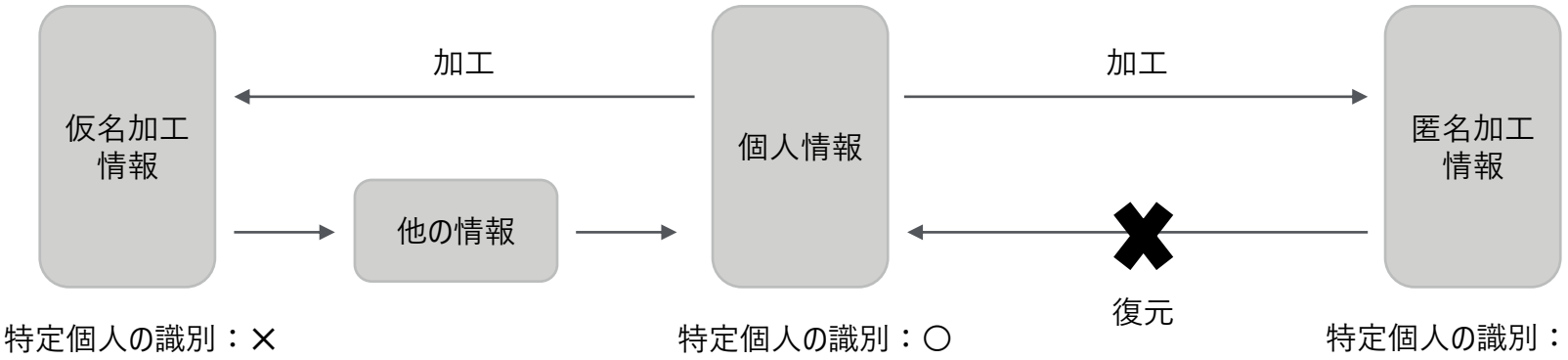
仮名加工情報 * （第9項）	次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて**他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報**をいう 一　第一項第一号に該当する個人情報　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む） 二　第一項第二号に該当する個人情報　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）
仮名加工情報取扱事業者 （第10項）	仮名加工情報を含む情報の集合物であって、特定の仮名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の仮名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるものを事業の用に供している者をいう。ただし、第五項各号に掲げる者を除く
匿名加工情報 （第11項）	次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて**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 一　第一項第一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（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を含む） 二　第一項第二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（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）
匿名加工情報取扱事業者 （第12項）	匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（第三十六条第一項において「匿名加工情報データベース等」という）を事業の用に供している者をいう。ただし、第五項各号に掲げる者を除く

* 仮名加工情報は、個人情報保護法令和2年改正にて新設された

出所：個人情報の保護に関する法律

仮名加工情報は他の情報と照合する事で特定の個人を識別する事ができるが、匿名加工情報は特定の個人を識別することができない

仮名加工情報と匿名加工情報の違い



単独では特定の個人を識別する事は出来ないが、他の情報と照合する事で特定の個人を識別することができる

単独では特定の個人を識別する事は出来ず、個人情報に復元することができない

個人情報を取り扱うに当たっては、利用目的の特定が求められる。利用目的の範囲を超えて取り扱う場合は、別途本人同意が必要となる

個人情報の利用目的に関する規定

（利用目的の特定）第15条

1　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的(以下「利用目的」という)をできる限り特定しなければならない

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない

（利用目的による制限）第16条

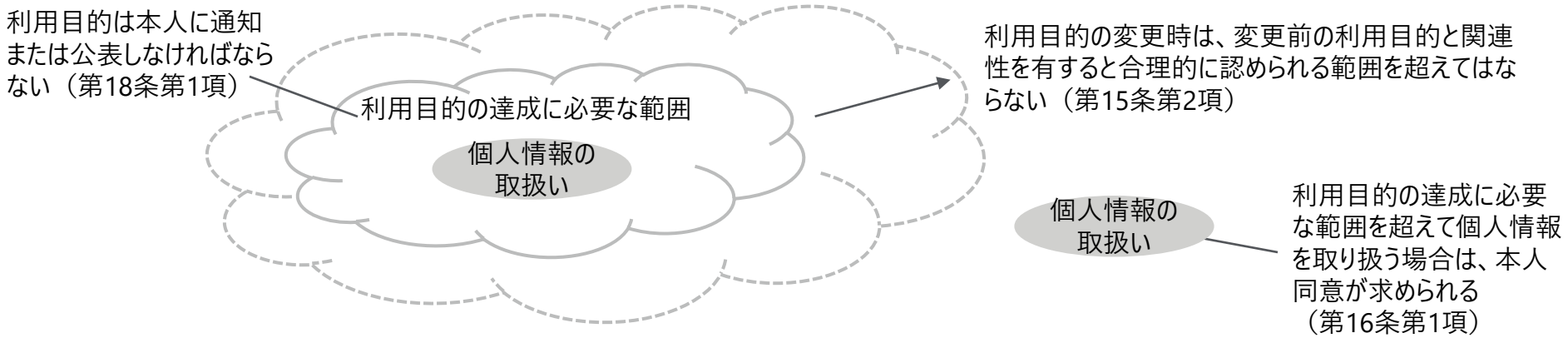
1　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない

（取得に際しての利用目的の通知等）第18条

1　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない

(中略)

3　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない



　出所：個人情報の保護に関する法律

要配慮個人情報の取得時には、本人の同意が必要である

個人情報の取得および第三者提供（1/2）

（適正な取得）第17条

1　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない

2　**個人情報取扱事業者は、**次に掲げる場合を除くほか、**あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない**

一　法令に基づく場合

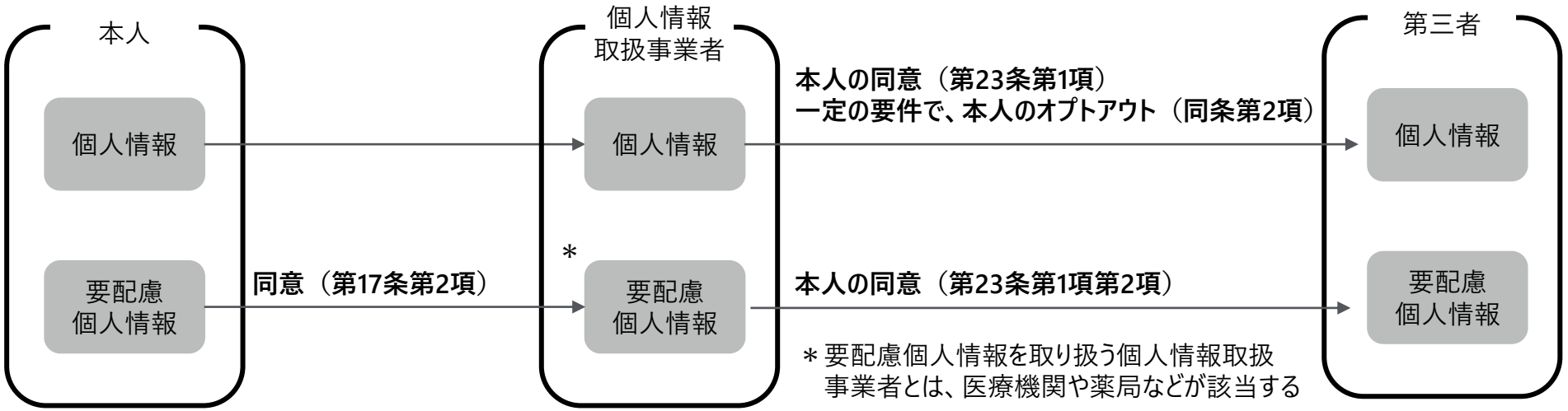
二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

五　当該要配慮個人情報が、本人、国の機関、地方公共団体、第七十六条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合

六　その他前各号に掲げる場合に準ずるものとして政令で定める場合



　出所：個人情報の保護に関する法律

個人情報は、第三者提供時にオプトアウトが認められているが、要配慮個人情報は、取得時と第三者提供時に同意が必要である

個人情報の取得および第三者提供（2/2）

（第三者提供の制限）第23条

1　個人情報取扱事業者は、次に掲げる場合を除くほか、**あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない**

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

2　**個人情報取扱事業者は、**第三者に提供される個人データについて、**本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。ただし、第三者に提供される個人データが要配慮個人情報又は第十七条第一項の規定に違反して取得されたもの若しくは他の個人情報取扱事業者からこの項本文の規定により提供されたもの（その全部又は一部を複製し、又は加工したものを含む）である場合は、この限りでない**

一　第三者への提供を行う個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人。以下この条、第二十六条第一項第一号及び第二十七条第一項第一号において同じ）の氏名

二　第三者への提供を利用目的とすること

三　第三者に提供される個人データの項目

四　第三者に提供される個人データの取得の方法

五　第三者への提供の方法

六　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること

七　本人の求めを受け付ける方法

八　その他個人の権利利益を保護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事項

　出所：個人情報の保護に関する法律

【参考】治療目的で第三者提供の同意を取る場合には、黙示の同意が認められていることから、この手法を用いることが一般的である

治療目的での同意の種類

	同意	黙示の同意
取得場面	治療目的で同意する場合	治療目的で第三者提供の同意を取得する場合
関連法等	個人情報保護法	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
規制の目的	個人の権利利益を保護することを目的とする	個人情報保護法の医療・介護関係事業者が行う個人情報の適正な取扱いの確保に関する活動を支援するための具体的な留意点・事例等を示す
規制対象	すべての事業者	医療・介護関係事業者
対象者から取得するもの	明示的な同意 (利用の目的をできる限り特定しなければならないと規定)	黙示の同意 患者の傷病の回復等を含めた患者への医療の提供に必要であり、かつ、個人情報の利用目的として院内掲示等により明示する
特徴	形式要件はなく、文章でも口頭でも可	院内掲示等により利用目的を明示するのみで可

同意が困難な場合は、個人情報保護法第23条*に定めがある場合に限り、同意不要で利用可能

*個人情報保護法第23条：法令に基づく場合、生命の保護や公衆衛生の向上で本人同意が困難な場合などが定められている

18　出所：個人情報の保護に関する法律、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

匿名加工情報の作成方法は、個人情報保護委員会規則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

匿名加工情報の作成（1/3）

（匿名加工情報の作成等）第36条

1　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**

個人情報の保護に関する法律施行規則（個人情報保護委員会規則第３号）
（匿名加工情報の作成の方法に関する基準）第19条

法第36条第１項の個人情報保護委員会規則で定める基準は、次のとおりとする

一 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）

二 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）

三 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）

四 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）

五 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

　出所：個人情報の保護に関する法律、個人情報の保護に関する法律施行規則

匿名加工情報の作成方法は、個人情報の保護に関する法律についてのガイドラインでも加工手法が説明されている

匿名加工情報の作成（2/3）

個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）でも、匿名加工情報の加工方法が説明されている

個人情報の保護に関する法律についてのガイドライン
・事業者が個人情報の適正な取扱いの確保に関して行う活動を支援すること、及び当該支援により事業者が講ずる措置が適切かつ有効に実施されることを目的として、具体的な指針として個人情報保護委員会が定めたもの **・記述した具体例は、**事業者の理解を助けることを目的として典型的なものを示したものであり、**全ての事案を網羅したものでなく、記述した内容に限定する趣旨で記述したものでもない。**また、記述した具体例においても、個別ケースによっては別途考慮すべき要素もあり得るので注意を要する

個人情報保護委員会規則　第19条	ガイドラインでの説明
（第1号）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	・単体で特定の個人を識別することができる情報（氏名など）は、削除する ・記述等が合わさることによって特定の個人を識別することができる情報（住所、生年月日）は、削除または他の記述に置き換える
（第2号）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	・個人識別符号は、削除または他の記述等に置き換える。
（第3号）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符号を削除すること	・安全管理の観点から個人情報を分散管理する際に、情報を相互に連結するための符号としてIDを付していることがあるが、このようなIDは元の個人情報の復元につながり得ることから、加工対象となる個人情報から削除または他の符号への置き換える
（第4号）特異な記述等を削除すること	・特異であるがために特定の個人を識別できる記述等に至り得るもの（116歳という年齢情報、希少疾患の病歴など）は、削除または他の記述に置き換える
（第5号）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	・第1号から第4号までの加工を施した情報であっても、特定の個人を識別することが可能である状態あるいは元の個人情報を復元できる状態の場合がある。必要に応じて、別表1(次頁の＊1参照)の方法により、適切な追加措置を講じなければならない ・どの情報をどの程度加工する必要があるかは、加工対象となる個人情報データベース等の性質も勘案して個別具体的に判断する必要がある

　出所：個人情報の保護に関する法律施行規則、個人情報の保護に関する法律についてのガイドライン

匿名加工情報の作成方法は、個人情報の保護に関する法律についてのガイドラインでも加工手法が説明されている

匿名加工情報の作成（3/3）

＊1 （別表1）匿名加工情報の加工に係る手法例

匿名加工情報の作成に当たっての一般的な加工手法を例示したものであり、その他の手法を用いて適切に加工することを妨げるものではない

手法名	解説
項目削除／レコード削除／セル削除	加工対象となる個人情報データベース等に含まれる個人情報の記述等を削除するもの。例えば、年齢のデータを全ての個人情報から削除すること（項目削除）、特定の個人の情報を全て削除すること（レコード削除）、又は特定の個人の年齢のデータを削除すること（セル削除）
一般化	加工対象となる情報に含まれる記述等について、上位概念若しくは数値に置き換えること又は数値を四捨五入などして丸めることとするもの。例えば、購買履歴のデータで「きゅうり」を「野菜」に置き換えること
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して、特に大きい又は小さい数値をまとめることとするもの。例えば、年齢に関するデータで、80歳以上の数値データを「80歳以上」というデータにまとめること
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後、グループの代表的な記述等に置き換えることとするもの
データ交換（スワップ）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えることとするもの
ノイズ（誤差）付加	一定の分布に従った乱数的な数値を付加することにより、他の任意の数値へと置き換えることとするもの
疑似データ生成	人工的な合成データを作成し、これを加工対象となる個人情報データベース等に含ませることとするもの

 出所：個人情報の保護に関する法律についてのガイドライン

匿名加工情報は、第三者に提供する際に、当該提供に係る情報が匿名加工情報である旨を明示しなければならない

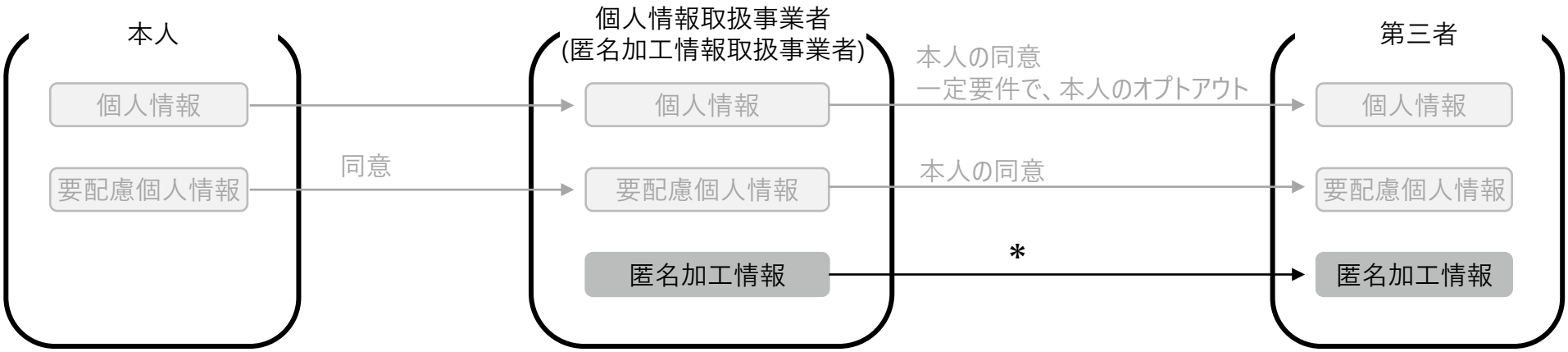
匿名加工情報の第三者提供

（匿名加工情報の作成等）第36条

4　個人情報取扱事業者は、匿名加工情報を作成して当該匿名加工情報を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない

（匿名加工情報の提供）第37条

匿名加工情報取扱事業者は、匿名加工情報（自ら個人情報を加工して作成したものを除く。以下この節において同じ）を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない



＊ 本人の同意は必要ない

　出所：個人情報の保護に関する法律

個人情報取扱事業者は、体制整備、第三者提供時の記録作成および苦情処理の義務を負う

個人情報取扱事業者が負う主な義務

体制整備	（データ内容の正確性の確保等） 第19条	・個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは個人データを遅滞なく消去する
	（安全管理措置） 第20条	・個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じる
	（従業者の監督） 第21条	・個人データの安全管理が図られるよう、従業者に対する必要かつ適切な監督を行う
	（委託先の監督） 第22条	・個人データの安全管理が図られるよう、委託先に対する必要かつ適切な監督を行う
	（漏えい等の報告等） 第22条の2	・個人データの安全の確保に係る事態であって個人情報保護委員会規則で定める事態が生じたときは、事態が生じた旨を個人情報保護委員会へ報告するとともに、本人に通知しなければならない
第三者との個人データ授受における記録作成	（第三者提供に係る記録の作成等） 第25条	・個人データの第三者提供する場合は、提供年月日や提供先名称など個人情報保護委員会規則で定める事項の記録を作成及び保存しなければならない
	（第三者提供を受ける際の確認等） 第26条	・個人データを第三者から受け取る場合は、提供元の名称や個人データ取得の経緯などを確認するとともに、個人情報保護委員会規則で定める事項の記録を作成および保存しなければならない
苦情処理	（個人情報取扱事業者による苦情の処理） 第35条	・個人情報の取扱いに関する苦情を適切かつ迅速に処理しなければならない

出所：個人情報の保護に関する法律

個人情報を学術研究目的に用いる場合は、個人情報保護法における第4章(個人情報取扱事業者の義務等)の規定は適用されない

学術研究目的での利用

（適用除外）第76条

個人情報取扱事業者等のうち次の各号に掲げる者については、その個人情報等を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、第四章の規定は、適用しない

一　放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む）　報道の用に供する目的

二　著述を業として行う者　著述の用に供する目的

三　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的

四　宗教団体　宗教活動（これに付随する活動を含む）の用に供する目的

五　政治団体　政治活動（これに付随する活動を含む）の用に供する目的

主体要件
放送機関、新聞社、通信社その他の報道機関
著述を業として行う者
大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者
宗教団体
政治団体

＋

目的要件
報道の用に供する目的
著述の用に供する目的
学術研究の用に供する目的
宗教活動の用に供する目的
政治活動の用に供する目的

＝

個人情報保護法の第4章「個人情報取扱事業者の義務等」の規定は、適用しない *

* 適用除外となる主な規定
- ・個人情報の第三者提供時における、同意又はオプトアウト（第23条第1項第2項）
- ・要配慮個人情報の取得時における、同意（第17条第2項）
- ・要配慮個人情報の第三者提供時における、同意（第23条第2項）
- ・第三者との個人データ授受に際した記録の作成及び保存（第25条、第26条）

　出所：個人情報の保護に関する法律

個人情報保護委員会は、個人情報取扱事業者による個人情報等の取扱いに関する監督機関である

個人情報保護委員会の概要

構成、運営

- 2016年1月に設置。内閣府の外局であり、委員長1名および委員8名（常勤4名、非常勤4名）で構成される（2021年3月時点）。事務局職員数は、139名である（2020年度）
- 毎月2～3回の委員会が開催され、議事録等は個人情報保護委員会ホームページで開示される

主な業務（個人情報保護委員会ホームページより抜粋）

個人情報の保護に関する基本方針の策定・推進	個人情報保護法に基づく「個人情報の保護に関する基本方針」の策定等により、官民の個人情報保護の取組みを推進
個人情報等の取扱いに関する監督	**個人情報取扱事業者等に対して指導・助言や報告徴収・立入検査を行い、法令違反があった場合には勧告・命令等を実施**
認定個人情報保護団体に関する事務	認定個人情報保護団体の認定、報告徴収や命令等を実施
特定個人情報の取扱いに関する監視・監督	行政機関など特定個人情報の取扱者に対して、必要な指導や助言等を行い、法令違反があった場合には勧告・命令等を実施
特定個人情報保護評価に関する事務	特定個人情報保護評価の指針作成や、行政機関等が作成した特定個人情報保護評価書の承認等を実施
苦情あっせん等に関する事務	個人情報保護法に関する質問への回答、苦情の申出について必要な助言・あっせんを実施
国際協力	個人情報の保護に関する国際会議へ参加するほか、海外の関係機関との協力関係の構築に努める
広報・啓発	個人情報の保護及び適正かつ効果的な活用について、パンフレット等を活用した広報・啓発活動を実施
その他	上記の事務のほか、委員会の所掌事務の処理状況を示すための国会報告や必要な調査・研究等を実施

個人情報保護法に規定された主な役割

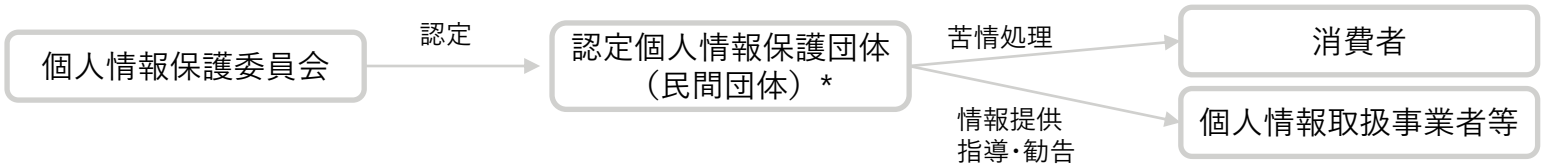
- 個人情報取扱事業者より情報漏洩時の報告を受ける（第22条の2）
- 個人情報の第三者提供時にオプトアウトを採用する場合の届け出を受ける（第23条第2項）
- 個人情報取扱事業者等への助言指導および立入検査を行う（第40条、第41条）
- 個人情報取扱事業者等への違反行為の中止および必要な是正措置の勧告・命令、命令違反時の公表（第42条）
- 認定個人情報保護団体の認定（第47条）
- 個人情報保護委員会規則の制定（第74条）

出所：https://www.ppc.go.jp/aboutus/commission/、https://www.ppc.go.jp/files/pdf/saiyouannai2020.pdf

認定個人情報保護団体は、個人情報保護委員会によって認定され、苦情の処理や個人情報取扱事業者等への情報提供や指導・勧告を行っている

認定個人情報保護団体の認定および業務に関する規定

（認定） 第47条	・認定個人情報保護団体は、個人情報保護委員会によって認定され、以下の業務を行う ①個人情報取扱事業者等による個人情報等の取扱いに関する苦情の処理 ②個人情報等の適切な取扱いの確保に寄与する情報を個人情報取扱事業者等へ提供 ③そのほか個人情報取扱事業者等による個人情報等の適正な取扱いの確保に関する必要な業務
（対象事業者） 第51条	・第47条の業務を行う場合は、対象とする個人情報取扱事業者等の同意を取得しなければならない
（苦情の処理） 第52条	・本人その他の関係者から個人情報等の取扱いに関する苦情の申し出があった場合は、相談および調査を実施して、苦情を個人情報取扱事業者等に通知する事で、その解決に努める
（個人情報保護指針） 第53条	・個人情報等の適正な取扱いの確保のために、個人情報に係る利用目的の特定など安全管理のための措置その他の事項に関し、この法律の規定の趣旨に沿った指針（個人情報保護指針）の作成に努める ・個人情報保護指針が個人情報保護委員会より公表されたときは、対象とする個人情報取扱事業者等に対し、個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとる
（目的外利用の禁止） 第54条	・第47条の業務を行うに際して知り得た情報を、同業務の用に供する目的以外に利用してはならない
（報告の徴収） 第56条	・第47条の業務に関する報告を個人情報保護委員会の求めに応じて行う
（命令） 第57条	・第47条の業務を行う方法の改善、個人情報保護指針の変更その他の必要な措置をとるべき旨を個人情報保護委員会から命令された場合は、その命令に従う
（認定の取消し） 第58条	・認定個人情報保護団体が同条各号のいずれかに該当する場合、個人情報保護委員会はその認定を取り消すことができる



図は、個人情報保護委員会ホームページ「認定個人情報保護団体＞制度の概要」をもとに作成した。

*主に個人情報取扱事業者の事業分野ごとに設立されており、2021年2月時点で41団体（個人情報保護委員会ホームページ「認定個人情報保護団体一覧」より）

出所：個人情報の保護に関する法律

個人情報保護法は、一部罰則を除いて間接罰である。令和2年改正により、個人情報保護委員会の命令違反や虚偽報告に対する懲役刑および罰金刑が引き上げられた

個人情報保護法に規定される罰則

個人情報保護委員会のホームページより抜粋

		懲役刑	罰金刑
個人情報保護委員会からの命令への違反	行為者（第83条）	【改正前】6か月以下　→　**【改正後】1年以下**	【改正前】30万円以下　→　**【改正後】100万円以下**
	法人等（第87条）	－	【改正前】30万円以下　→　**【改正後】1億円以下**
個人情報データベース等の不正提供等	行為者（第84条）	【改正前】1年以下　→　【改正後】1年以下	【改正前】50万円以下　→　【改正後】50万円以下
	法人等（第87条）	－	【改正前】50万円以下　→　**【改正後】1億円以下**
個人情報保護委員会への虚偽報告等	行為者（第85条）	－	【改正前】30万円以下　→　**【改正後】50万円以下**
	法人等（第87条）	－	【改正前】30万円以下　→　**【改正後】50万円以下**

※**太字**は、令和2年改正で引き上げられた懲役刑または罰金刑

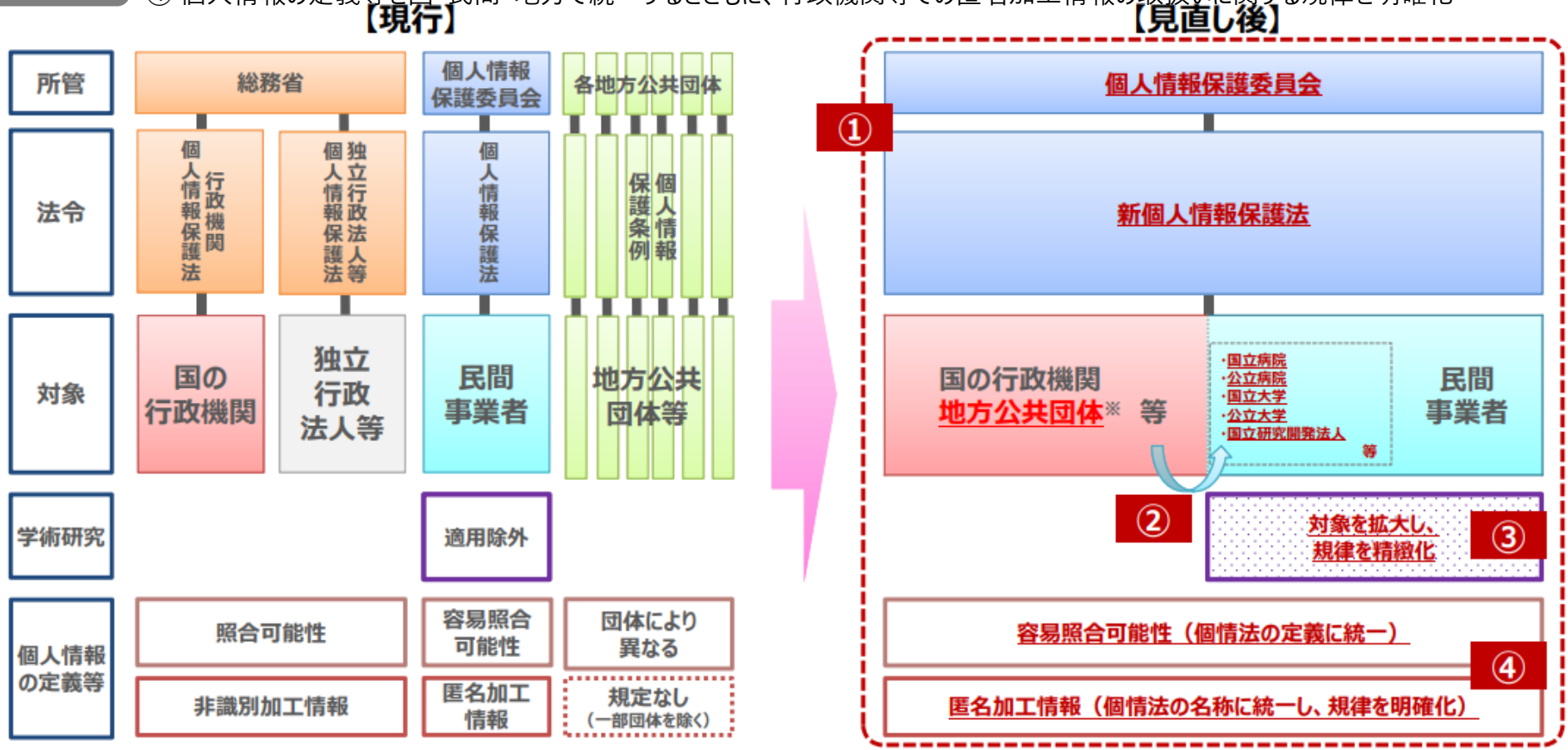
　出所：https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

いわゆる2000個問題への対応など個人情報保護制度の見直しを含む「デジタル社会の形成を図るための関係法律の整備に関する法律案」が令和3年通常国会に提出された

個人情報保護制度見直しの全体像

ポイント

① 3本の法律を1本の法律に統合するとともに、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化
② 医療分野・学術分野の規制を統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用
③ 学術研究に係る適用除外規定について、一律の適用除外ではなく、義務ごとの例外規定として精緻化
④ 個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取扱いに関する規律を明確化



 出所：「個人情報保護制度の見直しに関する最終報告(概要)」(令和2年12月 個人情報保護制度の見直しに関するタスクフォース)

1.2 次世代医療基盤法

健康・医療に関する先端的研究開発及び新産業創出を促進するため、2018年5月に次世代医療基盤法が施行された

次世代医療基盤法の全体像

次世代医療基盤法が成立する以前の課題

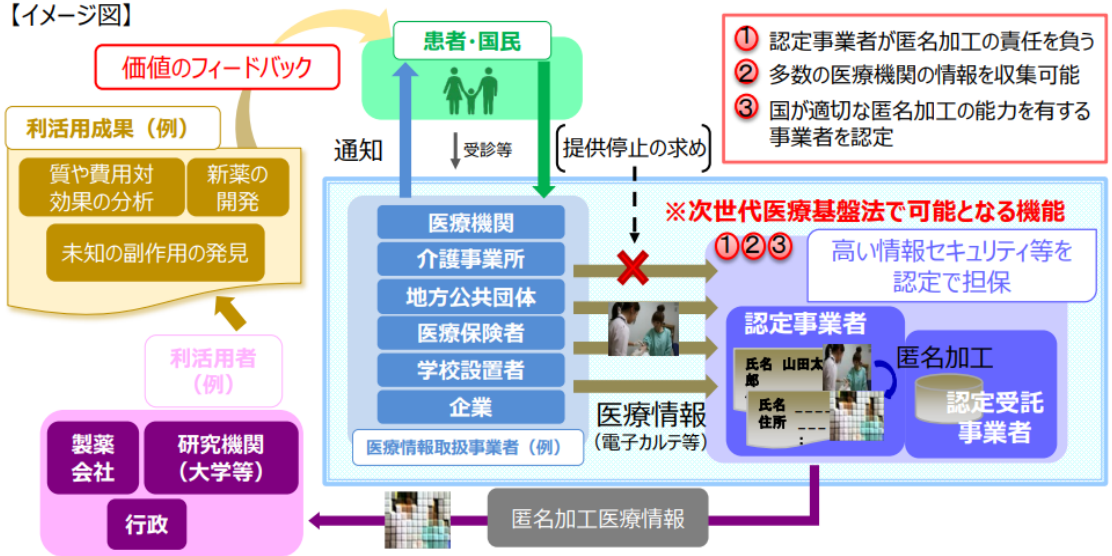
アウトカムも含む医療情報の利活用	レセプト(診療報酬明細書)は、インプット(診療行為の実施に関する情報)を含むが、アウトカム(診療行為を実施した結果に関する情報)を含まない。医療分野の研究開発に資するよう、カルテ(診療録)など、アウトカムを含む医療情報の利活用のための仕組みを整備することが求められた
医療情報の分散保有	我が国では、国民皆保険制度の下、医療情報が豊富に存在しているものの、医療情報が分散して保有されている。医療分野の研究開発に資するよう、医療情報を「集めて」「つなぐ」仕組みを整備することが求められた
改正個人情報保護法の施行	2017年5月に施行された改正個人情報保護法では、下記が規定された ① 病歴を始めとする要配慮個人情報を第三者に提供するに当たっては、学術研究等を除いては、オプトイン(あらかじめ本人が同意すること)によらなければならず、オプトアウト(本人が停止を求めないこと)によることができない ② 特定の個人を識別できないように加工された匿名加工情報については、個人情報と比較して緩やかな規律で第三者に提供することができる

個人情報保護法の特則となる次世代医療基盤法が2018年5月に施行された

法律のポイント

①高い情報セキュリティを確保し、十分な匿名加工技術を有するなどの一定の基準を満たし、匿名加工医療情報を提供するに至るまでの一連の対応を適正かつ確実に行うことができる者を認定する仕組みの設定
②一定の要件を満たすオプトアウト(あらかじめ通知を受けた本人又はその遺族が停止を求めないこと)により、認定事業者に対し、医療情報を提供できる
③ 医療情報の提供に当たっては、倫理審査委員会の承認が不要
④我が国の医療分野の研究開発に資する限り、産学官といった主体の種別にかかわらず、匿名加工医療情報を利活用することが可能

【イメージ図】



出所：「「次世代医療基盤法」とは」(2020年11月 内閣官房健康・医療戦略室及び内閣府日本医療研究開発機構・医療情報基盤担当室)

次世代医療基盤法では、特定の個人の病歴その他の当該個人の心身の状態に関する情報であって、特定の個人を識別することができるものを医療情報と定義している

用語の定義

（定義）
第2条

医療情報 （第1項）	**特定の個人の病歴その他の当該個人の心身の状態に関する情報**であって、当該心身の状態を理由とする当該個人又はその子孫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政令で定める記述等であるものが含まれる個人に関する情報のうち、次の各号のいずれかに該当するものをいう 一　当該情報に含まれる氏名、生年月日その他の記述等により**特定の個人を識別することができるもの**（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む） 二　**個人識別符号が含まれるもの**
本人 （第2項）	医療情報によって識別される特定の個人をいう
匿名加工医療情報 （第3項）	次の各号に掲げる医療情報の区分に応じて当該各号に定める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**医療情報を加工して得られる個人に関する情報**であって、**当該医療情報を復元することができないようにしたもの**をいう 一　第一項第一号に該当する医療情報　当該医療情報に含まれる記述等の一部を削除すること 二　第一項第二号に該当する医療情報　当該医療情報に含まれる個人識別符号の全部を削除すること
匿名加工医療情報作成事業 （第4項）	医療分野の研究開発に資するよう、医療情報を整理し、及び加工して匿名加工医療情報を作成する事業をいう
医療情報取扱事業者 （第5項）	医療情報を含む情報の集合物であって、特定の医療情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の医療情報を容易に検索することができるように体系的に構成したものとして政令で定めるものを事業の用に供している者をいう

第8条第1項
第9条第1項

認定匿名加工医療情報作成事業者	匿名加工医療情報作成事業を行う者として、主務大臣より認定を受けた者をいう

出所：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

認定匿名加工医療情報作成事業者は、医療分野の研究開発に資するという趣旨に反することのないよう、認定事業の目的の達成に必要な範囲を超えて医療情報を取り扱ってはならない

利用目的による制限

（認定）第8条

1 匿名加工医療情報作成事業を行う者（法人に限る）は、申請により、匿名加工医療情報作成事業を適正かつ確実に行うことができるものと認められる旨の主務大臣の認定を受けることができる

（主務大臣等）第39条

1 この法律における主務大臣は、内閣総理大臣、文部科学大臣、厚生労働大臣及び経済産業大臣とする

2 この法律における主務省令は、主務大臣の発する命令とする

3 主務大臣は、主務省令を定め、又は変更しようとするときは、あらかじめ、個人情報保護委員会に協議しなければならない

（利用目的による制限）第17条

1 認定匿名加工医療情報作成事業者は、第二十五条又は第三十条第一項の規定により医療情報の提供を受けた場合は、当該医療情報が医療分野の研究開発に資するために提供されたものであるという趣旨に反することのないよう、認定事業の目的の達成に必要な範囲を超えて当該医療情報を取り扱ってはならない

2 前項の規定は、次に掲げる場合については、適用しない

一　法令に基づく場合

二　人命の救助、災害の救援その他非常の事態への対応のため緊急の必要がある場合

　出所：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

医療情報取扱事業者は、一定の要件を満たすオプトアウト（あらかじめ通知を受けた本人又はその遺族が停止を求めないこと）により、当該医療情報を認定匿名加工医療情報作成事業者への提供することができる

医療情報の認定匿名加工医療情報作成事業者への提供（1/2）

（医療情報取扱事業者による医療情報の提供）第30条

1 医療情報取扱事業者は、認定匿名加工医療情報作成事業者に提供される医療情報について、主務省令で定めるところにより**本人又はその遺族（死亡した本人の子、孫その他の政令で定める者をいう。以下同じ）からの求めがあるときは、当該本人が識別される医療情報の認定匿名加工医療情報作成事業者への提供を停止することとしている場合**であって、**次に掲げる事項について、主務省令で定めるところにより、あらかじめ、本人に通知するとともに、主務大臣に届け出たときは、当該医療情報を認定匿名加工医療情報作成事業者に提供することができる**

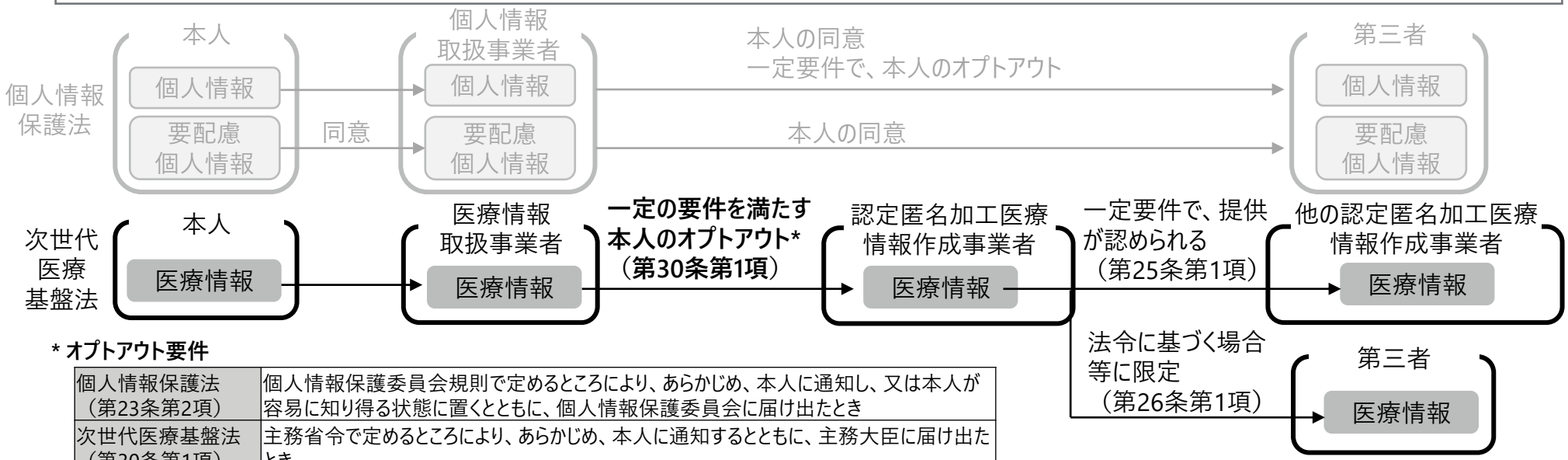
一　医療分野の研究開発に資するための匿名加工医療情報の作成の用に供するものとして、認定匿名加工医療情報作成事業者に提供すること

二　認定匿名加工医療情報作成事業者に提供される医療情報の項目

三　認定匿名加工医療情報作成事業者への提供の方法

四　本人又はその遺族からの求めに応じて当該本人が識別される医療情報の認定匿名加工医療情報作成事業者への提供を停止すること

五　本人又はその遺族からの求めを受け付ける方法



*** オプトアウト要件**

個人情報保護法（第23条第2項）	個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たとき
次世代医療基盤法（第30条第1項）	主務省令で定めるところにより、あらかじめ、本人に通知するとともに、主務大臣に届け出たとき

出所：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

医療情報の提供を受けた認定匿名加工医療情報作成事業者は、他の認定匿名加工医療情報作成事業者からの求めに応じ、医療情報を提供することができる

医療情報の認定匿名加工医療情報作成事業者への提供（2/2）

（他の認定匿名加工医療情報作成事業者に対する医療情報の提供）第25条

1 第三十条第一項の規定により医療情報の提供を受けた認定匿名加工医療情報作成事業者は、主務省令で定めるところにより、他の認定匿名加工医療情報作成事業者からの求めに応じ、匿名加工医療情報の作成のために必要な限度において、当該他の認定匿名加工医療情報作成事業者に対し、同項の規定により提供された医療情報を提供することができる

2 前項の規定により医療情報の提供を受けた認定匿名加工医療情報作成事業者は、第三十条第一項の規定により医療情報の提供を受けた認定匿名加工医療情報作成事業者とみなして、前項の規定を適用する

（第三者提供の制限）第26条

1 認定匿名加工医療情報作成事業者は、前条の規定により提供する場合及び次に掲げる場合を除くほか、同条又は第三十条第一項の規定により提供された医療情報を第三者に提供してはならない

一　法令に基づく場合

二　人命の救助、災害の救援その他非常の事態への対応のため緊急の必要がある場合

2 次に掲げる場合において、当該医療情報の提供を受ける者は、前項の規定の適用については、第三者に該当しないものとする

一　第十条第一項、第二項又は第四項から第六項までの規定による事業譲渡その他の事由による事業の承継に伴って医療情報が提供される場合

二　認定匿名加工医療情報作成事業者が第二十三条第一項の規定により医療情報の取扱いの全部又は一部を委託することに伴って当該医療情報が提供される場合

　出所：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

匿名加工医療情報の作成方法は、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施行規則に定める基準に従い、医療情報を加工しなければならない

匿名加工医療情報の作成（1/2）

（匿名加工医療情報の作成等）第18条

1 認定匿名加工医療情報作成事業者は、匿名加工医療情報を作成するときは、特定の個人を識別すること及びその作成に用いる医療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主務省令で定める基準に従い、当該医療情報を加工しなければならない

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施行規則
（匿名加工医療情報の作成の方法に関する基準）第18条

法第十八条第一項の主務省令で定める基準は、次のとおりとする

一　医療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）

二　医療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）

三　医療情報と当該医療情報に措置を講じて得られる情報とを連結する符号（現に認定匿名加工医療情報作成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医療情報と当該医療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）

四　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）

五　前各号に掲げる措置のほか、医療情報に含まれる記述等と当該医療情報を含む医療情報データベース等を構成する他の医療情報に含まれる記述等との差異その他の当該医療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

　出所：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、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施行規則

匿名加工医療情報の作成方法は、省令に加え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により加工手法が説明されている

匿名加工医療情報の作成（2/2）

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（匿名加工医療情報編）においても、匿名加工医療情報の適切な加工が説明されている

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施行規則　第18条	ガイドラインでの説明
（第1号）医療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	・単体で特定の個人を識別することができる情報（氏名など）は、削除する ・記述等が合わさることによって特定の個人を識別することができる情報（住所、生年月日）は、削除または他の記述に置き換える
（第2号）医療情報に含まれる個人識別符号の全部を削除すること	・個人識別符号は、削除または他の記述等に置き換える
（第3号）医療情報と当該医療情報に措置を講じて得られる情報とを連結する符号を削除すること	・安全管理の観点から医療情報を分散管理する際に、情報を相互に連結するための符号としてIDを付していることがあるこのようなIDは元の医療情報の復元につながり得ることから、加工対象となる医療情報から削除または他の符号へ置き換える
（第4号）特異な記述等を削除すること	・特異であるがために特定の個人を識別できる記述等に至り得るもの（116歳という年齢情報、希少疾患の病歴など）は、削除または他の記述に置き換える
（第5号）前各号に掲げる措置のほか、医療情報に含まれる記述等と当該医療情報を含む医療情報データベース等を構成する他の医療情報に含まれる記述等との差異その他の当該医療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	・第1号から第4号までの加工を施した情報であっても、特定の個人を識別することが可能である状態あるいは元の医療情報を復元できる状態の場合がある。必要に応じて、別表1(*)の手法を参照するなどにより、適切な追加措置を講じなければならない ・どの情報をどの程度加工する必要があるかは、加工対象となる医療情報データベース等の性質も勘案して個別具体的に判断する必要がある

* 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（匿名加工医療情報編）の別表1「匿名加工情報の加工に係る手法例」は、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）の別表1より抜粋となっている

 出所：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施行規則、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

認定匿名加工医療情報作成事業者は、体制整備、医療情報を受領した際の記録作成および苦情処理等の義務を負う

認定匿名加工医療情報作成事業者が負う主な義務

体制整備	（消去） 第19条	・医療情報等または匿名加工医療情報を利用する必要がなくなったときは、遅滞なく当該情報等を消去する
	（安全管理措置） 第20条	・医療情報等または匿名加工医療情報の漏えい、滅失又は毀損の防止その他の当該情報等の安全管理のために必要かつ適切な措置を講じる
	（従業者の監督） 第21条	・医療情報等または匿名加工医療情報の安全管理が図られるよう、従業者に対する必要かつ適切な監督を行う
	（委託先の監督） 第24条	・医療情報等または匿名加工医療情報の安全管理が図られるよう、委託先に対する必要かつ適切な監督を行う
医療情報の受領時における記録の作成	（医療情報の提供を受ける際の確認） 第33条	・医療情報等を医療情報取扱事業者から受け取る場合は、提供元の名称や医療情報の取得経緯などを確認するとともに、主務省令で定める事項の記録を作成および保存しなければならない
苦情処理	（苦情の処理） 第27条	・医療情報等または匿名加工医療情報の取扱いに関する苦情を適切かつ迅速に処理しなければならない

出所：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

認定匿名加工医療情報作成事業者の監督は、主務大臣が行う。次世代医療基盤法の規定の違反に対して、罰則がある

主務大臣による監督

- 認定匿名加工医療情報作成事業者等の事務所への立入検査（第35条第1項）
- 事業の適確な実施を目的とした、認定匿名加工医療情報作成事業者等に対する指導助言（第36条）
- 次世代医療基盤法の規定に違反した認定匿名加工医療情報作成事業者等への必要な是正措置の命令（第37条）

罰則

		懲役刑	罰金刑
・正当な理由のない医療情報データベース等の提供等	個人（第44条）	2年以下	100万円以下
	法人（第49条）	–	1億円以下
・不正な手段による認定匿名加工医療情報作成事業者の認可取得 ・主務大臣からの命令への違反	個人（第46条）	1年以下	100万円以下
	法人（第49条）	–	1億円以下
・主務大臣への虚偽報告等	個人（第47条）	–	50万円以下
	法人（第49条）	–	50万円以下

(備考)令和2年改正による引上げ後の罰則

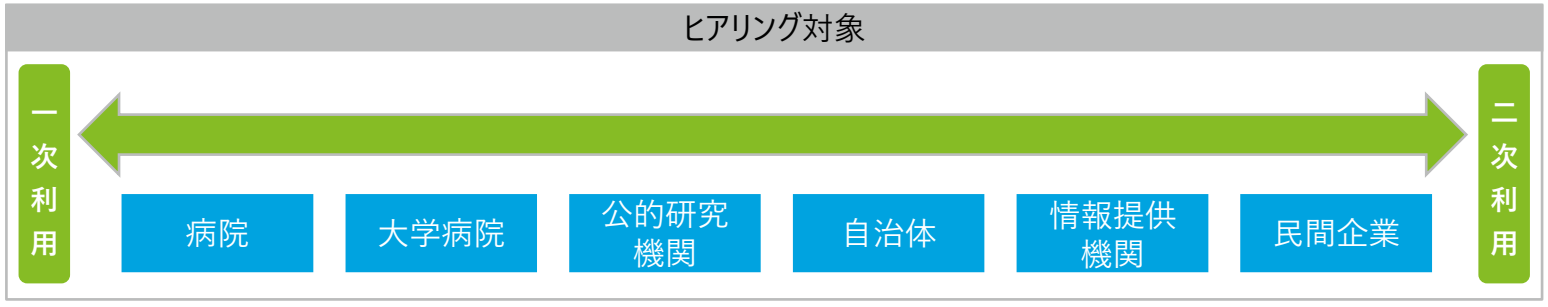
出所：医療分野の研究開発に資するための匿名加工医療情報に関する法律

2.日本の現行制度に対する課題

医療情報の保護と利活用について、文献・Web等調査に加え、医療情報を取り扱っている計33機関に対してヒアリング調査を実施した

国内調査の概要

文献・Web 等調査	■ 医療情報の保護と利活用について、我が国において一般的に課題として取り上げられている事例等の調査を実施した ■ 具体的には、国内における個人情報保護関連法の概要、2000個問題、匿名加工基準、公益性等の解釈・運用、データベース、データ標準化などの項目について調査を実施した
ヒアリング調査	■ 現行の法制度やガイドラインのもとにおいて、医療機関や自治体、研究機関による医療情報の取扱いを把握したうえで、個人情報の保護と利活用の観点から現行の法制面や運用面における課題等を整理することが、調査の目的である ■ 医療情報の利活用に関して現場の課題を把握するため、医療情報を取り扱っている計33機関にヒアリング調査を行った ■ ヒアリング調査の対象は、病院、大学病院、公的研究機関、自治体、情報提供機関、民間企業である



ヒアリング調査の結果、第三者が研究目的で医療情報の利活用を行う場合に課題があるという意見が多く聞かれた

医療情報の利活用に関する課題

医療情報の利活用の分類	医療情報の利活用に関する課題
【治療目的】	■ 利活用に関する課題は少ない ただし、以下のような課題が指摘された ➢ 同意や黙示の同意が行われた場合、患者がどこまで理解して同意したのかは不明確な点がある ➢ 法令上の問題が無い場合であっても、患者や医療機関担当者が慎重に対応することにより、利活用が滞ることがある
【研究目的】 病院等(*)が自院で入手した医療情報を、自院内で利活用する場合	
【研究目的】 病院等(*)が自院で入手した医療情報を、第三者が利活用する場合	■ 第三者が医療情報を研究目的に利活用する場合に、課題があるとする意見が多く聞かれた **当該分類に関して、課題を法律面、運用面、インフラに分類した上で、次頁以降で取りまとめを行う**

*今回のヒアリング対象では、病院、大学病院、一部の公的研究機関が該当する

法律面では、2000個問題に加え、民間企業では学術研究目的による利活用が行いづらいという課題がある

【第三者が研究目的で医療情報の利活用を行う場合】法律面の課題(1/2)

課題の主要因	課題	課題の詳細	課題を感じているグループ
2000個問題	医療情報の取扱い主体ごとに適用ルール及び解釈権が異なるため、データの取扱いが困難である	■ 個人情報に関する法律に加え、都道府県、市町村、東京23区、広域連合がそれぞれ条例を制定しているため、合計で約2,000個の個人情報保護規定がある ➢ 共同研究を行うに際して、法律や条例の解釈の違いにより求められる要件が異なるため、共同研究を諦めるというケースがある ➢ 複数の機関と共同研究を行う際に、適用される法律及び条例が複数となる場合がある。その法律及び条例をすべて把握することは難しく、医療情報の取扱者として法令順守に不安がある ➢ 将来的に、介護や健康といった医療以外の分野との連携、国際的な連携を行う場合に、連携を困難にする可能性がある	■ 病院 ■ 大学病院 ■ 自治体 ■ 公的研究機関 ■ 民間企業 ■ 情報提供機関
適用除外規定 (学術研究目的)	「学術研究目的」の利活用でも、「研究主体」により個人情報保護法の適用範囲が異なるため、利用の障害となることがある	■「大学をはじめとする学術研究機関、学術研究団体、それらに属する者」が「学術研究目的」で個人情報を利活用する場合のみ、個人情報保護法の一部が適用除外となる（第76条） ➢ 民間企業では、学術研究機関との共同研究であれば、第76条の適用除外が認められる。ただし、研究結果の権利帰属が自社単独でないことから、その後の用途が限定される	■ 自治体 ■ 民間企業 ■ 情報提供機関

法律面では、研究目的で利用する場合に同意を得ずに利活用できる方法が限られていることに加えて、仮名加工情報の取扱いは限定的という課題がある

【第三者が研究目的で医療情報の利活用を行う場合】法律面の課題(2/2)

課題の主要因	課題	課題の詳細	課題を感じているグループ
同意を得ずに利用可能な方法	研究目的で利活用する場合、同意と匿名加工以外の方法がない (学術研究目的を除く)	■ 同意を得ずに医療情報を利活用する際は、匿名加工を行う必要がある。ただし、匿名加工がそぐわないデータである場合、再度同意を取り直す必要がある ➢ 研究成果を、別の研究に用いる際や事業に転用する際（例えば、学術研究目的のデータ解析結果をもとに事業化を行う際）には、当初から別の利用目的を特定して同意取得することは難しい。匿名加工による利活用は可能であるが、匿名加工による情報量の減少が望ましくない場合は、同意の再取得が求められる。ただし、患者が多数に及ぶ場合は、全員に再度連絡して同意を取り直すことは困難である	■ 自治体 ■ 民間企業 ■ 情報提供機関
仮名加工情報の取扱い	現状、仮名加工情報の第三者提供は行えない	■ 匿名加工情報は、「特定の個人を識別することができない」かつ「復元することができない」ように加工する必要がある ➢ 求められる匿名加工水準が高いため、匿名加工情報の利活用には限界がある ➢ 仮名加工情報の取扱いが広がると、情報の利活用が推進されると考える。ただし、令和２年改正後であっても、仮名加工情報を第三者提供することはできない	■ 自治体 ■ 民間企業 ■ 情報提供機関

ルールが複雑と感じられる中、データ提供等のリスクは医療機関に集中している。また、提供のリスクや手間と比較すると、十分なインセンティブが感じられないという課題もある

【第三者が研究目的で医療情報の利活用を行う場合】運用面の課題(1/2)

課題の主要因	課題	課題の詳細	課題を感じているグループ
ルールの複雑さ	2000個問題に加え、研究倫理指針等が難解であり、解釈・理解の統一を図ることが困難であるため、病院からのデータ提供が慎重となる	■ 2000個問題に加え、研究倫理指針等が難解であり、解釈・理解の統一を図る事が難しい ➢ 特に複数の研究機関が関与するような場合には、個々の判断が異なることが多く、具体的なユースケースもないことから、取扱いに迷う	■ 病院 ■ 大学病院 ■ 自治体 ■ 公的研究機関 ■ 民間企業 ■ 情報提供機関
責任主体	データ漏洩等のリスクが医療機関に集中しており、データ提供が消極的となる	■ データ提供における漏洩等のリスクは医療機関にある ➢ 漏洩したデータに匿名化の不備があった等の責任は医療機関が負うため、データ提供には消極的となる	■ 病院 ■ 大学病院 ■ 公的研究機関
インセンティブ	医療機関が外部へデータ提供することに対するインセンティブが乏しい	■ データ提供に対するインセンティブが乏しい ➢ 医療機関は、情報提供のリスクと比較した場合、データ提供のインセンティブを感じられないことも多く、データ提供に消極的な面がある ➢ 情報提供機関においても、医療機関から情報を円滑に提供してもらうためのインセンティブ提示が難しいと感じている	■ 病院 ■ 大学病院 ■ 公的研究機関 ■ 情報提供機関
丁寧なオプトアウト (次世代医療基盤法)	実質的にオプトインと同様の手続が想定されており、現場の負担感が大きい	■ 丁寧なオプトアウトの手続は、実質的にオプトインと同様の手続が想定されており、現場の負担感が大きい ➢ 通知等による手間が医療現場に生じることから、従来通り、患者へ説明して同意を取得する、匿名加工されたデータを入手するといったデータ利活用が行われている	■ 民間企業 ■ 情報提供機関

匿名加工基準が不明確であること、倫理審査委員会の専門性の不統一による判断の分散が大きいことに加え、判定主体が不明瞭であるという課題がある

【第三者が研究目的で医療情報の利活用を行う場合】運用面の課題(2/2)

課題の主要因	課題	課題の詳細	課題を感じているグループ
匿名加工基準が不明確	匿名加工基準が不明確であり、各病院に判断が任されているため、加工手法に分散が大きい	■ 匿名加工基準は、曖昧な記載に留まっている ➢ 匿名加工基準が不明確であるため、一義的な責任を負うことやインセンティブが乏しいことも相まって、匿名加工データの提供を断念する病院がある一方で、十分な匿名加工が行われないままデータが提供される可能性もある	■ 病院 ■ 大学病院 ■ 自治体 ■ 公的研究機関 ■ 民間企業 ■ 情報提供機関
倫理審査委員会(個人情報保護審査会)	倫理審査委員会（又は個人情報保護審査会）の委員の専門性にばらつきがあり、個人情報保護法に詳しいメンバーがいないケースもあるため、判断の分散が大きい	■ 医療情報を提供する場合には、倫理審査委員会の承認が求められる ➢ 病院ごとに設置される倫理審査委員会では、委員の経歴や専門性等にばらつきがあり、個人情報保護法の取扱いに詳しいメンバーが必ずしも含まれるとは限らないため、取扱い判断の分散が大きい ➢ 倫理審査委員会では、法的な側面より倫理的な側面が強くなることにより、データ提供が行われないケースもある ➢ 公立の場合は、個人情報保護審査会にも同様の課題が生じている	■ 自治体 ■ 公的研究機関 ■ 民間企業 ■ 情報提供機関
判定主体	取扱いの判断に迷う場合に、問合せできる外部機関が不明瞭であり、仮に個人情報保護委員会に問い合わせたとしても個別事例に合わせた具体的な回答が返ってこず、判断が難しい	■ 問合せをしても明確な回答を得られる外部機関がない ➢ 具体的な医療情報の取扱いに迷う場合に問い合わせたとしても、個別事例に合わせた具体的な回答が返ってくる機関はなく、現場の判断に委ねられている	■ 病院 ■ 大学病院 ■ 公的研究機関

民間企業から、米国等で運用されているような大規模医療DBを求める声が大きい。データの標準化や名寄せをすることによりデータ結合を行う仕組みが必要である

【第三者が研究目的で医療情報の利活用を行う場合】インフラの課題

課題の主要因	課題	課題の詳細	課題を感じているグループ
標準化	電子カルテ等のフォーマットが異なり、データを結合することが困難な場面がある	■ 標準化されたフォーマットはなく、電子カルテメーカーごとに出力されるフォーマットが異なる ➢ データを入手したとしてもデータの結合が難しい ➢ SS-MIX2など国内の独自フォーマットはあるものの、海外の規格（例えば、OMOP Common Date Model）とは整合しておらず、国際的なデータ比較を行うことができない ➢ 自治体などがスマートシティに取り組むにあたり、どの組織でも使える標準データセットを利活用したいが、データセットの標準化は自治体主導では行えない	■ 大学病院 ■ 公的研究機関 ■ 民間企業 ■ 情報提供機関
データ結合	匿名加工後は、同じ患者の情報であったとしても名寄せは不可能である	■ 匿名加工情報の名寄せは不可能である ➢ 民間企業がデータを取得する際に、匿名加工情報を入手することが多い。匿名加工情報は名寄せできないため、例えば、診療時、投薬時、療養時のデータを別途に入手した場合、データの紐づけができない。そのため、患者の経時的な分析などには利活用することができない	■ 自治体 ■ 民間企業 ■ 情報提供機関
医療DB	主体や目的が限定された医療DBが多く広範な利活用を行う上で課題が多い	■ 主体や目的が限定された医療DBが多い ➢ 一部の母集団に偏った医療DBが散在している。米国等で活用されている医療DBと比較した場合、民間企業は使途が限定されており、利活用が可能なデータ量も少ない傾向にある	■ 大学病院 ■ 自治体 ■ 公的研究機関 ■ 民間企業

主に「学術研究機関以外の研究・事業」を行う場合において、医療情報の利活用のために解決すべき課題が多い傾向にある

第三者が研究目的で医療情報の利活用を行う場合における課題まとめ

医療情報の利活用のために解決すべき課題

課題分類	課題の主要因	課題	学術研究機関以外の研究・事業	学術研究機関との共同研究	研究・事業問わず
法律面	2000個問題	医療情報の取扱い主体ごとに適用ルール及び解釈権が異なるため、データの取扱いが困難である	●	●	
	適用除外規定(学術研究目的)	「学術研究目的」の利活用でも、「研究主体」により個人情報保護法の適用範囲が異なるため、利用の障害となることがある	●		
	同意を得ずに利用可能な方法	研究目的で利活用する場合、同意と匿名加工以外の方法がない(学術研究目的を除く)	●		
	仮名加工情報の取扱い	現状、仮名加工情報の第三者提供は行えない	●		
運用面	ルールの複雑さ	2000個問題に加え、研究倫理指針等が難解であり、解釈・理解の統一を図ることが困難であるため、病院からのデータ提供が慎重となる	●	●	●
	責任主体	データ漏洩等のリスクが医療機関に集中しており、データ提供が消極的となる	●	●	
	インセンティブ	医療機関が外部へデータ提供することに対するインセンティブが乏しい	●	●	●
	丁寧なオプトアウト(次世代医療基盤法)	実質的にオプトインと同様の手続が想定されており、現場の負担感が大きい			●
	匿名加工基準が不明確	匿名加工基準が不明確であり、各病院に判断が任されているため、加工手法に分散が大きい	●		
	倫理審査委員会(個人情報保護審査会)	倫理審査委員会（又は個人情報保護審査会）の委員の専門性にばらつきがあり、個人情報保護法に詳しいメンバーがいないケースもあるため、判断の分散が大きい	●	●	
	判定主体	取扱いの判断に迷う場合に、問合せできる外部機関が不明瞭であり、仮に個人情報保護委員会に問い合わせたとしても個別事例に合わせた具体的な回答が返ってこず、判断が難しい	●	●	
インフラ	標準化	電子カルテ等のフォーマットが異なり、データを結合することが困難な場面がある	●	●	●
	データ結合	匿名加工後は、同じ患者の情報であったとしても名寄せは不可能である	●		
	医療DB	主体や目的が限定された医療DBが多く広範な利活用を行う上で課題が多い	●	●	●

個人情報保護法等 / 個人情報保護法適用外 / 次世代医療基盤法

医療情報の円滑な利活用

医療情報の利活用の方向性の明示や周知、また医療情報を取り扱う専門人材の育成といった課題も聞かれた

国内のヒアリング調査によって聞かれた課題

■ 医療情報の利活用に関する国の方向性が不明瞭である

- 国として、医療情報をどのように蓄積して、どのように活用していくのかといった方向性が明確ではないことから、大規模なインフラ投資にかかる意思決定を各機関で行うことが困難である、との指摘がある
- 日本のデータ利活用に係る保護の考え方として、100%守られる（漏れることがない）ことが前提となっている。しかし、ルールが曖昧で各々の判断に基づき利活用される、優秀なハッカーへの対応は困難である等の課題がある中で、諸外国のようにデータ利活用を促進するためには、データ保護の考え方も見直すべきではないか、という指摘がある

■ 医療情報の取扱いの重要性やデータ利活用の意義を国民に周知して、理解を広げる必要がある

- 医療情報の取扱いに関する教育・研修は、主として医療従事者が受講しているのが、現状である。介護や健康といった分野との将来的な情報連携を踏まえると、地域住民など医療従事者以外にも、医療情報の適切な取扱いについて理解を広げる必要がある、という指摘がある

■ NDB等の医療DBの利活用を推進する場合、データ処理と医療知識を兼ね備えた人材が少ないため、利活用が進まない可能性がある

- 医療DBを公開する場合、データ処理技術と医療知識を十分に持つ人材でなければ利活用が進まない可能性があるが、それらを兼ね備えた人材は現時点で少ない。また、その先にある産業化を見据えた場合、医療DBを利活用した製品やサービス提供を考案できる人材は、さらに少ない。これら人材を育成するため、教育や職業訓練への投資が必要である、という指摘がある

3. 諸外国の状況

3.1「個人情報」の定義

死亡者の個人情報の取扱いに関する法令は各国で異なる。米国では死亡日から50年間HIPAAの適用を受け、またエストニアも死亡後10年間はデータ主体の同意が有効である

法令により保護対象となる個人情報の定義

国・法令	保護対象情報の概要	識別子の例	死者情報
日本 個人情報保護法	• 生存する個人に関する情報 • 個人識別符号が含まれるもの	• 氏名、生年月日その他の記述等により特定の個人を識別できるもの	• 個人情報に該当しない
米国 HIPAA	• 過去・現在・未来の個人の身体的・精神的な健康の状態に関する情報 • 個人に対する医療行為の情報 • 過去、現在、未来におけるヘルスケアの支払に関する情報	• De-identificationの加工で除去が求められる18の識別子等 • Internet Protocol (IP) アドレスも識別子に含む	• 死亡日から50年間、死者に関する個人特定可能な医療情報がHIPAA Privacy Ruleの適用対象となる
欧州 GDPR	• 識別された自然人又は識別可能な自然人（データ主体）に関する情報	• 氏名、識別番号、位置情報、オンライン識別子 • 身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素	• 個人情報に該当しない
英国 UK GDPR	• 識別された、又は識別可能な自然人（natural person）に関する情報	• 氏名、ID番号、位置情報、オンライン識別子（IPアドレス、Cookie） • 身体的、生理学的、遺伝子的、心理的、経済的、文化的、社会的な特有な要素	• 死者は個人情報の性質を持たないためUK GDPRの対象外である • ただし、守秘義務や他の法令により保護される
エストニア PDPA	• データのフォーマットに関わらず、識別された自然人又は識別可能な自然人に関する情報	（特に記載なく、EUのGDPRに準拠）	• データ主体が死亡した場合、その者の同意は死後10年間有効 (データ主体が未成年である場合は、その者の死後20年間有効) • ただし、データ主体の承継人の同意があればデータの処理が認められる
オランダ Dutch GDPR Implementation Act	（特に記載なく、EUのGDPRに準拠）	• 法令には特に記載はないが、オランダ政府のサイトで、氏名、住所、電話番号、国民ID(BSN)を例にあげている(Business.gov.nl)	（特に記載なく、EUのGDPRに準拠）
シンガポール PDPA2012	• 情報の虚偽に関わらず、個人の特定が可能となる情報。個人情報そのもの、又は組織がアクセス権を持つ（可能性のある）個人情報又はその他の情報	• 個人情報を集めていると判断される場合は、cookiesも個人情報に該当する(⇒動画再生に必要なデータを収集するだけのcookiesは個人情報に該当せず同意も必要としない)	• 死者に本条例は適用されない。ただし、個人情報の開示及び第24条(個人情報の保護)は死者であっても死去10年以内であれば適用される

シンガポールを除く調査対象国においては、医療情報を特別な取扱いの対象として定め、取扱い時の追加要件が定められている

個人情報保護法令等における医療情報の取扱い

国	分類	概要
日本 個人情報保護法 第2条第3項	要配慮個人情報	• ①本人の人種、②信条、③社会的身分、④病歴、⑤犯罪の経歴、⑥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政令で定める記述等が含まれる個人情報
米国 HIPAA	保護対象医療情報 Protected Health Information (PHI)	• HIPAAはPHIを対象とした法律であるため、個人情報と要配慮個人情報というような区別はない • 遺伝情報については特別な配慮がなされている（HIPAA,160.502(a)(5)）
欧州 GDPR	特別分類個人情報 Special Category Data	• ①人種・民族の出自、②政治的な意見、③宗教・思想上の信条、④労働組合への加入状況、⑤遺伝子データ、⑥生体データ、⑦健康データ、⑧性生活、⑨性的指向に関する情報の取扱いについてはGDPR第9条の要件を満たす必要がある
英国 DPA2018	特別分類個人情報 Special Category Data	• ①人種・民族の出自、②政治的な意見、③宗教・思想上の信条、④労働組合への加入状況、⑤遺伝子データ、⑥生体データ、⑦健康データ、⑧性生活、⑨性的指向の取扱い • DPA2018の2章にUKGDPRがあり、GDPR9条2項にあたる特別分類個人情報の例外要件の内容がDPAで追加されている
エストニア PDPA	特別分類個人情報 Special Categories of Personal Data	• 特別分類個人情報に関する詳細情報はPDPAには記載されていない。GDPRを精緻化し、補足する法律であるPDPAに規定がないため、GDPRにおける意義と同様に考えることができる
オランダ Dutch GDPR Implementation Act	特別分類個人情報 Special Category Data	• ①人種・民族の出自、②政治的な意見、③宗教・思想上の信条、④労働組合への加入状況、⑤遺伝子データ、⑥個人の唯一無二の識別子となる生体データ、⑦健康データ、⑧性生活、⑨性　的指向
シンガポール PDPA2012	–	• 医療情報に関する特別な取扱いは定められていない • ヘルスケアガイドライン(Advisory guidelines for the healthcare sector)にて、ヘルスケアセクター向けのPDPA解釈指針は出されている

個人を特定できない状態に加工した情報に関する用語や定義、確認方法等は各国により異なる

匿名加工・非識別化の考え方（概要）

国	用語	概要
日本 個人情報保護法 第2条第11項	匿名加工情報	• 特定の個人を識別することができない個人に関する情報であって、個人情報に復元することができないようにしたもの
米国 HIPAA	非識別化 De-identification	• 非識別化において削除対象となる18の識別子を指定 • 専門家によるリスクが最小化されている事の評価
欧州 GDPR	匿名化 Anonymous Data 仮名化 Pseudonymisation	• 識別された自然人又は識別可能な自然人との関係を持たない情報、又は、データ主体を識別できないように匿名化されたデータ(GDPR, 前文26) • 個人情報の仮名化は本人に対するリスクを軽減し管理者が情報保護義務を果たす上で役立つ(GDPR 前文28)
英国 Anonymisation code of practice	匿名化 Anonymisation	• 国内法であるDPAでは匿名化に関する規定はないが、DPA Section 51に基づき、情報独立機関であるICOが匿名化に関するガイドラインを公表している • ICOのガイドラインでは、匿名化とは個人を識別することが起こりえない形にデータを処理することと定義している
エストニア PDPA	仮名化 Pseudonymisation	• 科学的、歴史的研究、統計目的で追加調査が必要だと認められる場合においてのみDepseudonymisation(非仮名化)やその他の方法によって識別不能なデータは識別可能なデータに再び変換される　（”Anonymisation”についてPDPAに記載なし）
オランダ Dutch Medical Treatment Act	匿名化された物質 Anonymous substances	• Dutch GDPR Implementation Actには定めがないため、EUGDPRに準拠 • 身体から分離され、匿名化された物質及び体の一部(Anonymous substances and parts separated from the body)は、その由来となった本人が反対しない限り、医学研究や医療統計に利用可能
シンガポール Advisory Guidelines on the PDPA	匿名化 Anonymisation	• 個人を特定できないデータに変換するプロセスを指す。 • データ自体・他のデータを組み合わせることによって個人を再特定(re-identification)できる可能性がある場合、匿名化されたとは認められない

3.2「個人情報」の取扱いに関して個人に認めている権利

調査対象各国ともに定義や表現は異なるものの、日本と比較すると特に同意の撤回やデータポータビリティ権などの個人情報に関係する権利が充実している傾向にある

個人の権利の各国比較概要

	アクセス	訂正	消去	利用停止	同意の撤回	データポータビリティ
データ管理者が保有する個人情報に対して行使可能な権利の概要	本人が個人情報にアクセスする権利	個人情報の修正を要求する権利	個人情報の消去を要求する権利	個人情報の利用制限を要求する権利	個人情報の使用又は開示に関する同意を撤回する権利	個人情報を第三者に転送することを要求する権利
日本 (個人情報保護法)	開示	訂正等 ※不正確な場合に限る	訂正等及び利用停止等に消去の概念が含まれる	利用停止等 ※主に不正時	–	–
米国 (HIPAA)	Access	Amendment ※不正確な場合等条件有	–	Restriction of use	Revocation	Transmit the copy ※個人の署名が必要
英国 (UK GDPR、DPA等)	Access	Rectification ※不正確な場合に限る	Erasure ※保護規則に違反する場合等	Restriction	Withdraw	Data subject access right / Data portability
エストニア (GDPR、PDPA等)	Obtain information / Access	Rectification / Correction ※不正確な場合に限る	Erasure ※保護規則に違反する場合等	Deny access	Withdraw	Allow third parties to access
オランダ (Dutch GDPR、Implementation Act等)	Access	Rectification ※不正確な場合に限る	Destroy ※自らの治療に関する記録の場合	Restriction	Withdraw	Data portability
シンガポール (PDPA2012)	Access	Correction ※データ保有者に合理的な反対根拠がない場合	–	–	Withdraw ※合理的な通知が必要	Data portability ※施行直後諸条件あり

【参考】日本では開示、訂正等、利用停止等は認められているが、同意撤回権やデータポータビリティ権といった他国で認められている権利の規定がない

日本で認められている権利概要

権利	個人情報保護法	概要	要件
開示	○ （第28条）	個人情報取扱事業者に、当該本人が識別される保有個人データの開示を請求できる権利	行使に必要な要件はない（本人が指定した範囲で開示請求可能）
訂正等	○ (第29条)	個人情報取扱事業者に、当該本人が識別される保有個人データの訂正・追加・削除を請求できる権利	保有個人データが不正確な場合
利用停止等 (同意以外のケースも含)	○ (第30条)	個人情報取扱事業者に、当該保有個人データの利用の停止または消去を請求できる権利	個人情報取扱事業者が、 • 本人の同意を取得せず情報を得た場合（第16条違反）→停止または消去 • 不正の手段で情報を得た場合（第17条違反）→停止または消去 • 同意を取得せず情報を第三者に提供した場合（第23条、第24条違反）→提供の停止

米国では開示請求権、訂正権、利用制限権や承認の撤回権が認められ、個人が第三者にデータを転送要求する権利も認められているが消去権はない

米国で認められている個人の権利（HIPAA）

権利	HIPAA	概要	要件
開示請求権 (Access)	○ （§164.524）	• 個人がPHIを精査し、それらの情報のレコードセットの複製を得るために当該情報にアクセスする権利	• 個人が指定したレコードセットにアクセスを要求する情報がある場合 • 研究が一時停止されない場合 • 個人や他人に危害を引き起こさない場合 等
訂正権 (Amendment)	○ (§164.526(a))	• 個人がPHIや指定されたレコードセットの情報をCovered Entitiesに修正させる権利	• 個人が指定したレコードセットにアクセスを要求する情報がある場合 • CEにより作成されたデータである場合 • 正確かつ完全でない場合 等
消去権	—	—	—
利用制限・停止権 (Restriction of use) (同意以外のケースも含)	○ (§164.522)	• CEに治療や支払、ヘルスケア業務に関するPHIの使用や開示を制限するよう要請する権利	• 救急治療の際に必要となる場合を除く
承認撤回権 (Revocation)	○ (§164.508(b)(5))	• PHIの使用または開示に関する承認を個人が撤回する権利	• 以下の場合を除き、書面での撤回が必要 • CEが承認を信頼して行動していた場合 • 保険契約のために承認した場合
データ転送要求権 (Transmit the copy)	○ (§164.524(c)(3))	• 個人がCEに、PHIの複製を個人が指定した第三者に直接転送することを要請する権利	• 個人が署名した文書で、送付する場所を明確に特定すること

英国は国内法とGDPRで開示請求権、同意撤回権、データポータビリティ権などの個人の権利が認められている

英国で認められている個人の権利（UKGDPRおよびDPA）

権利	DPA, GDPR	概要	要件
開示請求権 (Access)	○ (DPA Section45)	• データ主体がデータ管理者から以下に関する情報を取得する権利 ✓ 自身の個人データが処理されているか ✓ 処理されている場合の処理内容	• 書面で請求すること • 公的な調査を妨害する目的、犯罪目的等ではないこと
訂正権 (Rectification)	○ (DPA Section46)	• データ主体に関する不正確な個人データについて、管理者に修正を要求する権利	• データが不完全または不正確である場合
消去権 (Erasure)	○ (DPA Section47)	• データ主体が個人データの消去をデータ管理者に要求する権利 • ただしデータ管理者が証拠として保管しておくべき個人データは、消去ではなく「利用制限・停止」としても良い	• データ保護規則(Section35-42)に違反する場合 • 機微な情報を保管する上での保護措置が取られていない場合 • データ管理者がデータを消去する義務がある場合
利用制限・停止権 (Restriction)	○ (DPA Section47)	• データ主体が個人データの処理の制限を管理者に要求する権利	• データ主体がデータの正確性に異議を唱え、管理者が正確性を説明できない場合(推奨) • 公的な調査を妨害する目的、犯罪目的等ではないこと
同意撤回権 (Withdraw)	○ (GDPR第7条)	• データ主体が自己の同意をいつでも撤回することができる権利	• 行使に必要な要件はない
データポータビリティ権 (Data subject access right/Data portability)	○ (DPA Section185(4)/ GDPR第20条)	• DPAの”data subject access right”はGDPRの”right to data portability”(第20条)に該当 • GDPRのデータポータビリティ権は個人データを一般的に利用され機械可読性のある形式で受け取り、別の管理者に移行する権利のこと	• 行使に必要な要件はない

エストニアでは個人の権利として開示請求権や訂正消去権、利用停止権、第三者の個人データアクセス権などが国内法で認められている

エストニアで認められている個人の権利（GDPR、PDPA）

権利	法令	概要	要件
開示請求権 (Obtain information/ Access)	○ (PDPA Section24/ Statue of the Health Information System Section16)	• データ処理者が保有しているデータの内容や、入手元、取扱いの目的や法的根拠に関する情報を求めることができる権利	• 行使に必要な要件はない
訂正権 (Rectification/ Correction)	○ (PDPA Section25/ Statue of the Health Information System Section18)	• データ主体がデータ処理者に、個人データの訂正を要求する権利	• 個人データが不正確である場合
消去権 (Erasure)	○ (PDPA Section25)	• データ主体がデータ管理者に個人データを消去するよう要求する権利 • ただし、データを保管する必要がある場合は、消去ではなく「利用制限・停止」にしてもよい	• 個人データが不完全である場合、データ処理の目的が不適切である場合 • 法律で認められていない場合、個人データの処理原則が処理時に考慮されていない場合
利用制限・停止権 (Deny access) (同意以外のケースも含)	○ (Statue of the Health Information System Section19)	• データ主体が、医療従事者の個人データへのアクセスを拒否する権利	• 書面で意思表示すること
同意撤回権 (Withdraw)	○ (GDPR第7条)	• データ主体が自己の同意をいつでも撤回できる権利	• 行使に必要な要件はない
第三者のアクセス権 (Allow third parties to access)	○ (Statue of the Health Information System Section20/ GDPR第20条)	• データ主体が第三者に個人データへのアクセスを許可する権利 • 個人データを一般的に利用され機械可読性のある形式で受け取り、別の管理者に移行する権利	• 行使に必要な要件はない

オランダのDutch Medical Treatment Actでは、医療機関が保有する患者情報の破棄を求める権利も認められている

オランダで認められている個人の権利（GDPR、Dutch Medical Treatment）

権利	法令	概要	要件
開示請求権 (Access)	○ (The Citizen Service Number Use in Healthcare Act 15d)	• データ主体が関係するデータファイルまたは医療従事者が電子交換システムを通じて利用できるデータへのアクセスまたはコピーを要請する権利	• 行使に必要な要件はない
訂正権 (Rectification)	○ (GDPR第16条)	• データ主体が管理者に個人データの訂正を要請する権利	• 個人データが不正確な場合
消去権 (Destruction of the file)	○ (Dutch Medical Treatment Act 455)	• 患者が医療機関に、保有する文書を破棄するよう要求する権利	• 自らの治療に関する記録の場合 • 文書の保管が患者以外の人物にとって非常に重要を除く
利用制限・停止権 (Restriction) (同意以外のケースも含)	○ (GDPR第18条)	• データ主体がデータ管理者から取扱いの制限を得る権利	• 管理者が個人データの正確性を証明しうる期間に、データ主体により個人データの正確性が争われている場合 • 違法な処理であるが、データ主体が個人データの削除に異議を唱え、代わりにその利用の制限を請求する場合 • 管理者の処理のためには必要でなくなったものの、データ主体の法的主張の構成、行使または反論のために必要とされる場合 • データ主体が異議を唱えていて、管理者の正当な根拠がデータ主体の根拠に優先するか否かについて証明が未了の場合
同意撤回権 (Withdraw)	○ (GDPR第7条)	• データ主体が自己の同意をいつでも撤回することができる権利	• 行使に必要な要件はない
データポータビリティ権 (Data portability)	○ (GDPR第20条)	• 個人データを一般的に利用され機械可読性のある形式で受け取り、別の管理者に移行する権利	• 行使に必要な要件はない

シンガポールでは開示請求権や訂正権、同意撤回権が認められているが、消去権、停止権はない。データポータビリティ権は2021年2月法改正により導入された

シンガポールで認められている個人の権利（PDPA）

権利	PDPA	概要	要件
開示請求権(access)	○ (PDPA Section21)	• 組織が処理または管理しているデータや、それらのデータが今後一年以内にどのように使用・開示されるかについての情報提供を個人が要求する権利	• 物理的または精神的な健康を害しない場合 • 公共の利益に反しない場合
訂正権(correction)	○ (PDPA Section22)	• 組織が処理または管理しているデータの誤りや省略の訂正を個人が要求する権利	• 訂正するべきでない合理的な根拠を、組織が示せない場合
消去権	—	—	—
利用制限・停止権 (同意以外のケースも含)	—	—	—
同意撤回権(withdraw)	○ (PDPA Section16)	• PDPAに基づく、個人データの収集・使用・開示に関する同意またはみなし同意をいつでも撤回することができる権利	• 対象機関に合理的な通知をすること
データポータビリティ権 (Data portability) (2021年2月施行)	○ (PDPA Part VIB)	• データを保持している組織に対して、個人が指定したデータの受領組織に転送するよう要求する権利(=data porting request)	• 要求された時点でデータが電子形式であること • 要求を受ける前の所定期間内に、porting organisationにより収集または作成されたこと • 物理的または精神的な安全を脅かさないこと

 出所：https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210#pr13-

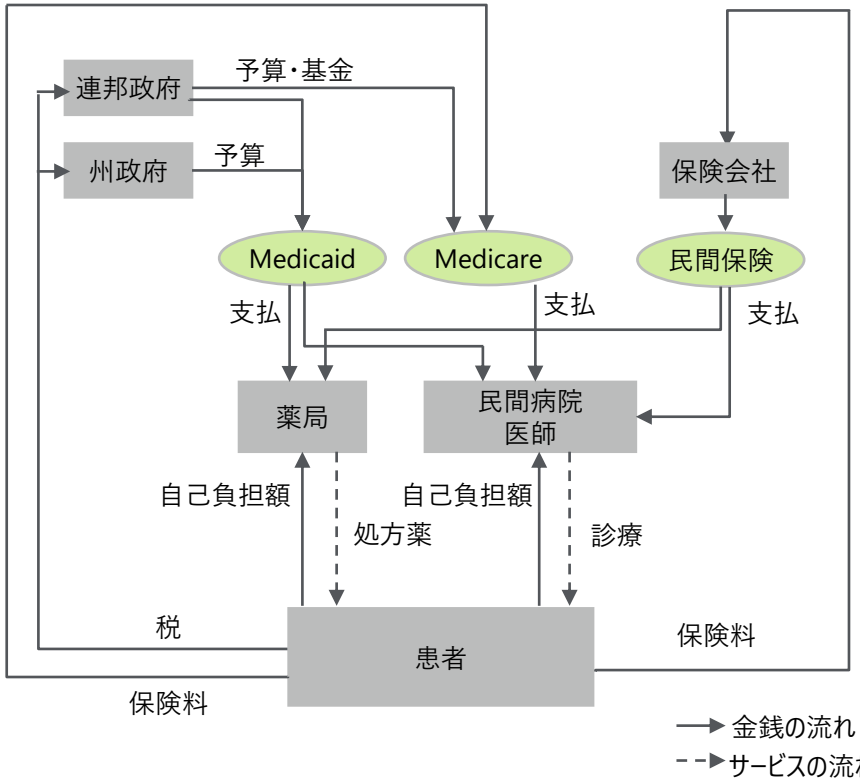
3.3 諸外国における医療情報の保護と利活用

3.3.1 米国 

米国の医療は、公的保険と民間保険が混在して成り立っている。医療情報の取扱いに関しては、主に1996年に制定されたHIPAAにて規定されている

■ 医療制度の概要

制度	概要
医療保険	・現役世代は民間医療保険、高齢者・障がい者は公的医療保険制度が中心である ・公的医療保険制度は高齢者・障がい者に対するMedicareと、低所得者の公的医療扶助であるMedicaidに分かれている ・加入率はMedicare17.8%、Medicaid17.9%、民間医療保険の加入率67.3%である(2018年時点) （保険未加入者は2018年時点で推定2,750万人）
医療機関数	・病院数6,146病院、うち連邦立が209病院（2018年）



■ 健康・医療及び情報保護の法体系

➢ 連邦法

✓ 情報保護関連法

[Federal Trade Commission Act of 1914]
不公平な競争方法及び不公正又は欺瞞的な行為又は慣行を禁止

The Privacy Act of 1974
連邦政府機関によって記録される個人を特定できる情報に関する公正な取扱いの規則を定めた

✓ 医療関連法

Health Insurance Portability and Accountability Act: HIPAA (1996年)
患者の機密情報が患者の同意又は知識なしに開示されることを防ぐ国家標準を定める

Health Information Technology for Economic and Clinical Health Act：HITECH（2009年）
ヘルスケアシステムにおける相互運用可能な電子カルテの使用について制定

年	近年の動向
1996年	・HIPAA制定
2002年	・HIPAAプライバシールール制定
2004年	・医療ITイニシアティブ発表、HHS内にONC設置
2006年	・NHIN構想スタート、eHealth Exchange運用開始
2009年	・HITECH制定
2010年	・Meaningful Use策定
2011年	・ONC推奨のEHR導入インセンティブ開始
2016年	・21st Century Cure Act制定
2018年	・My Health Edataイニシアティブ発表
2021年	・HIPAA改正案発表

出所：https://www.mhlw.go.jp/wp/hakusyo/kaigai/20/dl/t2-04.pdf、http://j-strategy.com/wp-content/uploads/2016/04/461_01.pdf

HIPAAは、州を越えて医療保険の移転が円滑に行われるための連邦法であるものの、情報の電子化・標準化による情報漏洩リスクに対応するため、関連規則を整備している

HIPAAの制定背景

HIPAA

■ 制定の背景
- 従来米国では、医療保険を含む保険は州政府の管轄であり、全米を統一する連邦のルールは存在しなかった
- そのため、まず米国の労働者が別の州の企業へ転職した場合に医療保険の引継ぎを可能にするためHIPAAが制定された
- その後、州を越えた医療情報の移転を円滑に行うためには、医療事務の簡素化並びに情報の電子化・標準化を行う必要がある一方で、電子化等に伴う情報漏洩リスクに対応するため、（一般的な個人情報保護法制が州法、連邦法のいずれにも存在しなかったこともあり）HIPAAに基づく保健福祉省の規則として、HIPAA Privacy Rule やHIPAA Security Rule が、医療分野だけを対象に制定された

■ HIPAAの目的
- 医療保険市場における移転可能性及び継続性（portability and continuity）を改善すること
- 医療保険につき、冗費、不正請求、濫用を防止すること
- 医療費のための貯蓄口座（medical savings accounts）の利用を促進すること
- 長期的な医療保険のサービスへのアクセス及びその対象範囲を改善すること
- 医療保険の事務を簡素化すること

HIPAAに基づく保健福祉省規則

HIPAA Privacy Rule

■ HIPAA Privacy Ruleは、規制対象となる医療機関が保有している特定の個人識別可能な医療情報の利用及び開示に関する詳細な規則を定めている

HIPAA Security Rule

■ HIPAA Security Ruleは、規制対象となる機関に対し、全ての電子化された個人情報に関する機密性、統合性、可用性を確保するために、十分なセキュリティ対策を講ずることを要求している

HIPAAでは、本人が承認した場合、もしくはHIPAA Privacy Ruleに収載されている許可項目以外のデータは使用・開示してはならないと規定されている

HIPAA Privacy Ruleの主な項目

基本原則
Statutory basis and purpose

- データ保持者は、**<u>以下の場合以外にデータを使用、開示してはならない</u>**
  - 対象となる個人（又は代諾者）が文書により承認（Authorize）した場合
  - HIPAA Privacy Ruleにより許可、要求される場合

保護対象情報
Protected Health Information

- 保護対象となる医療情報を「**<u>保護対象医療情報(PHI)</u>**」と規定しており、個人を特定可能な以下の情報が含まれる
  - 過去・現在・未来の個人の身体的・精神的な健康の状態
  - 個人に対する医療行為
  - 過去・現在・未来におけるヘルスケアの支払いに関する情報

対象者
Applicability

- Covered Entities(CE)
  - Health Plan：医療保険組合などの医療保険者
  - Health Care Clearinghouse：保険事務代行業者などの医療情報伝達機関
  - Healthcare Provider：病院、クリニックなどの医療提供者
- Business Associate(BA)
  - CEに代わってPHIの生成、受領、保管、送信等を行う第三者（保護情報取扱組織、電子処方ゲートウェイなど、PHIへのアクセスを日常的に必要とする組織）
  - 法務、保険数理、会計、コンサルティング、データ集約、経営、事務管理、認証、財務等のサービスをCEに提供する者（サービス内容が保護対象情報の開示に関わる場合）

使用又は開示
Uses and disclosure

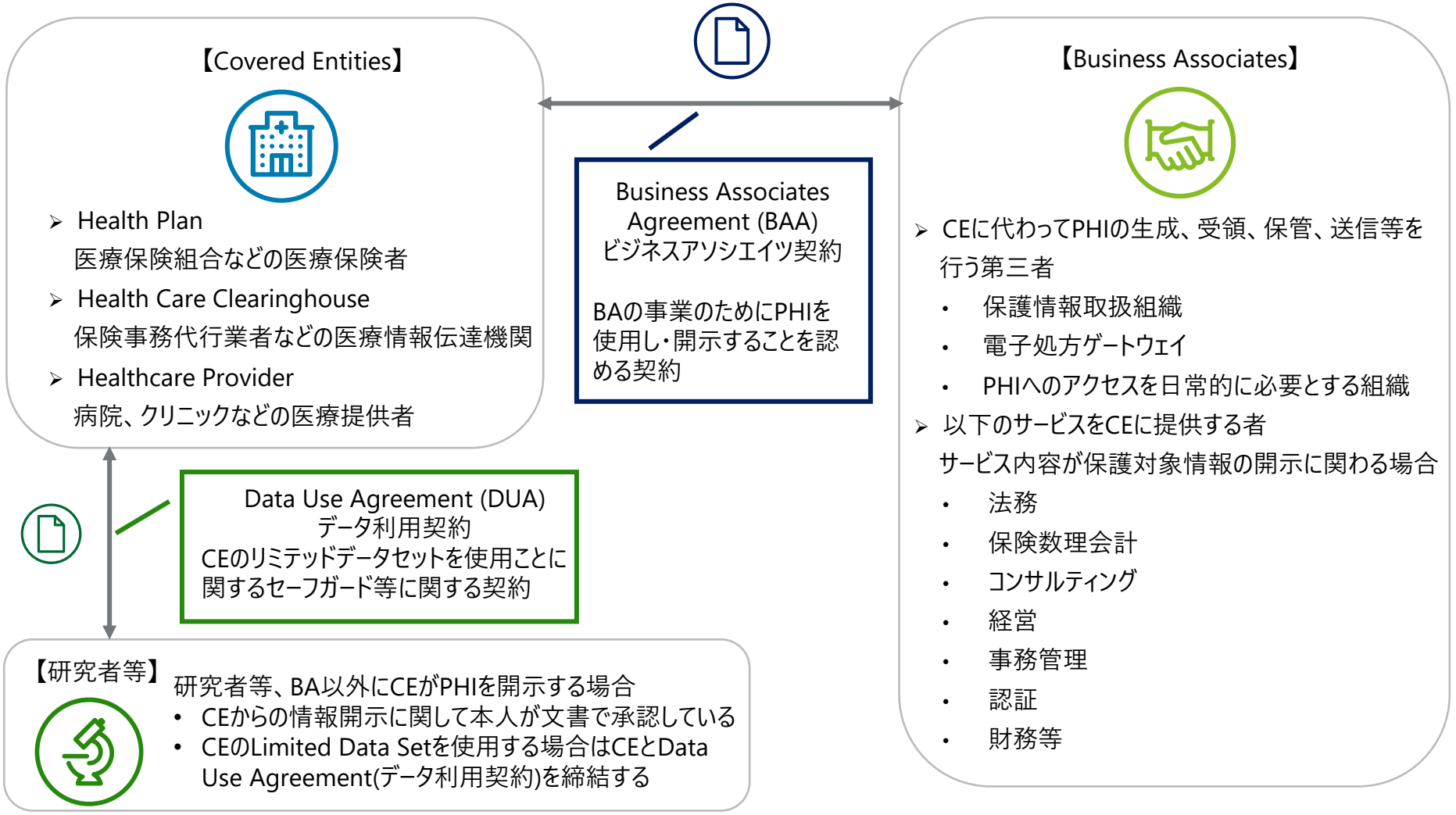
- データ保持者は、治療、支払い、ヘルスケア、それ以外のHIPAA Privacy Ruleにより許可された使用以外に、PHIを使用又は開示する際には、個人の書面による承認を得なくてはならない
- PHIの使用及び開示においては、目的を達成する上で必要最低限(minimum necessary)な範囲にとどめること

違反時の取扱い
Civil money penalty

- 違反した場合の制裁として、保健福祉省は、HIPAA 違反があった場合には、連邦裁判所を通じてその執行を行うことができるほか、制裁金(monetary penalty)を科すこともできる

CEとBAはビジネスアソシエイツ合意書を締結することにより、BAはCEが保有する医療情報へのアクセスが可能となり、BAもHIPAAの遵守が求められる

CEとBAの役割と関係



出所： https://www.hhs.gov/hipaa/for-professionals/faq/251/what-agreements-are-needed-limited-data-set/index.html

HIPAAでは、合意（Agreement）の取り方に関して具体的な方法論を示していないが、承認（Authorization）は、一定の定められた方法がある

同意と承認の違い

項目	一次利用	二次利用
用語	同意（Consent)	承認（Authorization)
関連規則	HIPAA Privacy Rule　§ 164.506	HIPAA Privacy Rule　§ 164.508
規制の目的	健康情報の保護	健康情報の保護
規制対象	CE	CE
該当するケース（例）	■ 名簿管理（氏名、一般的な健康状態、宗教等） ■ 治療・支払い・ヘルスケア業務	■ 心理療法カルテ ■ マーケティング目的での使用・開示 ■ PHIの販売
特徴	■ CEは治療、支払い、ヘルスケア業務に係るPHIの使用と開示に関する同意を取得しても良い（必須ではない） ■ 同意を取得する場合は、形式要件は定められておらず、口頭も認められる（§164.510）	■ 書面による本人の承認を得ることにより、PHIを研究目的で使用・開示して良い ■ Authorizationの文章に含まれる項目を詳細に規定 ■ ただし、「本人の要求に応じて(at the request of the individual)」という記載により、将来の未確定の研究に関しても「十分な目的説明」と解釈することが可能である

研究目的や公益目的等では、本人の承認なくPHIを使用できる要件が別途定められている

　出所：https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA Privacy Ruleでは、治療や支払いに係る業務、研究目的、公益目的等で医療情報の保護と利活用に係る規則を定めている

■ 医療情報の活用場面や目的別に、本人の同意や承認が不要な場合または免除される場合や、本人の承認を取得する場合のHIPAAの規定を整理した

医療情報の活用場面

	項目	内容要約
A	治療、支払い、ヘルスケア業務での医療情報の使用・開示(§164.506)	■ 治療、支払い、ヘルスケア業務に係るPHIの使用と開示が許可されている ヘルスケア業務：病院やクリニックにおける品質保証活動、コンピテンシーの保証活動、詐欺及び不正行為の検出、コンプライアンス活動など診療や支払い以外の医療関係の業務である
B	研究目的での医療情報の使用・開示	■ 研究、公衆衛生、ヘルスケア業務のために非識別化されたデータセットを利用及び開示することができる ■ データ利用契約を締結したリミティッド・データ・セットを利用する ■ CEがPHIを第三者提供する旨について、本人が承認する ■ 「本人の承認」要件の放棄・変更について倫理審査委員会が承認する
C	公益目的での医療情報の使用・開示(§164.512)	■ 個人が合意もしくは反対を行う機会なしに、PHIを使用又は開示することができる場合として、以下の項目が列挙されている(ただし、各項目の適用要件に従う必要がある) a. 法律によって要求される使用と開示 b. 公衆衛生活動のための使用と開示 c. 虐待、育児放棄又は家庭内暴力の被害者についての開示 d. 保健監督活動のための使用と開示 e. 司法及び行政の手続のための開示 f. 法執行を目的とする開示 g. 故人についての使用と開示 h. 死体の臓器、眼又は組織の献体のための使用と開示 i. 研究目的の使用と開示 j. 健康又は安全に対する深刻な脅威を回避するための使用と開示 k. 政府の専門的機能のための使用と開示 l. 労災補償のための開示

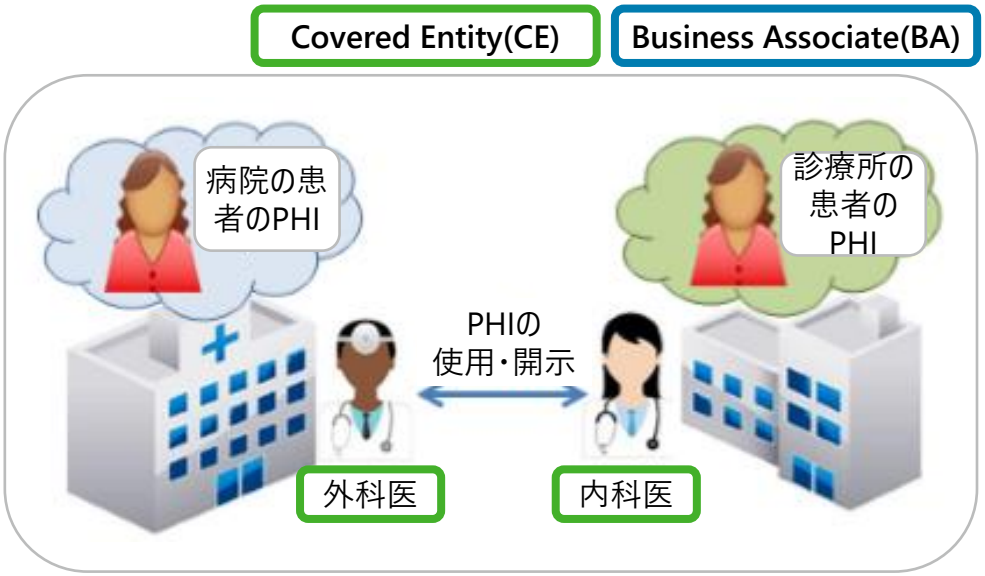
A 治療、支払い、ヘルスケア業務の医療情報の使用・開示

治療・支払いにおいてCEは、Protected Health Information(PHI)を本人の同意や承認なく使用・開示しても良い

■ 「治療(treatment)」：健康管理業務のコーディネーションや運営、医療機関間の患者に関するコンサルテーション、医療機関間の患者の紹介、退院後のリハビリ施設等での将来の継続的なケアを含む

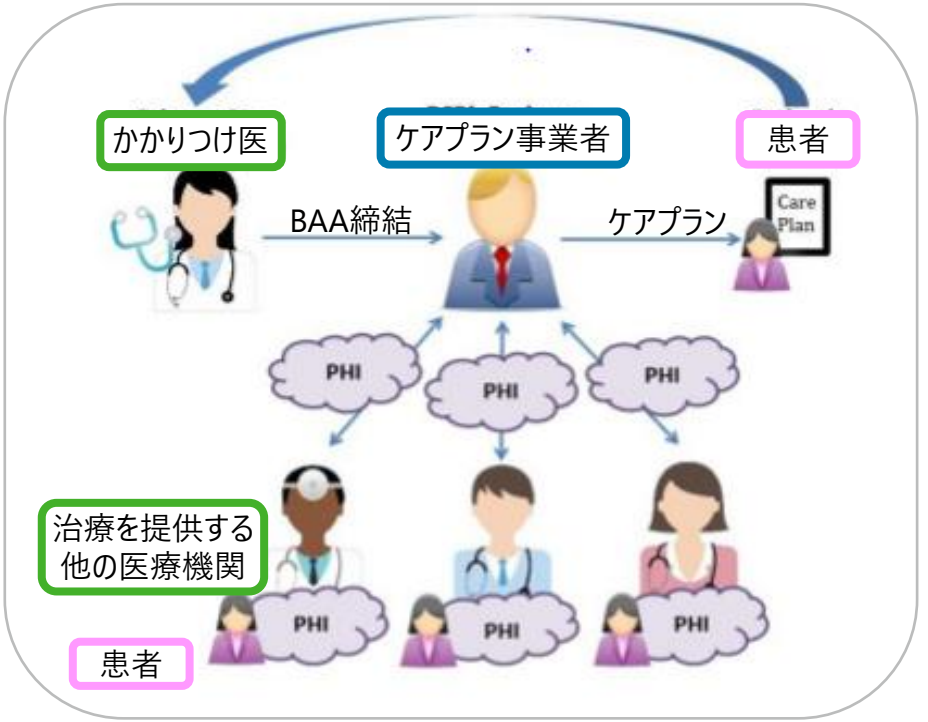
シナリオ１：かかりつけ医と病院の場合

- 患者のPHIを保有する医療機関は、患者の承認(authorization)を取得することなく、他の医療機関にPHIを開示しても良い
- 患者の退院後のリハビリ施設を家族が探す場合や、入居希望先の施設が受入れ判断をする際に患者のPHIが必要な場合、医療機関はPHIを開示しても良い
- PHIを受領した医療機関や施設は、別のCEとしてHIPAAに則って受領したPHIの使用や開示に関する責任を負う



シナリオ２：かかりつけ医師がケアプラン事業者を雇う場合

- 患者が退院した後の経過観察のため、かかりつけ医がケアプラン事業者を雇い包括的なケアプランを管理する場合、かかりつけ医とケアプラン事業者はBusiness Associate Agreement(BAA)を締結する
- 患者のPHIを保有するその他の医療機関は、ケアプラン事業者とBAAを締結することなく、PHIをケアプラン事業者に開示して良い
- 電子PHIを送信する場合のシステムや管理にはHIPAA Security Ruleが適用される



71 出所：Office for Civil Rights, Permitted use and disclosures: Exchange for Treatment (January 2016)

患者の安全管理や医療従事者の資質レビュー等のヘルスケア業務の実施においてもCEは、PHIを本人の同意や承認なく使用・開示しても良い

ヘルスケア業務の内容及び開示の条件

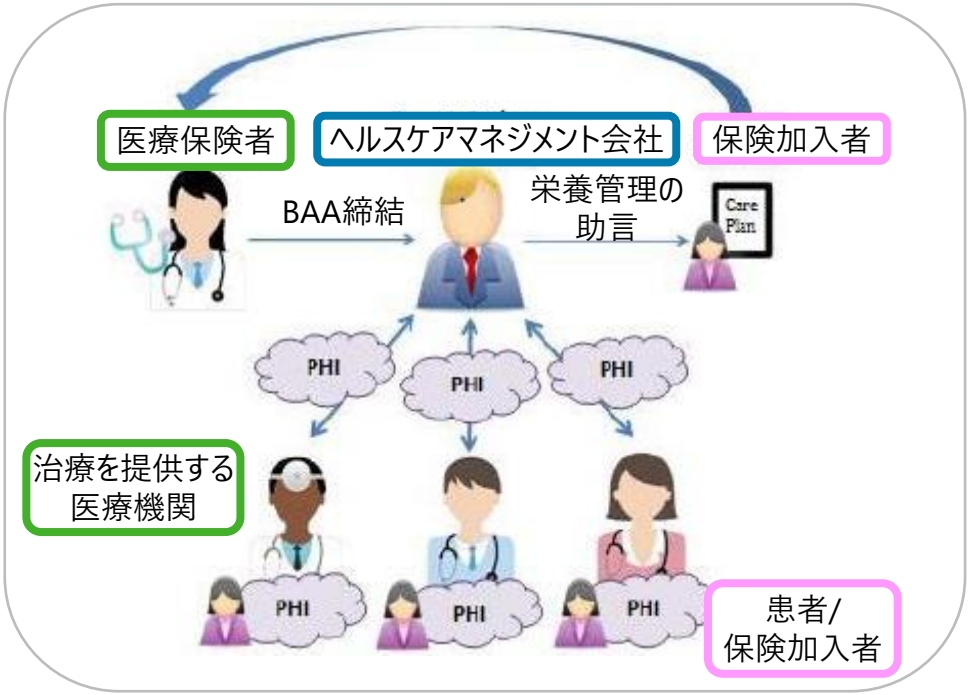
■ ヘルスケア業務（Health Care Operations）の内容
- 品質評価及び改善の取組み
- クリニカルガイドラインの策定
- 規定で定められている患者の安全管理
- 健康改善又は医療費削減に係る集団ベースの活動
- プロトコールの策定
- 症例管理（ケースマネジメント）及びケア計画
- 他の治療方法の情報入手のための医療従事者や患者への連絡
- 医療従事者の資質レビュー
- ヘルスケアプロバイダーや医療保険者の業務評価
- 研修や資格認定業務の実施
- 詐欺や悪用の予防やコンプライアンスプログラムの支援

■ PHIを開示する際の3条件
1. PHIを提供するCEと受領するCEの両者が、患者と関係があること（現在又は過去の患者であること）
2. 求められたPHIが上記の関係に関連するものであること
3. 開示する側は、近い将来のヘルスケア業務のために必要最低限の情報のみを開示すること

■ CEがHIPAAで定義されるOrganized Health Care Arrangement (OHCA)に属している場合は、業務間のPHIの共有が認められる追加的な措置もある

シナリオ３：健康改善・医療費削減に関するヘルスケア業務

- 医療保険者がヘルスケアマネジメント会社をBAとして雇い、糖尿病や糖尿病予備軍の保険加入者に半月ごとの栄養管理の助言を行う
- ヘルスケアマネジメント会社は、保険加入者が医療機関で受けている治療に合った助言を行うために、医療機関にPHIを要求できる
- このシナリオは「健康改善又は医療費削減に係る集団ベースの活動」や「症例管理」のヘルスケア業務に該当する
- 医療保険者はヘルスケアマネジメント会社とBAAを締結するが、治療を提供している医療機関はBAAの締結なく、ヘルスケアマネジメント会社にPHIを直接開示しても良い



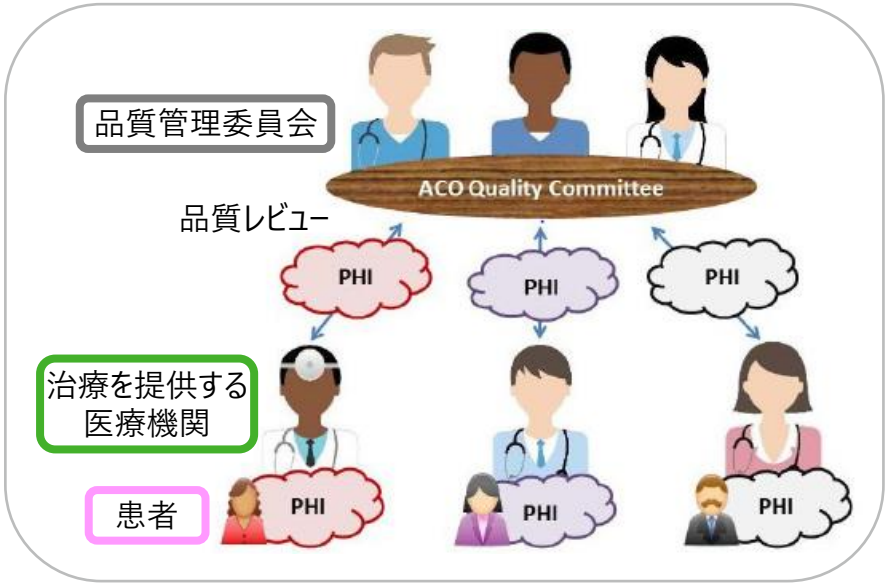
 出所：Office for Civil Rights, Permitted use and disclosures: Exchange for Health Care Operations (January 2016)

医療の質の評価や改善に係るヘルスケア業務においても、本人の同意や承認なくPHIを共有することが可能である

シナリオ４ ：品質評価

【ケース１】　品質管理委員会による評価

- Accountable Care Organization (ACO)がスポンサーとなって、複数の医療機関の医療従事者で構成される品質管理委員会が設置される
- 品質管理委員会は院内感染や医療事故にあった患者の治療や治療の結果に関する情報を入手し、評価する

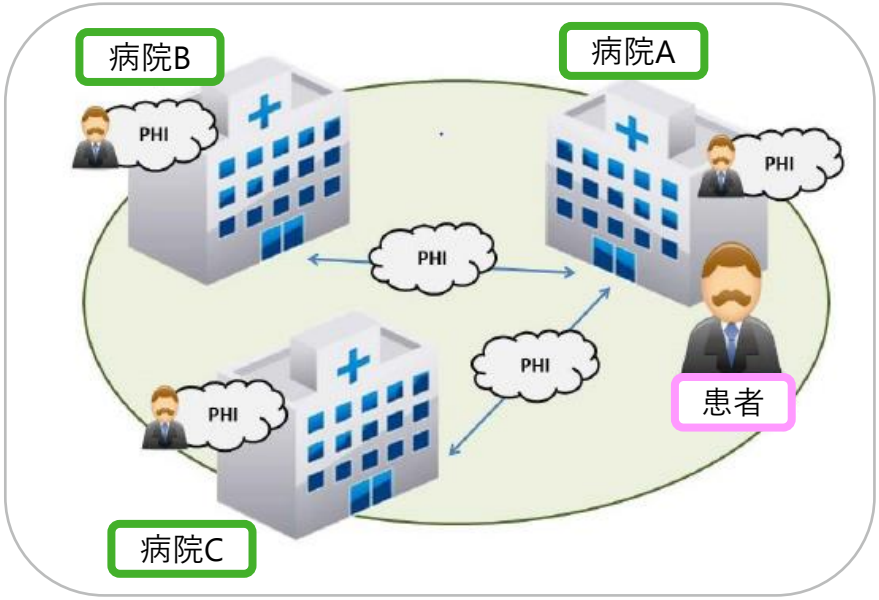


【ケース２】　PHIの共有による品質管理

- 品質管理目的で、ある医療機関が過去に治療を受けていた患者の健康状態の経過を知りたい場合、その患者が治療を受けている他の医療機関にPHIを求めることができる

シナリオ５ ：複数の医療機関の連携による品質改善

- 同じ地域にあるものの協定関係のない医療機関同士では、院内感染を受けた患者が、現在治療を受けている医療機関で感染したのか、これまでに受診した医療機関で感染したのかわからない
- 感染源を特定し、感染拡大を防ぐために、地域内の医療機関は必要なPHIを共有することが可能である
- 電子PHIを共有する際のツールはHIPAA Security Ruleを遵守する必要がある



出所：Office for Civil Rights, Permitted use and disclosures: Exchange for Health Care Operations (January 2016)

B 研究目的での医療情報の使用・開示

HIPAA Privacy Ruleでは研究目的で使用するPHIについて、本人の承認を得る場合と、本人の承認を得なくても良い場合について定めている

研究目的にPHIを使用・開示する場合

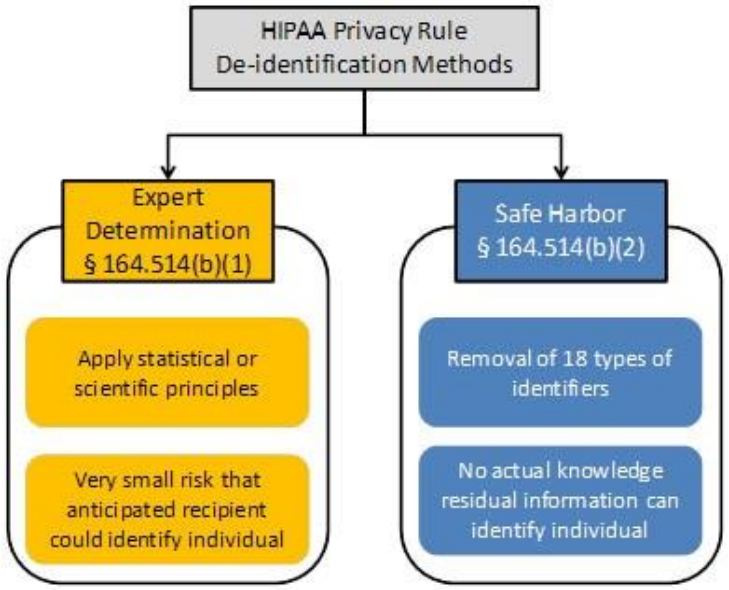
本人の承認は不要	非識別化	■ CEはいつでもに非識別化されたPHIを使用・開示して良い De-identified PHI
	Limited data set	■ データの利用者とデータ利用契約(DUA)を締結することなどにより、CEは本人の承認なくリミテッド・データ・セットの開示が可能である Limited Data Set with a Data Use Agreement
本人の承認の取得が困難な場合	IRB承認	■ PHIへのアクセスが必要であるものの本人の承認要件の放棄がないと研究が不可能である場合、倫理審査委員会（IRB)又はプライバシー委員会から「本人の承認」要件の放棄・変更の認可を得る Documented Institutional Review Board (IRB) or Privacy Board Approval
本人の承認	本人の承認	■ 本人の承認によるPHIの使用・開示 Research Use/Disclosure with Individual Authorization

出所：https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/research/index.html

【非識別化】HIPAA Privacy Ruleに定められた手法で非識別化されたPHI（De-identified protected health information）の利活用には本人の承認は不要である

PHIの非識別加工には、専門家が統計学を使って加工し、個人の識別化リスクを小さく(very small)した場合と、18個の識別子を取り除くことで非識別化されたとするセーフハーバー方式がある

非識別化の２つの手法



非識別化された保健情報は、個人を特定することが不可能であるか、個人を特定できる合理的な事項を提供しないと定められており、情報の非識別化には、以下の2つの方法がある

1. 専門家による計画、加工、リスクが最小化されている事の評価
2. セーフハーバー方式：個人の特定に繋がりうる18個の識別子を除く

セーフハーバー方式で定められている18個の識別子

(A)氏名
(B)所在地住所（市、郡、警察管区、郵便番号、及びこれらに相当するジオコードを含め、州より下位のすべての地理的区画）
(C)出生日、入院日、退院日、死亡日を含めて個人に直接関係する日付についてのすべての日付要素（年を除く）
(D)電話番号
(E)ファックス番号
(F)電子メールアドレス
(G)社会保障番号
(H)カルテ番号
(I)医療保険の受益者番号
(J)口座番号
(K)証明書/ライセンス番号
(L)ナンバープレートの番号を含めて、車両の識別子と製造番号
(M)デバイスの識別子と製造番号
(N)ウェブのURL
(O)インターネットプロトコル、IPアドレスのナンバー
(P)指紋及び声紋を含め、生体認証の識別子
(Q)全体の写真画像及びこれに相当する画像
(R)その他の識別番号、特徴又は識別コード

 出所：https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

【非識別化】専門家(expert)に求められる学位や認証はないが、専門家が非識別加工を実施した場合、専門家の知見や非識別加工の手法を書面化する必要がある

専門家とは

■ 専門家とは誰を指すのか

- 専門家の明確な定義は存在しない
- 個人を特定できない情報を提供するための、一般的に認められた統計的・科学的な原則と方法に関する適切な知識と経験を有する者
- PHIのde-identificationを行う専門家と認めるためのプログラム・学位等も存在しない
- 専門家となりうる人物として、統計学、数学、その他科学分野に関連する事が考えられる
- これらの分野に限定されるわけではなく、様々な教育や経験を通じてde-identification関連の専門性が得られる事が考えられる
- HHSの Office for Civil Rights (OCR)は、CEが使用した専門家の職務経験や学術的又はその他の教育、医療情報の非識別化の手法を採用した専門家の実務経験を評価する

■ 非識別化の加工基準

- 識別リスクが"Very small"のレベルであればde-identificationとして認められるため、明確な数値基準等は存在しない
- 明確な基準を設けていない理由として、ある特定の環境下で適切とされたデータセットの識別リスクは、異なる環境下においては適切な識別リスクとは評価されない可能性があるためである
- 専門家は、情報の利用者が個人を識別化し得る能力を考慮したうえで、許容可能な"Very small"リスクを定義し、評価する必要がある

専門家による個人識別化リスクの評価プロセス

■ 専門家によるリスク評価のプロセス

- OCRは特定のプロセスを要求していないが、プロセスが正当であるということを分析の方法と結果を含めて文書化し、必要に応じてOCRが利用できるようにすることを要求している

【非識別加工に関する専門家の判断プロセス】

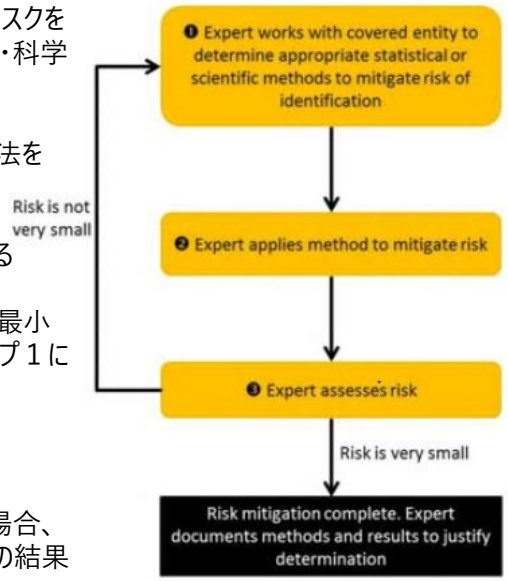
1.専門家とCEは識別化のリスクを抑えるための適切な統計的・科学的な手法を決定する

2. 専門家が非識別化の手法を実践する

3. 専門家がリスクを評価する

リスク評価の結果、リスクの最小化が認められなければステップ１に戻る

リスクの最小化が完了した場合、専門家は手法と非識別化の結果について書面化する



77 出所：https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#expert

【非識別化】2つの非識別化(de-identification)の手法は、個人を識別するリスクをゼロにすることではなく軽減することを目指しているため、再識別化のリスク評価も行われている

非識別化の目的は、非識別化情報の利用と個人のプライバシーの保護であるが、非識別化の量と非識別化情報の有用性はトレードオフ関係にある。そのため、適切なセキュリティレベルを定め、非識別化とデータの有用性のバランスを保つ必要がある（NIST）

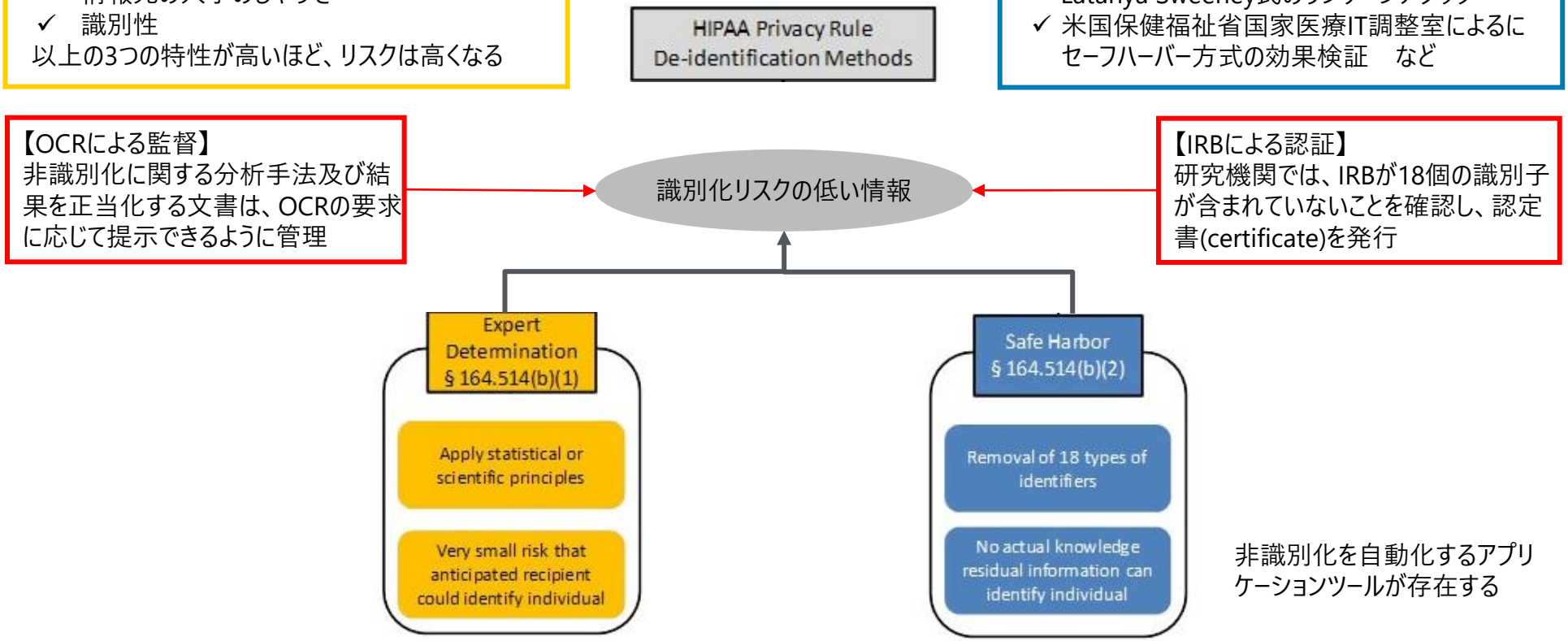
専門家によるリスク評価

統計学の知見のある専門家によるリスク評価
- ✓ 反復性
- ✓ 情報元の入手のしやすさ
- ✓ 識別性

以上の3つの特性が高いほど、リスクは高くなる

セーフハーバー方式の効果検証

研究者による再特定アタック(re-identification attacks)やデータ侵入テスト
- ✓ Latanya Sweeney氏のリンケージアタック
- ✓ 米国保健福祉省国家医療IT調整室によるにセーフハーバー方式の効果検証　など



非識別化を自動化するアプリケーションツールが存在する

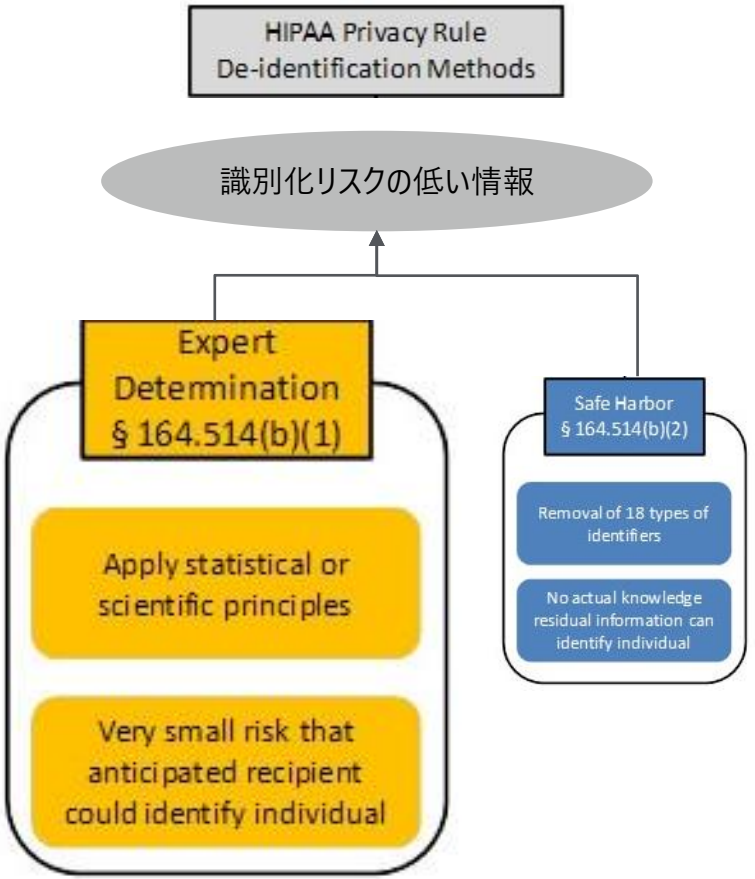
出所：De-Identification of Personal Information (NIST: National Institute of Standards and Technology, U.S. Department of Commerce)
https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

【非識別化】専門家に求められる特定の学位や認定はないが、米国統計学基準の知識と非識別加工の経験を有する者が、個人が識別されるリスクを軽減するように加工する

専門家（expert）による識別化リスクの判定基準（HHS）

基準	概要	リスクレベル（例）
①反復性 Replicability	個人に関係する一貫性のある医療情報は、リスクレベルをあげる	低：患者の血糖値の検査結果は異なる
		高：患者背景（誕生日など）は安定した情報である
②情報元の入手のしやすさ Data source availability	どの外部データに患者の識別子となるもの、又は反復性の特徴があるか、そして誰がそのデータにアクセスできるかを判定する	低：検査結果は医療環境外で識別可能な状態で開示されることはまずない
		高：患者の氏名や患者背景、出生、死亡、結婚、住民登録などの情報
③識別性 Distinguishability	医療情報の中で本人のデータを識別できる度合いを判定する	低：生年、性別、郵便番号３桁の組合せで唯一無二な人は全米の0.04％であると推定されており、この組合せのデータで特定される住人はほとんどいない
		高：患者の誕生日、性別、5桁の郵便番号の組合せで唯一無二な人は全米の住人の50％以上と推定されており、この3つの要素だけで全米の半数の人を特定できる
リスク評価 Assess Risk	上記①～③の可能性が高いほど識別化のリスクは高くなる	低：検査値は識別性が高いかもしれないが、それらの複製可能性は低く、多くの人がアクセスできる複数のデータで開示されることはまずない
		高：患者背景は識別性が高く、反復性があり、公共の情報源から入手しやすい

専門家は統計学の原理を適用し、予測し得るデータ利用者が個人を識別できるリスクを評価する



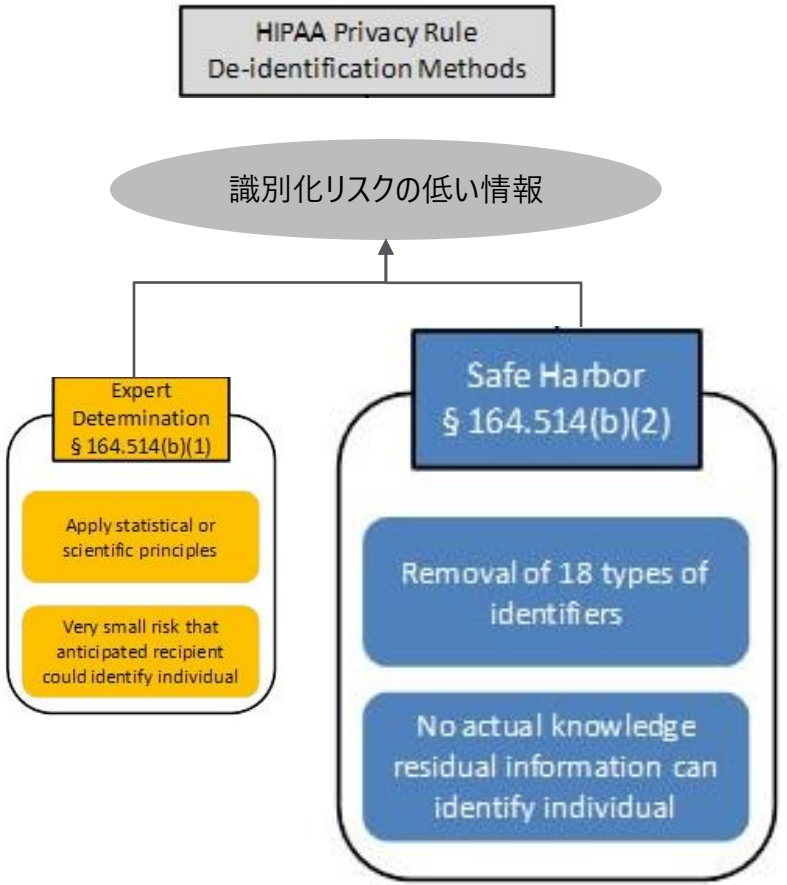
 出所：https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

【非識別化】米国保健福祉省のONCが実施した、セーフハーバー方式による非識別化の有効性の検証によると3万件のデータのうち再識別化される可能性は非常に低かった

セーフハーバー方式の有効性

【セーフハーバー方式の効果検証】
米国保健福祉省の国家医療IT調整室が2010年に実施
Office of the National Coordinator for Health Information Technology
(ONC HIT)

1. 研究者は2004年～2009年の15,000医療機関のヒスパニック系受診者の記録を与えられた
2. 研究者はその非識別化情報と、2億3,500万人分の米国の消費者データを有するInfoUSA社の市販データ3万件との突合を試みた
3. 国勢調査のデータに基づき、研究者は3万件の市販データの中には、5,000人の患者が含まれると推定した
4. 実験において、性別、郵便番号3桁、年齢を使い、医療機関データから216件の唯一無二(unique)なデータを見つけ、InfoUSA社データからは84件の唯一無二なデータを見つけた。そしてそれらのうち20件が両方のデータセットと一致した。
5. 研究者がこの20件を精査した結果、2件が同じ名字、番地、電話番号であった
6. この実験の結果、再特定の可能性は0.013％と推定された。より保守的な算定手法を持ってしても、再特定の可能性は0.22％であった。ただし、この実験は一つの人種グループに基づいた算定結果であるため、全国レベルの率ではない



出所：https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

【本人の承認】CEが医療情報を第三者に使用・開示する場合、研究目的や開示先等の必須項目を記載した書面にて本人の承認を取得する必要がある

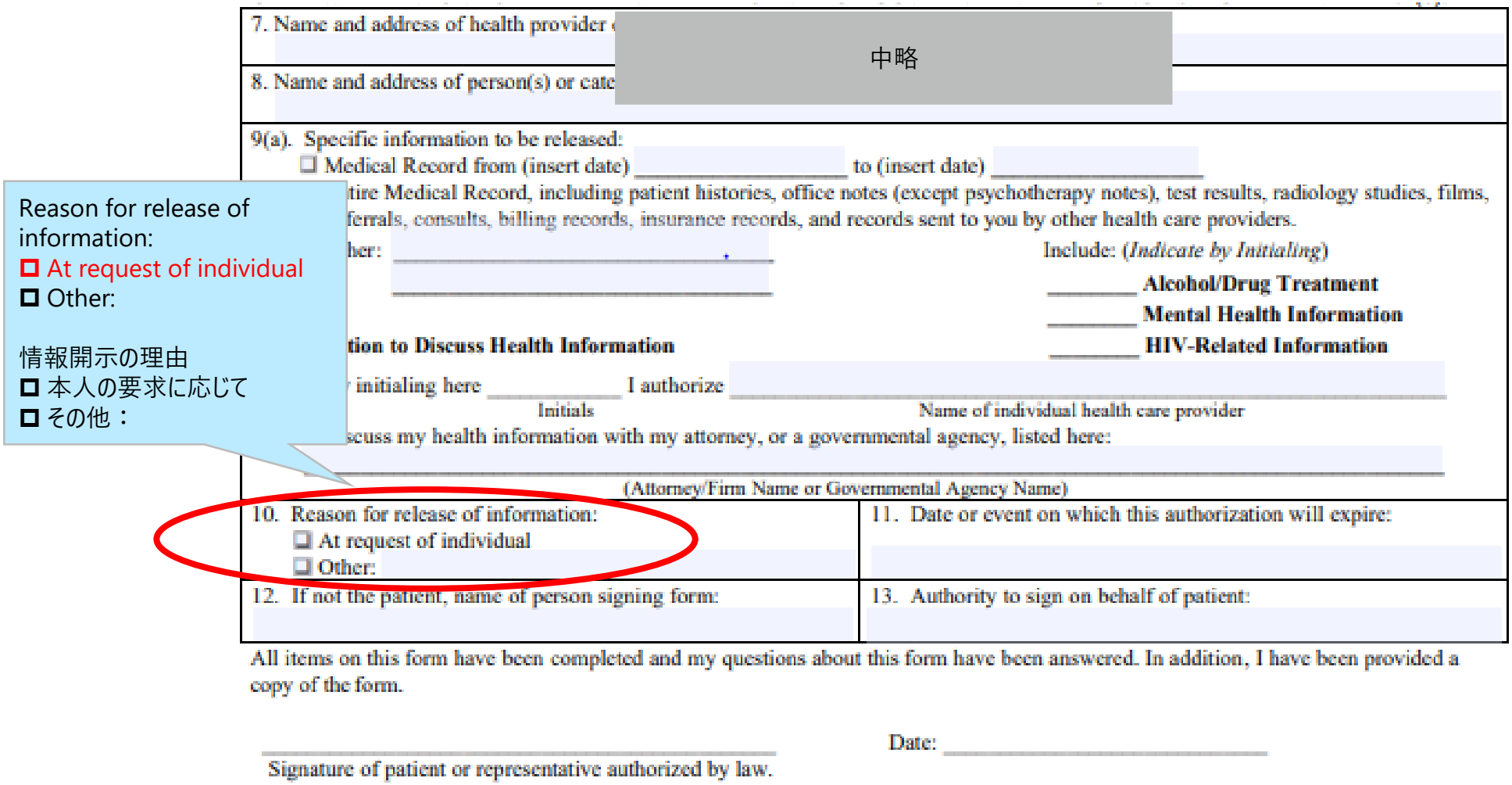
研究目的でのAuthorization（承認）の文書に含まれる項目

項目		記載内容	詳細・記載例
必須項目 (Core Elements)	何を	使用・開示されるPHIの説明	医療記録の全て、検査結果、病歴など
	誰が	承認を受ける者の氏名又はその人物を特定できる情報	「○○医療機関(CE)の全ての医者」など
	誰に	PHIを使用する、又はCEがPHIを開示する相手の氏名又はその人物を特定できる情報	研究者とその補助研究員の氏名、研究の依頼者 (Sponsor)、その他PHIにアクセスする者など
	何故	PHIの使用・開示の目的となる研究内容	「本人の要求に応じて（at the request of the individual)」という記載により、将来の未確定の研究に関しても「十分な目的説明」と解釈することが可能
	いつまで	承認の有効期限	研究データベースやリポジトリの作成・維持を含む研究については、「研究の終了時」、「なし」という記載も可能
	署名	個人による署名、日付の記載	個人の代理人により署名された承認の場合、代理人が個人のために行動する権限の説明を記載する
必要説明文 (Required Statements)	承認の取消し	書面による個人の承認を取り消す権利等	承認を取り消す権利に加え、下記のいずれかを記載する (1)承認を取り消す権利の例外事項、及び個人が承認を取り消す方法の説明、又は(2)CEのプライバシー慣行の通知(Covered Entity's Notice of Privacy Practices)の承認の取消しに該当する部分についての言及
	承認取消しによる影響	個人が承認を拒否した場合、研究関連の治療等が受けられなくなる可能性についての通知	(1)署名は任意であるが署名しない場合には研究関連の治療を受けられなくなること、(2)該当する場合は承認への署名を拒否することによる結果
	HIPAA Privacy Ruleの適用範囲	PHIがデータの利用者によって更に開示される可能性があり、その場合はHIPAA Privacy Ruleの適用を受けないこと	本人の承認によりCEでない個人や組織（研究依頼者や資金提供者など）にPHIが開示された場合、HIPAA Privacy Ruleは彼等には適用されないが、他の連邦法やCEとの契約により継続的にプライバシーが守られる可能性はある

出所：https://privacyruleandresearch.nih.gov/authorization.asp
https://www.hhs.gov/sites/default/files/hipaa-future-research-authorization-guidance-06122018%20v2.pdf

【本人の承認】「本人の要求に応じて（at the request of the individual)」という記載により、将来の未確定の研究に関しても「十分な目的説明」と解釈することが可能である

医療情報の開示に関する承認文書のサンプル



7. Name and address of health provider

中略

8. Name and address of person(s) or cate

9(a). Specific information to be released:

☐ Medical Record from (insert date) _____ to (insert date) _____

tire Medical Record, including patient histories, office notes (except psychotherapy notes), test results, radiology studies, films, ferrals, consults, billing records, insurance records, and records sent to you by other health care providers.

her: _____

Include: (*Indicate by Initialing*)

_____ **Alcohol/Drug Treatment**

_____ **Mental Health Information**

_____ **HIV-Related Information**

tion to Discuss Health Information

initialing here _____ I authorize _____

Initials — Name of individual health care provider

scuss my health information with my attorney, or a governmental agency, listed here:

_____

(Attorney/Firm Name or Governmental Agency Name)

Reason for release of information:
☐ At request of individual
☐ Other:

情報開示の理由
☐ 本人の要求に応じて
☐ その他：

10. Reason for release of information: ☐ At request of individual ☐ Other:	11. Date or event on which this authorization will expire:
12. If not the patient, name of person signing form:	13. Authority to sign on behalf of patient:

All items on this form have been completed and my questions about this form have been answered. In addition, I have been provided a copy of the form.

_____ Date: _____

Signature of patient or representative authorized by law.

 出所：https://18yb2h2362gn1q057p2y390z-wpengine.netdna-ssl.com/wp-content/uploads/2015/03/HIPAA-OCA-official-Form-No.-960.pdf

【本人の承認】本人が承認を取り消した場合、CEはPHIの将来の使用・開示を停止する必要があるが、承認の取消し後もPHIの使用・開示が認められる例外措置がある

承認の取消しに関する原則と例外

【原則】
- 「承認の取消し」は、CEが実施してきた研究におけるPHIの使用・開示を限定するものであり、CEによる将来の使用・開示を避けることができる
- 本人はいつでも承認を取り消すことができる
- 承認取消しの際は、所定の宛先に文書を提出する必要がある。又は、EHRのポータルサイトで承認を取り消す方法でも良い。なお、CEが口頭による承認の取消しを受諾するのであれば、HIPAA Privacy Ruleはそれを妨げない
- 本人の承認取消しをCEが認識することにより、取消しが有効になる。例えば、CEでない研究者に承認の取消し文書が提出されても、その研究者はCEに承認の取消しを通知することは求められていない。そのため、CEが本人の承認取消しの意思を認識できなければ、承認が無効であることにならない

【例外】
- 「承認の取消し」により個人の情報が研究目的で全く使用されなくなるわけではなく、また他の目的で開示されないとは限らない。以下に、例を挙げる

研究実施主体	本人の承認が取り消されてもPHIの使用・開示が認められる場合
CE	■ 承認の取消し前に取得したPHIについては、承認の内容に基づいて実施する研究の範囲であれば、PHIの使用・開示の継続が可能
	■ CEが現在実施中の研究の完全性・信用性を維持するために必要な場合 • 本人が研究から退いた理由の説明 • 研究不正に関する調査 • 治療や処置に際して見られる好ましくない徴候、症状、疾患、検査値異常の報告
	■ HIPAA Privacy Ruleで認められている他の業務内容においてPHIを引き続き使用することが可能 • 品質評価や品質改善のようなヘルスケア業務を行うための研究目的で収集したPHIの利用
CE以外	■ 研究主体がCE以外の場合でも、研究に関与しているCEは、現在実施中の研究の完全性・信用性を維持する上で必要な場合、PHIの使用・開示を継続して良い

出所：https://privacyruleandresearch.nih.gov/authorization.asp
https://www.hhs.gov/sites/default/files/hipaa-future-research-authorization-guidance-06122018%20v2.pdf

【IRB承認】倫理審査委員会又はプライバシー委員会の認可により、CEは本人の承認要件の放棄・変更をし、本人の承認なく研究目的にPHIを使用・開示することが可能である

研究の種類によっては、研究者が被験者から書面による承認を得ることが現実的でないケースも存在する。このようなケースに対処するため、HIPAA Privacy Ruleには、IRB又はPrivacy Boardによる承認要件の放棄又は変更を行うための基準が設定されている

倫理審査委員会(IRB)とプライバシー委員会

■ 倫理審査委員会（IRB：Institutional Review Board *1)

- 被験者が人間である研究を審査するために、機関が正式に指定した理事会、委員会、又はその他グループのことを指す
- IRBは、HHS及びFood and Drug Administration(食品医薬品局) の「Human Subjects Regulations」の対象となっているすべての研究活動を承認、修正、又は不承認とする権限を有している

■ プライバシー委員会（Privacy Board *2)

- Privacy Boardとは、特定の研究のためのPHIの使用・開示に関して、HIPAA Privacy Ruleに基づいて、承認要件の放棄又は変更の要求に対応するために設立されている審査機関である
- Privacy Boardは、特定の研究プロジェクト等の承認要件の全部又は一部を放棄、変更できる
- CEはPrivacy Boardから放棄・変更の文書を受け取ることで、承認なしでPHIを使用し、開示することができる

※IRBを設定していない機関やIRBにプライバシーに関する専門家がいない場合、IRBよりも構成人数が少なく、また他分野の専門家によって構成されるプライバシー委員からの審査書面の受領が認められている

「本人の承認」要件の放棄・変更に必要な条件

■ 「本人の承認」要件の放棄・変更に関する認可

- CEは、本人の承認要件の放棄・変更の下でPHIを使用・開示するためには、文書化されたIRB又はPrivacy Boardの認可が必要である

■ IRB又はPrivacy Boardによる認可を得るために必要な3つの基準

1. 以下の要素をもってPHIの使用・開示に係る個人のプライバシーに対するリスクが最小限におさえられている

   ①識別子の不適切な使用・開示から保護する計画がある

   ②健康上・研究上の正当な理由がない場合や、法律で保持が要求されていない場合には、研究と整合性を保ちつつ、速やかに識別子を破棄するための適切な計画がある

   ③法律で要求されている場合を除いて、PHIの再利用や開示がされない旨の書面による保証が十分ある

2. 「本人の承認」要件の放棄・変更がないと、研究が実質的に不可能である
3. PHIへのアクセス及び利用がないと、研究が実質的に不可能である

出所：*1 National Institute of Health　https://privacyruleandresearch.nih.gov/irbandprivacyrule.asp
*2 National Institute of Health　https://privacyruleandresearch.nih.gov/privacy_boards_hipaa_privacy_rule.asp

【Limited data set】研究・公衆衛生・ヘルスケア関連業務目的のためにデータ利用契約を締結した上で本人の承認なしにLimited data setの使用と開示が許可されている

リミテッド・データ・セット (Limited data set)

- 16種類の直接識別情報を除外したPHIのことで、研究・公衆衛生・ヘルスケア関連業務目的のためにData use agreementを結んだうえで、個人の許可なしに使用と開示が許可されている
- 16種類の識別子と、セーフハーバー方式で定められている匿名化のための18種類の識別子の違いは「出生日、入院日、退院日、死亡日を含めて個人に直接関係する日付についてのすべての日付要素（年を除く）」と「その他の識別番号、特徴、または識別コード」である
- 個人の居住都市、何らかの日付・番号等、直接識別情報ではない情報は、Limited data setに含まれる可能性がある

【除外される16種類の識別子】

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

※ なお、データ利用契約を締結した場合であっても、使用と開示に当たって、倫理審査委員会の審査を経る必要がある

データ利用契約（Data use agreement)

- Data use agreement とはCovered entity（CE）と研究者の双方が締結するデータ利用契約で、この締結に基づき、CEは研究、公衆衛生、またはヘルスケア関連の運営等のために、Limited data setを研究者に開示することができる
- Limited data setは直接個人特定が可能となる特定の識別情報(specified direct identifiers of the individual)を除外しなければならない
- Data use agreement は以下を満たさなければならない

1. データの利用者によるLimited data setの使用・開示が研究の目的と整合しており、プライバシールールを侵害しない範囲のものとすること
2. 情報の利用者を限定する
3. Limited data setの利用者が以下について同意する
   - ➢ Data use agreementまたは法によって認められた場合は情報を使用・開示してはならない
   - ➢ Data use agreementに含まれていない情報の使用・開示に関する安全管理方法の適用
   - ➢ Data use agreementに含まれていない情報の使用・開示に関する報告義務
   - ➢ Limited data setの利用者から情報を受領した再委託の受託先等にもLimited data setの利用書と同様の制限や条件が適用される

出所：National Institutes of Health　https://privacyruleandresearch.nih.gov/pr_08.asp
HHS　https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

【Limited Data Set】Centers for Medicare & Medicaid Services (CMS) が管理している3種類の医療データを研究目的に使用することも可能である

CMSデータの種類と内容

- Centers for Medicare & Medicaid Services (CMS)とは、米国保健福祉省(HHS)内の機関で、米国の主要な医療プログラムを管理している
- CMSはMedicare、Medicaid、子供の健康保険プログラム、州と連邦の健康保険市場を含むプログラムを監督している
- CMS dataとは、そのCMSにより収集・分析されたデータのことで、このデータに基づき調査報告書の作成し、医療制度内での不正や乱用の事例を排除するために活動している

CMSデータの種類	概要
1. Identifiable Data Files (IDF)	PHIやPII(personally identifiable information)を含み、特定の利害関係者のみが利用可能。IDFを要求するには、原則CMSへのDUA(Data Disclosures and Data Use Agreements)が必要となる
2. Limited Data Set (LDS)	PHIも含むが、HIPAA Privacy Ruleで定義される直接識別情報は含まれていない。LDSは研究目的で利用可能であり、すべてのデータ要求者はCMSにDUAを提出しなければならない
3. Public Use Files (PUF)	個人を識別するために使用できる情報は含まれていない。PUFのデータを要求するうえで、DUAは必要ない

出所： Investpedia　https://www.investopedia.com/terms/u/us-centers-medicare-and-medicaid-services-cms.asp
CMS DUAs　https://www.cms.gov/Research-Statistics-Data-and-Systems/Files-for-Order/Data-Disclosures-Data-Agreements/Overview

C 公益目的での医療情報の使用・開示

「公共の利益やベネフィットにつながる場合」は個人が合意もしくは反対を行う機会なく、PHIを使用又は開示することができる

公共の利益やベネフィットにつながる場合(§164.512)

項目	要件・概要
a. 法律によって要求される場合	■ 保護対象情報の使用又は開示が法律によって要求され、使用又は開示が法律に適合し該当する法律の要件に限定されている範囲で、使用又は開示することが可能 ■ (c)(e)(f)に準ずる
b. 公衆衛生活動のため	■ 適用対象機関は、公衆衛生活動を目的として、保護対象情報を使用又は開示することが可能 ■ 例えば、疾病、負傷、障がいの防止又は抑制のために情報を収集又は受領する権限を、公衆衛生当局又は公衆衛生当局の指示により行動している外国政府機関の職員に対して開示する場合等が該当
c. 虐待、育児放棄又は家庭内暴力の被害者についての開示	■ 本人が開示に同意する場合、法令又は規則によって明示的に承認され、重大な危害を防止するために必要と判断される場合 ■ 虐待、育児放棄又は家庭内暴力の報告を受け取る権限を法律によって認められている政府機関に対して開示する場合
d. 保健監督活動のため	■ 監査、民事事件、行政事件又は刑事事件の調査、検査、免許下付、懲戒の処分、手続、措置、保険医療システム等に対する適切な監督に必要なその他の活動を含め、法律によって承認される監督活動のために、保健監督機関に対して開示する場合
e. 司法及び行政の手続のため	■ 行政手続上必要な情報に限定 ■ 司法又は行政の手続の過程において保護対象情報を開示可能 ■ 例えば、裁判所又は行政審判所の命令に応じて開示する場合などが該当
f. 法執行を目的とする場合	■ 法執行の目的のために保護対象情報を法執行官に開示することが可能 ■ 例えば、容疑者、逃亡者、重要参考人、行方不明者を同定する又はその所在地を特定するために保護対象情報を求める法執行官の請求に応じて、情報を開示する場合などが該当

「公共の利益やベネフィットにつながる場合」は個人が合意もしくは反対を行う機会なく、PHIを使用又は開示することができる

公共の利益やベネフィットにつながる場合(§164.512)

項目	要件・概要
g. 故人について	■ 死亡者を同定し、死因を特定するため、又は法律によって認められている他の責務のため、検視官及び監察官に開示する場合 ■ 個人に関する葬儀業者の責務を実行するため、必要に応じて適用される法律に従い、葬儀業者に開示する場合
h. 死体の臓器、眼又は組織の献体	■ 臓器、眼又は組織の献体と移植の促進のために保護対象情報を使用する際に、対象事業者(CE)が死体の臓器、眼、細胞組織の調達やバンキングを行う業者に情報の使用と開示を行う場合
i. 研究目的	■ 非識別化情報を使用することができず、研究対象者の承認が求められると研究を実施できないケースで、研究対象者の承認の変更又は権利放棄がIRB又はプライバシー委員会によって認められている場合
J. 健康又は安全に対する深刻な脅威を回避するため	■ 被害者に重大な被害を与える可能性がある暴力的な犯罪への関与を述べている者を識別する必要がある場合 ■ 刑務所や合法的留置から逃亡したと思われる場合
k. 政府の専門的機能のため	■ 米国軍や退役軍人の活動に関する場合 ■ 安全保障や諜報機関の活動に必要な場合 ■ 大統領やその他の者の保護に必要な場合 ■ 医学的適合性の判断をする場合 ■ 刑務所や拘留時における本人及び担当者等の健康管理に必要な場合 ■ 政府機関が公共の利益につながる計画を実行する場合
l. 労災補償のため	■ 職業に関連した、過失によらない怪我や疾病に対する補償について、保険者、行政、雇用者、その他労災補償の制度に関与する者に開示する場合 ■ 労災や他の関連法を遵守するのに必要な範囲で開示

運用の仕組み

各CEは組織のPHIの管理を監視するCompliance officerを設置しなければならず、政府監督機関であるOCRが調査や監査を実施している

法の適切な運用を確保するための仕組み

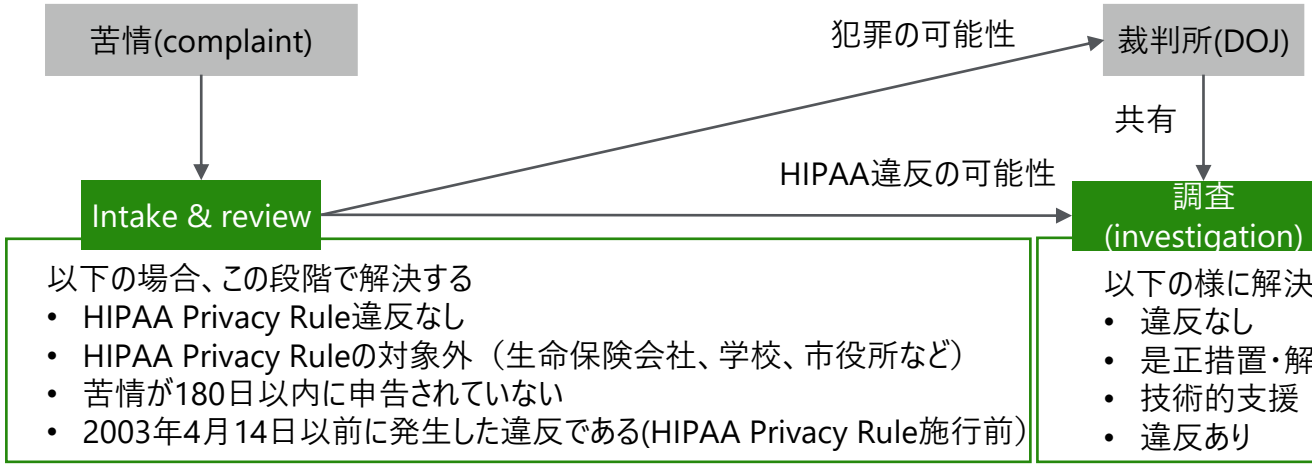
<table>
<tr><th></th><th>OCR</th><th colspan="2">Compliance officer</th></tr>
<tr><td>根拠法令等</td><td>Code of Federal Regulations(CFR)</td><td colspan="2">HIPAA</td></tr>
<tr><td>選任主体</td><td>HHS</td><td colspan="2">CE, BA</td></tr>
<tr><td>役割の範囲</td><td rowspan="2">■ 個人情報取扱い企業や団体の管轄
■ HIPAA Privacy RuleとHIPAA Security Rule施行の責任
■ 医療分野のみならず、市民の権利、信教の自由などの権利遵守の保証
■ 苦情の調査・処理
■ CEのコンプライアンスレビューの実施
■ 準拠性監査の実施
➢ CEやBAが違反報告ルール、HIPAA Privacy Rule、HIPAA Security Ruleに準拠しているか
➢ 苦情調査やコンプライアンスレビュー等の施行活動(enforcement activities)では明らかにされなかったリスクと脆弱性を発見する
➢ 2016-2017年にOCRは、166のCEと、41のBAに監査を実施した</td><td colspan="2">■ HIPAAの要件と手続に関連するすべての監督責任
■ 組織のPrivacy PolicyとPHIのセキュリティーを監督
■ コンプライアンスの確保と日常的モニタリング
■ Security officerとPrivacy officerは兼任することも可能
■ 求められる資質
1.組織力・分析能力・注意力・問題解決能力・協調性
2.医療分野での4年生学位取得
3.PHI保護のための医療法等に精通していること</td></tr>
<tr><td></td><td>Privacy officer
§ 164.530(a)(1)</td><td>Security officer
§ 164.308(a)(2)</td></tr>
<tr><td></td><td></td><td>■ HIPAAに準拠したPrivacy Programの開発と実施の責任
➢ PHI保護プログラムの実施
➢ HIPAAポリシーに関する従業員研修の実施
➢ HIPAA違反を、影響を受ける個人や機関の長(the Secretary)、場合によりメディアに報告
➢ リスクアセスメントの実施</td><td>■ Privacy officerと同様の役割を果たすが、組織的・技術的・物理的保護措置の遵守に焦点を当てる
➢ PHIを保護するための技術実装
➢ 全社的災害復旧計画の策定
➢ PHIの不正アクセス防止</td></tr>
</table>

出所：https://www.hhs.gov/ocr/about-us/index.html
https://www.hipaajournal.com/duties-of-a-hipaa-compliance-officer/
https://www.foxgrp.com/hipaa-compliance/hipaa-compliance-officer-the-role-and-purpose/
https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf
https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

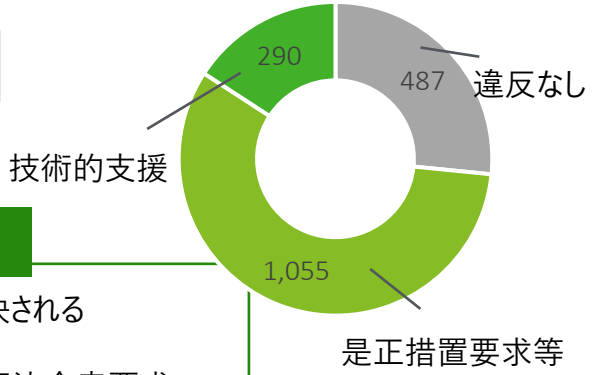
OCRは寄せられた苦情やコンプライアンスレビューにより調査を行い、HIPAA違反の有無を判断する

OCRによるレビューや調査の流れと制裁金

OCRによる苦情調査やコンプライアンスレビューにより、罰金が課されるか否かが決定される
2019年にOCRが対処した苦情は29,853件、コンプライアンスレビューは338件であり、うち19,589件はintake & reviewの段階で解決し、1,832件が調査まで進んだ



2019年調査結果内訳　合計：1,832件



制裁金の定め

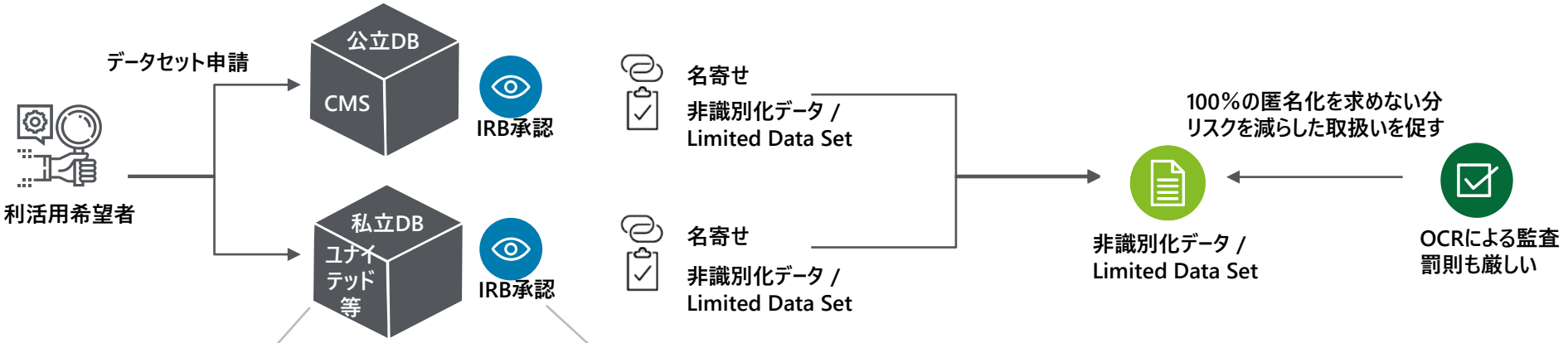
- ■ ①違反している自覚が無かった場合: 最低額USD100-最高額USD50,000, 同一規定内で違反した場合の年間罰金最高額USD25,000
- ■ ②合理的理由による違反の場合: 最低額USD1,000-最高額USD50,000, 同一規定内で違反した場合の年間罰金最高額USD100,000
- ■ ③故意による違反の場合(是正有): 最低額USD10,000-USD50,000, 同一規定内で違反した場合の年間罰金最高額USD250,000
- ■ ④故意による違反の場合(是正無): 最低額・最高額USD50,000, 同一規定内で違反した場合の年間罰金最高額USD1,500,000
- ■ 実際の罰金事例
  - ➢ 2018年10月、米国最大の健康保険会社は2016年に一連のサイバー攻撃を受けたことにより7,900万人のePHI情報を流出させ、USD1,600万を支払った。悪意のあるメールが原因で、名前、社会保障番号、医療識別番号、住所、生年月日、メールアドレス等の情報が流出した

出所：https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2015-2016-2017.pdf
https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html
https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html

米国では、二次利用に関して数千万人規模の医療DBが複数存在し、名寄せ等の加工をしたのち非識別化データとして提供することで情報保護を行っているケースが多い

米国の医療情報二次利用の主要パターン

米国の医療情報利活用関連基本ルール
・一次利用：本人の同意も承認(書面必要)も必要なし　【HIPAA】
・二次利用：本人の承認か、HIPAA Privacy Ruleに収載されている内容(BAへの提供など)が必要　【HIPAA】
・二次利用その他：本人の承認が事実上不可能なケースなど一定基準のもと、IRBが承認すれば個人情報の活用は可能　【HIPAA】



CMSが保有するMedicareデータ及びMedicaidデータは、データ統合ができること、データベースの規模が大きい（人口の3割程度）ことなど、有用な点が多い

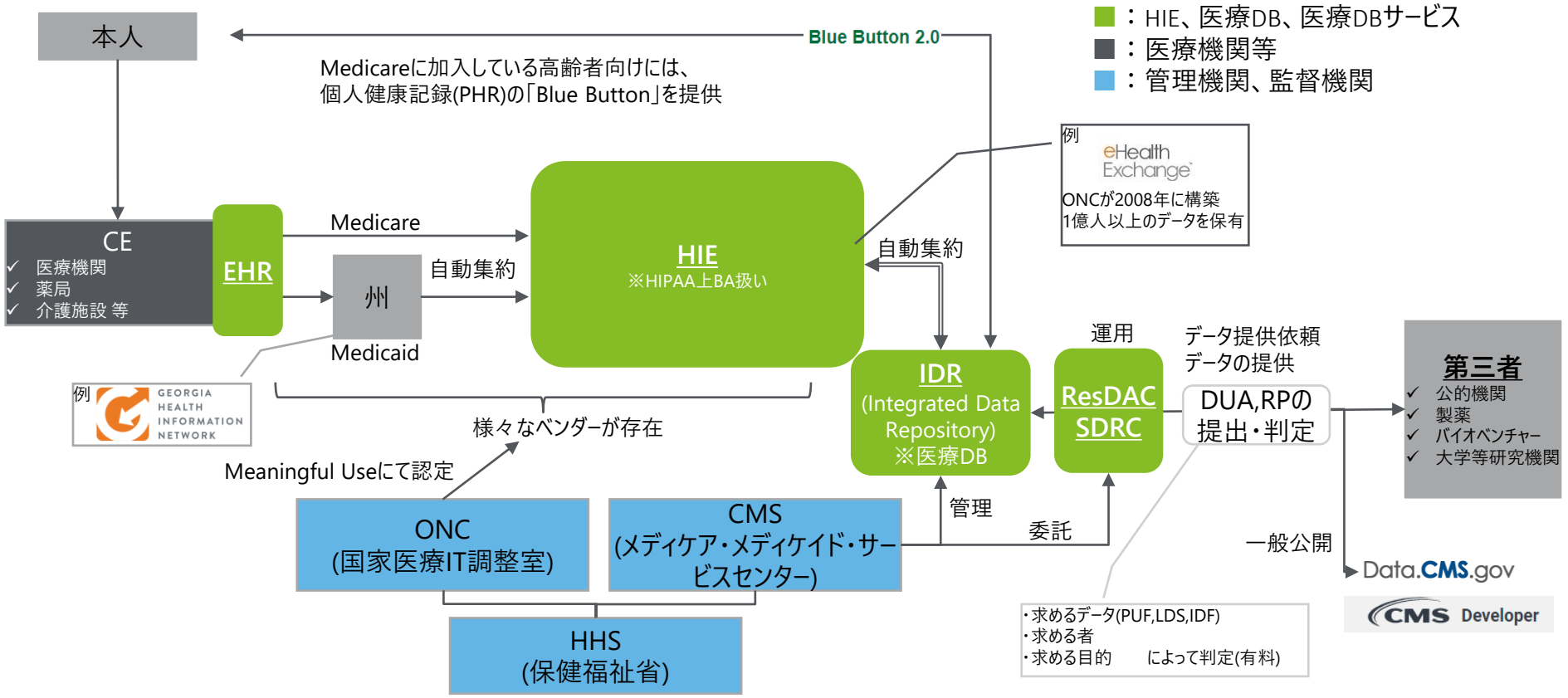
Medicare, Medicaid データの概要

項目	内容		
管理者・運営者	管理者はCMS(メディケア・メディケイド・サービスセンター)、運営はResDAC（ミネソタ大学）、SDRC（Econometrica Inc.）に委託		
規模	Medicare：56.8 百万人（2016）、Medicaid：66.6 百万人（2018）		
保有データ	Medicare	標準分析ファイル（SAFs） ※レセプトベース	外来の場合の治療日・入退院日、誕生日（年齢）、人種、性別、診断名（ICD-10）、治療内容（ICD-10）、治療内容に対する支出、治療を受けた医療施設ID、治療を受けた医師のUPI（Unique Physician Identifier）、主治医のUPI 等
		医療供給者分析ファイル（MedPAR） ※入院日から退院日までの在院日数ベース	
	Medicaid	患者サマリファイル（Personal Summary file）	生年月日、性別、人種、郵便番号、Medicaid入会日、managed care plan加入時期
		入院患者ファイル（Inpatient file）	医療施設ID、入退院日、転帰、診断名（9個まで、ICD-9-CM）、治療（6個まで、ICD-9-CM）、入院費用
		処方箋ファイル（Prescription Drug file）	処方箋コード（NDC）：製造販売業者、力価、剤型、処方量 等
		長期治療ファイル（Long Term Care file）	長期治療記録：施設規模、医療サービス提供日、診断、転帰 等
		その他の治療ファイル（Other Therapy file）	入院を除く医療サービスの記録・診療、臨床検査、放射線検査（検査記録は、実施日・検査項目のみであり、結果データは得られない）
	これらのデータを統合し、PUF（Public Use Files）， LDS（Limited Data Set）， IDF（Identifiable Data Files）の3種類のデータセットを作成		
データ利用可能者	IDFの申請は個人では行えない。主体者と目的によって開示されるデータセットが異なる。IDFが申請された場合CMSプライバシー委員会が審査する		
利用可能データ	データは有料で、ResDAC（Research Data Assistance Center※ミネソタ大学内に設置された機関)がサポートを行う 州が活用する場合は無料であり、SDRC（State Data Resource Center)がサポートする。活用できるデータは以下の通り ①Public Use Files（非識別情報） →比較的安価。購入者に対する規制や契約事項の設定なし ②Limited Data Set File（リミテッドデータセット） →申請者は、契約文書（DUA）及び research protocolを提出しなければならない →審査時間は比較的短い ③Identifiable Data Files（患者識別番号が付与されたデータ） →申請者は、DUA及びさらに詳細なresearch protocolを提出しなければならない →CMSによる1年前後の長期的な審査を経る必要がある →特定の利益団体と密接につながりのある研究機関・研究者には、データ提供されない（医薬品企業 等）		
その他特徴 問題点	• Medicare, Medicaidの両方の加入者のデータの統合が可能である • Social Security Number（社会保障番号）により、出生/死亡届、税金、年金等の行政データとのリンクも可能である • 保険の性質から母集団の一般性が低いとの指摘はある • 似た患者であっても、診療コードは異なる（消化管出血、吐血、下血 等）等の指摘はある（アウトカム抽出に際して、複数の診療コードに着目する必要がある） • ICD-9-CMの診断コードでは、詳細な調査ができない場合がある等の指摘がある		

出所：CMSホームページ、平成30年度厚生労働省「諸外国における健康・医療・介護分野のデータベースの現状調査」

公的保険を利用し、CMSが主にeHealth Exchangeを介して情報取得し、CMSが委託したResDACが申請主体や内容に応じて第三者に加工後の医療データを提供している

Medicare、Medicaidの医療情報の流れ



- eHealth Exchange(旧NHIN)
  - 2004年、HHSは医療ITの標準化や政策決定を統括する組織として、ONCを設置
  - ONCは、2008年に全米医療情報ネットワーク(NHIN：Nationwide Health Information Network)を構築、2012年より民間主体のSequoia Projectに移管され、名称をNHINからeHealth Exchangeに変更
  - 同ネットワークは病院、患者、薬局、政府機関、保険会社などの医療サービスのステークスホルダー個々に運営している医療ITシステムをつなげていくための全米規模のインフラ
  - eHealth Exchangeの利用状況は50州の4連邦機関、全米の約半数の病院、2万6千の医療グループ、8千3百の薬局等を接続し、一億人以上の患者のサポートをしている(2018年3月時点)
- Meaningful Use
  - ONCは医療ICTの普及とEHRの利用を促進するために、インセンティブ支払いプログラムを導入
  - EHR導入の際に、ONCが設定したシステム・モジュールに対する要件を満たした機器・システムを導入し、かつ一定の基準(この基準をMeaningful Useという)を満たすことでインセンティブをベンダーに提供
  - Meaningful Useの基準に準拠したEHR普及率は67%(2018年)

3.3.2 EU諸国共通の規制(GDPR)

医療情報の利活用に係る規則

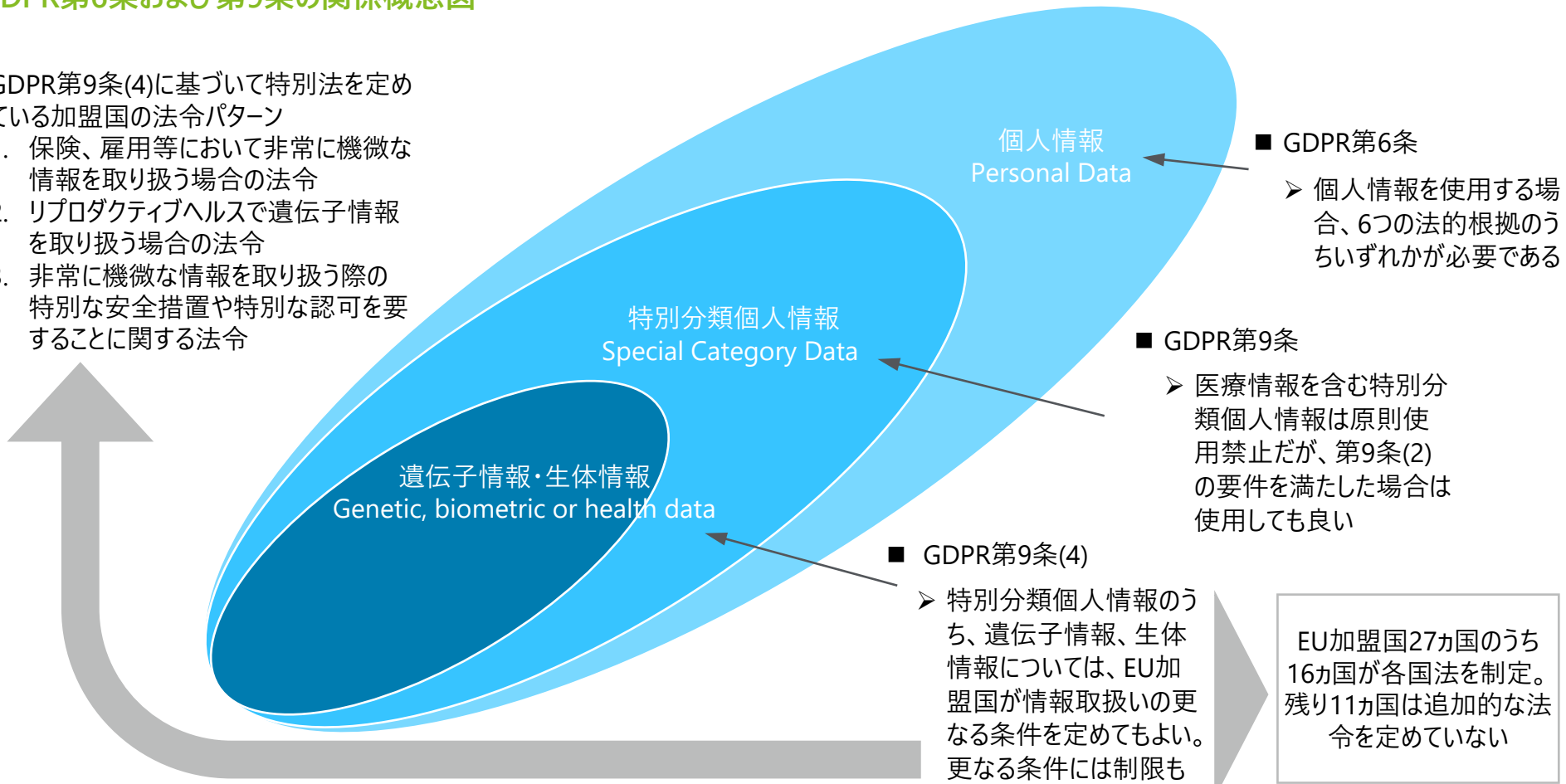
医療情報を取り扱う際には、GDPR第6条の個人情報の取扱いに係る法的根拠と、第9条の特別分類個人情報の取扱いに係る要件を共に満たす必要がある

GDPR第6条のどの法的根拠に基づいているか、またGDPR第9条で特別分類個人情報に含まれる医療情報の取扱いについてEU加盟国で追加的な国内法を定めているかにより、EU加盟国内でも取扱いに差が出る

GDPR第6条および第9条の関係概念図

GDPR第9条(4)に基づいて特別法を定めている加盟国の法令パターン

1. 保険、雇用等において非常に機微な情報を取り扱う場合の法令
2. リプロダクティブヘルスで遺伝子情報を取り扱う場合の法令
3. 非常に機微な情報を取り扱う際の特別な安全措置や特別な認可を要することに関する法令



■ GDPR第6条

- 個人情報を使用する場合、6つの法的根拠のうちいずれかが必要である

■ GDPR第9条

- 医療情報を含む特別分類個人情報は原則使用禁止だが、第9条(2)の要件を満たした場合は使用しても良い

■ GDPR第9条(4)

- 特別分類個人情報のうち、遺伝子情報、生体情報については、EU加盟国が情報取扱いの更なる条件を定めてもよい。更なる条件には制限も含まれる

EU加盟国27ヵ国のうち16ヵ国が各国法を制定。残り11ヵ国は追加的な法令を定めていない

 出所：https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

GDPR第6条では個人情報の処理が適法であるとする法的根拠(lawfulness)6つのいずれか一つを満たすことが求められる

GDPR第6条1項　適法性の確保(Lawfulness of processing)

- 6 つの法的根拠に優先順位をつけて選択するのではなく、最も適切な法的根拠 1 つに基づいて個人情報を取り扱う必要がある
- 「法的義務」と「公益の利益」は、EU法（Union law）又は情報管理者の加盟国の法律において、より詳細な要求事項を規定することができる

6要件	概要	EU法又は各国法で制定が必要
a. 同意の取得 Consent	■ 本人(データ主体)が、特定の目的のための個人データの取扱いに関し、明確な同意を与える	
b. 契約の履行 Contract	■ 本人(データ主体)が契約当事者となっている契約の履行のために取扱いが必要となる場合	
c. 法的義務 Legal obligation	■ 情報管理者が服する法的義務を遵守するため	○
d. 生命に関わる利益 Vital interest	■ 本人(データ主体)又は他の自然人の生命に関する利益を保護するため 【例】・感染症の拡大のモニタリング ・自然災害や人災における人道面での緊急事態における個人情報の取扱い	
e. 公共の利益 Public interest	■ 公共の利益又は管理者に与えられた公的な権限の行使において行われる職務の遂行のため	○
f. 正当な利益 Legitimate interest	■ 管理者又は第三者によって求められる正当な利益となる目的のため	

出所：https://gdpr-info.eu/art-6-gdpr/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

GDPR6条第1項の(C)Legal Obligationと(e)Legitimate Interestは、EU加盟国の各国法において活動内容を規定している場合に使用できる法的根拠である

GDPR第6条2項

■ 条文　和訳

加盟国は、第 1 項(c)及び(e)を遵守する取扱いに関し、第 9 章に定めるその他の特別の取扱いの状況に関す る場合を含め、適法かつ公正な取扱いを確保するため、取扱いのためのより詳細で細目的な要件及びその他の 措置を定めることによって、本規則の規定の適用を調整するためのより細目的な条項を維持し、又は、これを 導入できる。

■ 補足説明

各加盟国の「個人情報保護法制」で第1項(c)から(e)をより詳細化する規定をおいて良い、とするものである

【例】
例えば第1項(c)のLegal obligationの場合、以下のような各加盟国の個人情報保護法制における定義規定となる

- どれぐらいの義務があれば”Legal obligation”になるのか
- 刑事罰を伴う義務なのか
- 各業法で行える業務に入っている程度で良いのか

GDPR第6条3項

■ 条文　和訳

第1 項(c)及び(e)に定める取扱いのための根拠は、以下によって定められる：
(a) EU 法。又は、
(b) 管理者が服する加盟国の国内法。
取扱いの目的は、その法的根拠に従って決定され、又は、第1 項(e)に定める取扱いに関しては、公共の利益に おいて、若しくは、管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要なものと する。その法的根拠は、本規則の規定の適用を調整するための特別の条項を含みうる。特に、管理者による取 扱いの適法性を規律する一般的な条件、取扱いの対象となるデータの種類、関係するデータ主体、個人データ が開示されうる組織及びその目的、目的の限定、記録保存期間、並びに、第9 章中に定めるその他の特別の取 扱いの状況のための措置のような適法かつ公正な取扱いを確保するための措置を含めた取扱業務及び取扱手続を含めることができる。EU 法又は加盟国の国内法は、公共の利益の目的に適合するものであり、かつ、そ の求める正当な目的と比例的なものとする。

■ 補足説明

各加盟国の、個人情報取扱いが必要となる活動の根拠法令

【例】　例えば診療なら日本の医療法や医師法相当の法令であり、その活動をEU法か加盟国国内法できちんと規定していなければ、第1項(c)から(e)の根拠として使用できない

出所: https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

GDPR第9条では人種や宗教、遺伝子情報、健康データ等の特別分類個人情報の取扱いは禁止であるとした上で、この法令の適用除外の要件を定めている

GDPR 第9条 特別分類個人情報と適用除外

特別分類個人情報 (第9条第1項)

- 人種・民族の出自
- 政治的な意見
- 宗教・思想上の信条
- 労働組合への加入
- 遺伝子データ
- 生体データ
- 健康データ
- 性生活・性的指向

適用除外（第9条第2項）	概要
a. 明確な同意がある Explicit consent	データ主体が、一つ又は複数の特定された目的のためのその個人データの取扱いに関し、明確な同意を与えた場合
b. 労務、社会保障及び社会援助 Employment, social security and social protection	EU 法若しくは加盟国の国内法により認められている範囲内、又は加盟国の国内法による団体協約によって認められる範囲内で、雇用及び社会保障並びに社会的保護の法律の分野における管理者又はデータ主体の義務を履行する目的のためである場合
c. 本人の生命に関わる利益 vital interest	データ主体が物理的又は法的に同意を与えることができない場合で、データ主体又はその他の自然人の生命に関する利益を保護するために取扱いが必要となるとき
d. 非営利団体の構成員及び密接関係者関連の活動 NPO	その組織の構成員若しくは元構成員、又は、その組織の目的と関係してその組織と継続的に接触をもつ者のみに関するものであることを条件とし、かつ、データ主体の同意なくその個人データが当該組織の外部に開示されないことを条件とする場合
e. 本人による公表済みの情報である Made public by the data subject	データ主体によって明白に公開のものとされた個人データに関する取扱いの場合
f. 法的請求及び司法関連の行為 Legal claims and judicial acts	訴えの提起若しくは攻撃防御のため、又は、裁判所がその司法上の権能を行使する際に取扱いが必要となる場合
g. 重要な公益目的である Task carried out in the public interest	EU 法又は加盟国の国内法に基づき、求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、重要な公共の利益を理由とする取扱いが必要となる場合
h. 医療関係 Health and social care	EU 法又は加盟国の国内法に基づき、又は、医療専門家との契約により、予防医学若しくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の診断、医療若しくは社会福祉又は治療の提供、又は医療制度若しくは社会福祉制度及びそのサービス提供の管理のために取扱いが必要となる場合
i. 公衆衛生 Public health	EU 法又は加盟国の国内法に基づき、健康に対する国境を越える重大な脅威から保護すること、又は、医療及び医薬品若しくは医療機器の高い水準の品質及び安全性を確保することのような、公衆衛生の分野において、公共の利益を理由とする取扱いが必要となる場合
j. 研究活動 Research	EU 法又は加盟国の国内法に基づき、第 89 条第 1 項に従い、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取扱いが必要となる場合

特別分類個人情報に含まれる遺伝子データ、生体データ、健康データの取扱いを認めるため、国内法で公益目的、医療介護、公衆衛生、研究活動の内容や要件を定めている

英国 DPA 2018

GDPR 第9条第2項	国内法	特別分類個人情報の取扱いに関する要件
g. 重要な公益目的	Schedule 1, Part 2, Section 5～28	別段の定めがある場合を除き、本附則のこの部の条件が満たされるのは、データ管理者が適切なポリシー文書を所定の場所に有している場合に限られる （詳細は本報告書3.3.3英国で後述）
h. 医療介護	Schedule 1, Part 1, Section 2	(a)予防医学や職業医学 (b)従業員の労働能力評価 (c)医学的診断 (d)医療や治療の提供 (e)社会的ケアの提供 (f)医療介護制度やサービスの管理
i. 公衆衛生	Schedule 1, Part 1, Section 3	公衆衛生の分野における公衆の利益のために必要であり、以下の状態で行う場合 (i)医療専門家または、医療専門家の責任下で実施 (ii)法律または規則の下で守秘義務を負う者によって実施
j. 研究活動	Schedule 1, Part 1, Section 4	(a)アーカイブ目的、科学的もしくは歴史的研究目的または統計目的のために必要である場合 (b)GDPR第89条 (1) (第19条で補足)に従って実施されており、かつ、公共の利益になる場合

出所：https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/1/enacted
https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/2/enacted

特別分類個人情報に含まれる遺伝子データ、生体データ、健康データの取扱いを認めるため、国内法で公益目的、医療介護、公衆衛生、研究活動の内容や要件を定めている

エストニア　PDPA

GDPR 第9条第2項	国内法	特別分類個人情報の取扱いに関する要件
g. 重要な公益目的	PDPA 第1章 Article 7	（PDPAやHealth Service Organization Actにおいて公益目的が指す具体的な内容の記載はない） (1) 公共の利益におけるアーカイビングの目的のために個人データが取り扱われる場合、管理者又は処理者は、欧州議会及び理事会の規則 (EU) 2016/679の第15条、第16条及び第18条の21に規定するデータ主体の権利の行使が、公共の利益におけるアーカイビングの目的の達成を不可能にする可能性が高いか又は著しく阻害する可能性がある場合に限り、これらの権利を制限することができる (2) (1) に規定するデータ主体の権利は、記録の状態、真正性、信頼性、完全性及び利用可能性を損なわないように制限することができる
h. 医療介護 i. 公衆衛生	Health Service Organization Act Article 59	ENHISは、国の情報システムに属するデータベースであり、保健サービスの提供、保健サービスの質と患者の権利の保証、公衆衛生の保護 (健康状態に関する登録簿の維持、保健統計の編成、保健管理を含む) のための契約の締結と履行のために、保健医療情報を処理する
j. 研究活動	PDPA 第2章 Article 6	科学的及び歴史的研究又は公的統計を必要とするデータ主体に関するデータを、データ主体の同意を得ることなく、次の条件が満たされる場合に限り、データ主体を特定できる形式で処理することが認められる 1) 識別を可能にするデータの除去後にデータ処理の目的を達成することができなくなった場合、またはこれらの目的を達成することが不当に困難になる場合 2) 科学的及び歴史的研究を行う者の評価又は公式の統計を作成することについて、公衆の最大の関心がある 3) 処理された個人データに基づいてデータ主体の義務の範囲が変更されたり、その他の方法でデータ主体の権利が過度に損なわれることがない

特別分類個人情報に含まれる遺伝子データ、生体データ、健康データの取扱いを認めるため、国内法で公益目的、医療介護、公衆衛生、研究活動の内容や要件を定めている

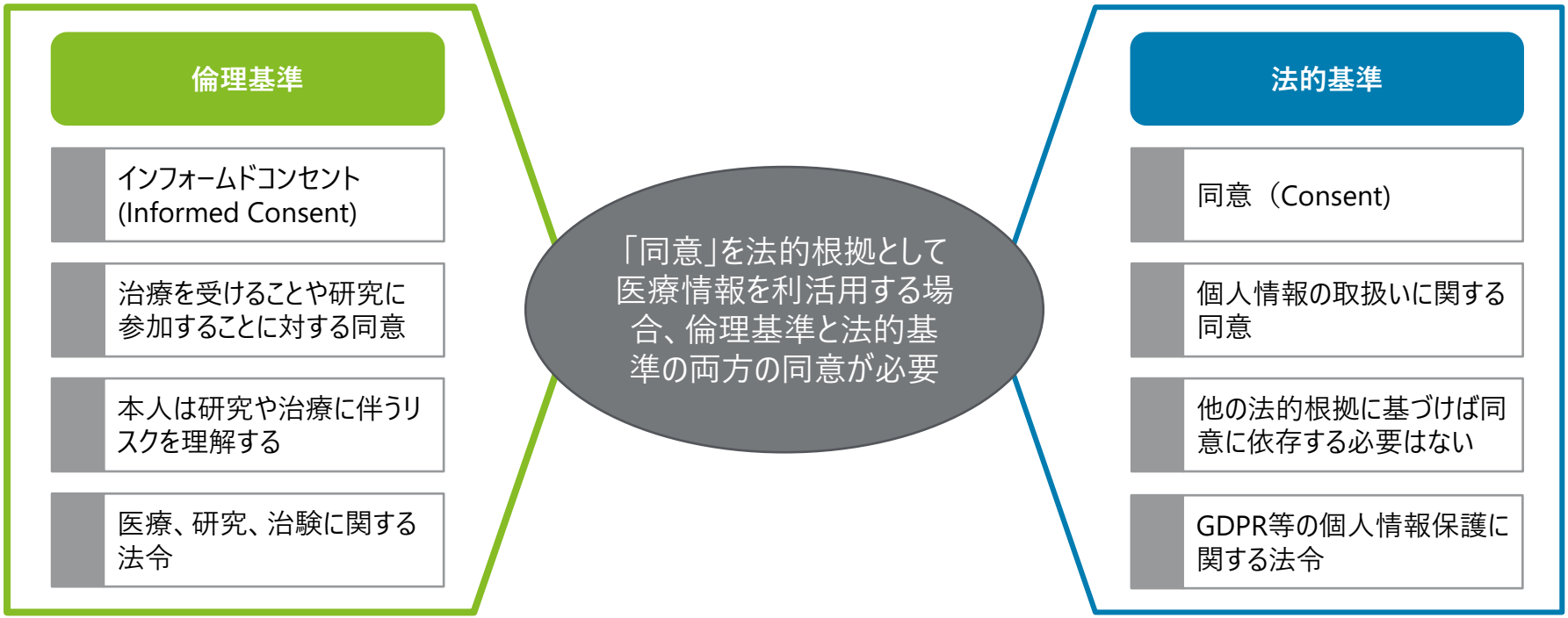
オランダ Dutch GDPR Implementation Act

GDPR 第9条第2項	国内法	特別分類個人情報の取扱いに関する要件
g. 重要な公益目的	Dutch GDPR Implementation Act Article 28, 29, 30	• 遺伝子情報の取扱いが公益目的に資する研究のためである場合 • 生体データの取扱いが認証(authentication)や安全管理目的である場合 • 学校において生徒の健康状態に関連した特別な目的のための処理 • 保護観察所や児童保護理事会、青少年法に定められた認定施設等が、任務を遂行する場合
h. 医療介護	Dutch GDPR Implementation Act Article 30	• 医療サービス提供者、医療機関、社会福祉サービスにおいて、適切なケアを提供する目的であり、また、専門業務の実施や施設運営に携わる場合 • 金融サービス提供者が保険業務に携わる場合
i. 公衆衛生	-	-（公益目的に含まれていると考えられる）
j. 研究活動	Dutch GDPR Implementation Act Article 24	• GDPR第89条の保護措置等をとった上で、科学的・歴史的研究または統計目的でデータの処理が必要な場合 • 公共の利益のための調査である場合 • 明示的な許可を求めることが不可能または過度な負担がかかる場合 • 個人のプライバシーを不均衡に侵害することのないように規定が定められている場合

【同意】診療目的で収集した医療情報を研究目的や公益目的等で二次利用する場合の法的基準の同意について、GDPRや各国法を整理した

「同意」の前提

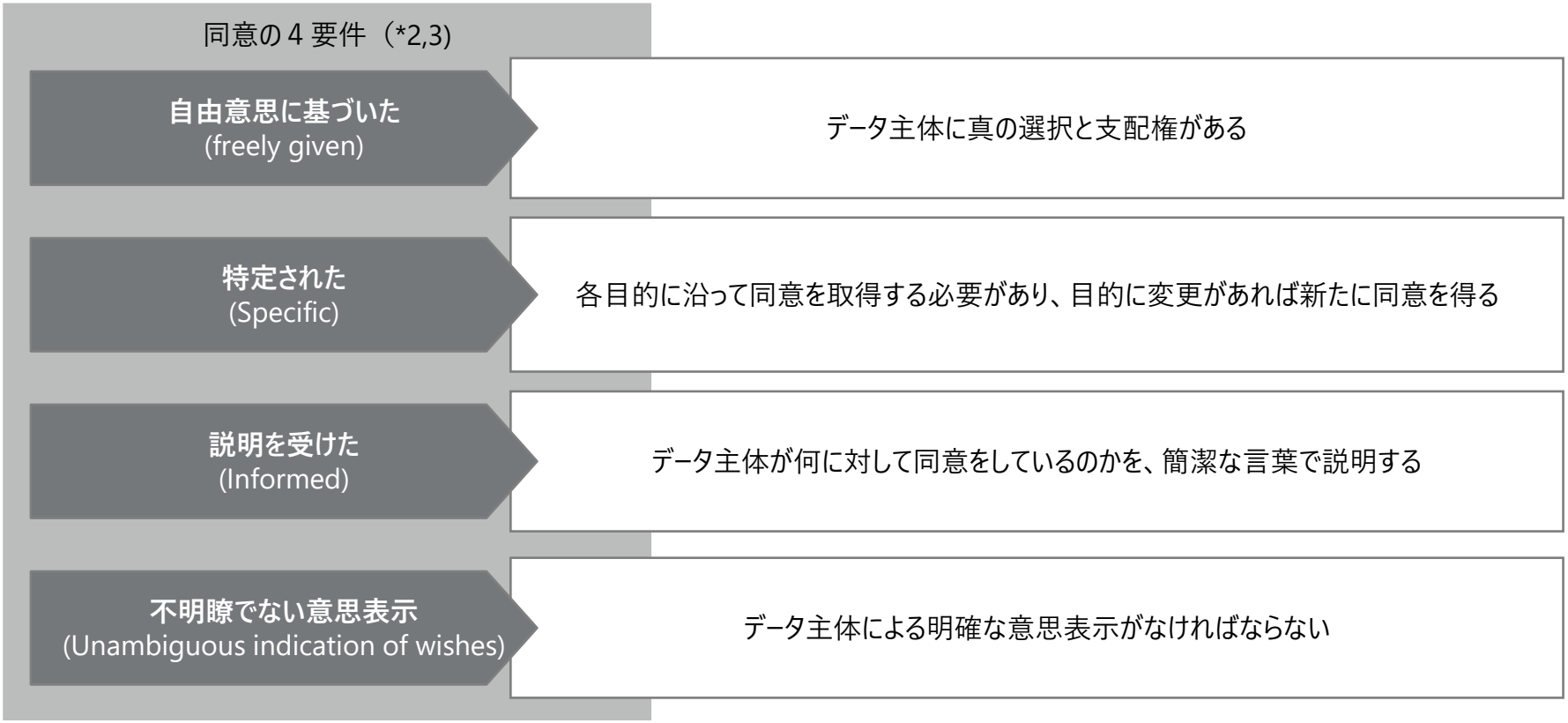
- 医療情報の取扱いに関する「同意」には、「倫理基準に基づいた同意(インフォームドコンセント)」と、「個人情報の取扱いに関する同意」がある
- GDPRで定めている「同意」は「個人情報の取扱いに関する法的基準の同意」であり、医療機関がこの同意を法的根拠として医療情報を利活用する場合は、倫理基準に基づいたインフォームドコンセントとは分けてそれぞれの同意を取得する必要がある



【同意】有効な「データ主体の同意」とは、同意の自由が与えられ、特定の目的や利用されるデータに関する説明があり、データ主体の明確な意思表示である必要がある

同意の定義及び要件(GDPR第4条第11項)

consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; (*1)



出所：*1 https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm
*2 一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関するガイドライン
*3 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

【同意】有効な同意を得るための条件として、データ主体の同意を証明できるようにすること、またデータ主体が同意をいつでも撤回する権利が与えられていることが必要である

同意の条件(GDPR第7条)

同意の条件

同意を得ていることの証明 (Demonstrate the consent)	■ 取扱いが同意に基づく場合、データ管理者は、データ主体がその個人データの取扱いに同意したことを証明することができるものとする
明確な区別 (Clearly distinguishable)	■ データ主体の同意が、他の事項にも関係する宣言文書の文脈において与えられる場合には、他の事項と明確に区別可能な方法で行う ■ 同意の要請は明瞭かつ平易な文言を用いて、理解しやすく、容易にアクセスできる形で提示されなければならない
同意の撤回 (Withdrawal of consent)	■ データ主体はいつでも同意を撤回することができる ■ 撤回前の同意に基づく取扱いの適法性に影響を及ぼさない ■ 同意の取得時に、データ主体に同意が撤回できる旨を通知する ■ 同意の取得時と同様に容易な方法を提供しなければならない
本人の自由意思か否かの評価 (Assessment)	■ 同意が自由意思に基づいて与えられるか否かを評価する際には、当該契約の履行に必要でない個人データの取扱いに対する同意を条件としていないか最大限の考慮が払われなければならない（特に、サービスの提供を含む契約の履行の場合）

出所： https://gdpr-info.eu/art-7-gdpr/

【仮名化】データ主体の同意に基づかずに目的外利用をする場合に、暗号化や仮名化の手段の有無を考慮することとし、行動規範の一例にも仮名化を挙げている

GDPRでの仮名化(Pseudonymisation)の取扱い

Article	タイトル	概要
第6条 第4項	データ処理の法的根拠	個人情報を収集した目的以外の目的のための取扱いが、データ主体の同意に基づくものでない場合、または、第23条 (1) で示す国家安全保障、防衛等の目的のEU法若しくは加盟国の国内法に基づくものでない場合、データ管理者は、次の事項を考慮する a. 個人データが収集された目的と意図された追加的取扱いの目的との間の関連 b. 個人データが収集された状況、特にデータ主体と管理者との関係 c. 個人データの性質、特に、第9条に従って特別分類個人情報が取り扱われるか否か、又は第10条に従って有罪判決及び犯罪に関連する個人データが取り扱われるか否か d. データ主体に対する意図された追加的取扱いの起こり得る結果 e. 暗号化や仮名化を含む適切な保護手段の存在
第40条	行動規範	管理者又は処理者のカテゴリーを代表する団体及びその他の団体は、本規則(GDPR)の適用を特定する目的で、以下に関するような行動規範を作成し、又は修正若しくは拡張することができる • 公正・透明な処理 • 特定の状況において管理者が追求する正当な利益 • 個人データの収集 • 個人データの仮名化 • 公衆及びデータ主体に提供される情報 • データ主体の権利の行使 • 児童に提供される情報、児童の保護及び児童の親権者の同意の取得方法 • 第24条及び第25条に規定する措置及び手続並びに第32条に規定する取扱いの安全性を確保するための措置 • 監督機関への個人データ侵害の通知及びそのような個人データ侵害のデータ主体への伝達 • 第三国又は国際機関への個人データの移転 • 第77条及び第79条に基づくデータ主体の権利を侵害することなく、取扱いに関する管理者とデータ主体との間の紛争を解決するための裁判外手続及びその他の紛争解決手続

出所：https://gdpr-info.eu/art-6-gdpr/、https://gdpr-info.eu/art-40-gdpr/

【仮名化】GDPRでは仮名化はデータ主体のプライバシー侵害のリスクを軽減し個人情報保護にも有用であるとしている。またデータ管理者が速やかに仮名化を行うことも推奨している

GDPRの前文での仮名化の取扱い

前文	タイトル	概要
26	匿名化情報は適用外	■ GDPRは、匿名(anonymous)の情報、すなわち、識別可能な自然人に関連しない情報、またはデータ主体が識別不能または識別不能になるような方法で提供される匿名個人データには適用されるべきではない したがって、この規制は、統計または研究目的を含む、匿名情報の処理に関するものではない ■ 付加的な情報を使用することによって自然人に起因する可能性のある仮名化（pseudonymisation）された個人データは、識別可能な自然人に関する情報であると考えるべきである
28	仮名化の導入	■ 個人情報の仮名化は本人に対するリスクを軽減し、管理者が情報保護義務を果たす上で役立つ ■ GDPRでの仮名化についての明示が情報保護に関する他の手段を除外するわけではない
29	同一のデータ管理者内での仮名化	■ データ管理者が、個人データを特定のデータ主体に帰属させるための追加情報を別個に保持するために必要な技術的及び組織的措置を講じている場合には、同一の管理者内で仮名化の措置が可能である
78	適切な技術的・組織的な措置	■ GDPRの遵守を実証できるよう、データ管理者は内部方針を策定し、以下のような措置をとるべきである • 個人データの取扱いを最小化する • できる限り速やかに個人データの仮名化を行う • 個人データの機能及び取扱いに関する透明性を確保する • データ主体がデータの取扱いを監視することを可能にする • 管理者がセキュリティ機能を作成し、改善することを可能にする
156	保管、科学的・歴史的研究及び統計目的での処理	■ 公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のための個人データの追加的な取扱いは、適切な保護措置が存在することを条件として、管理者が、データ主体の特定を許可しない又はもはや許可しないデータを取り扱うことにより、これらの目的を達成する可能性を評価した場合に行われる(例えばデータの仮名化)など

GDPR第89条は公共の利益のためのデータ保管や研究・統計目的でのデータ処理におけるデータ主体の保護を求める一方、個人の権利の行使制限を定めることも認めている

GDPR 第89条

1.) 公共の利益における保管の目的、科学的研究・歴史的研究の目的又は統計の目的のための取扱いは、
- 本規則(GDPR)に基づき、データ主体の権利及び自由のための適切な保護措置によるものとする
- これらの保護措置は、データ最小化の原則の尊重を確保するために、特に技術的及び組織的な措置がとられていることを確保する
- これらの手段は、仮名化を含むことができる

2.) 以下の表に規定する権利が特定の目的を不可能にし、又は深刻に損なう恐れがある場合は、EU法又は加盟国の国内法で第1項に規定する条件及び保護措置に従って、これらの権利の例外を定めることができる（⇒権利の行使の制限を定めて良い）

GDPR	データ主体の権利または データ管理者の義務	英文	権利の行使の制限を定めて良い場合	
			科学的・歴史的研究 又は統計目的利用	公共の利益のための データ保管
第15条	データ主体が情報にアクセスする権利	Right of access by the data subject	○	○
第16条	データ主体が修正を要求する権利	Right to rectification	○	○
第18条	データ主体が利用を制限する権利	Rights to restriction of processing	○	○
第19条	データ管理者が修正、消去、制限をしたことをデータ主体に通知する義務	Notification obligation regarding rectification or erasure of personal data or restriction of processing		○
第20条	データポータビリティ	Right to data portability		○
第21条	異議を述べる権利	Right to object	○	○

【例】エストニアのPDPA第6条では「科学的及び歴史的研究又は公的統計の目的の場合、データ管理者はGDPR第15条,第16条,第18条,第21条の個人の権利の行使を制限することができる」と定めている。PDPA第7条でも公共の利益のためのデータ保管の場合の個人の権利の行使を制限している

注）GDPR第17条の消去の権利(「忘れられる権利」)の3項(d)でも、第89 条第1 項に従い、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的、又は、 統計の目的のためであれば、データ主体の消去権は適用されないとしている。ただし、消去権の適用除外は当該取扱いの目的を達成できないようにしてしまうおそれがある場合、又は、それを深刻に阻害するおそれがある場合に限る。

 出所： https://gdpr-info.eu/art-89-gdpr/

GDPR第9条に基づく特別分類個人情報を取り扱う場合、データ管理者及びデータ処理者はDPOを指名する必要があり、DPOはデータ主体や監督機関の連絡窓口となる

DPOの指名及び役割

DPOの指名（GDPR第37条）

データ管理者及びデータ処理者は、次のいずれかの場合には、DPOを指名する

- データ処理が公的機関又によって行われる場合。ただし、裁判所がその司法的資格で行う場合を除く
- データ管理者又はデータ処理者の中核的な活動が大規模なデータ主体の定期的かつ体系的な監視を必要とする取扱業務から成る場合
- データ管理者又はデータ処理者の中核的な活動が、第9条に基づく特別分類個人情報又は第10条に定める有罪判決及び犯罪に関連する個人データの大規模な取扱いから成る場合
- DPOは専門的な資質、特に、データ保護に関する法律及び慣行に関する専門知識並びに第39条に規定する任務を遂行する能力に基づいて指名される

DPOの位置づけ（GDPR第38条）

- データ管理者とデータ処理者は個人情報保護に関する問題については、適切かつ適時にDPOと協力する
- DPOは任務を遂行した結果、解雇や懲罰を課されるべきではない
- データ主体は個人情報の保護に関する問題や、個人の権利の執行についてDPOに連絡をとることが可能である

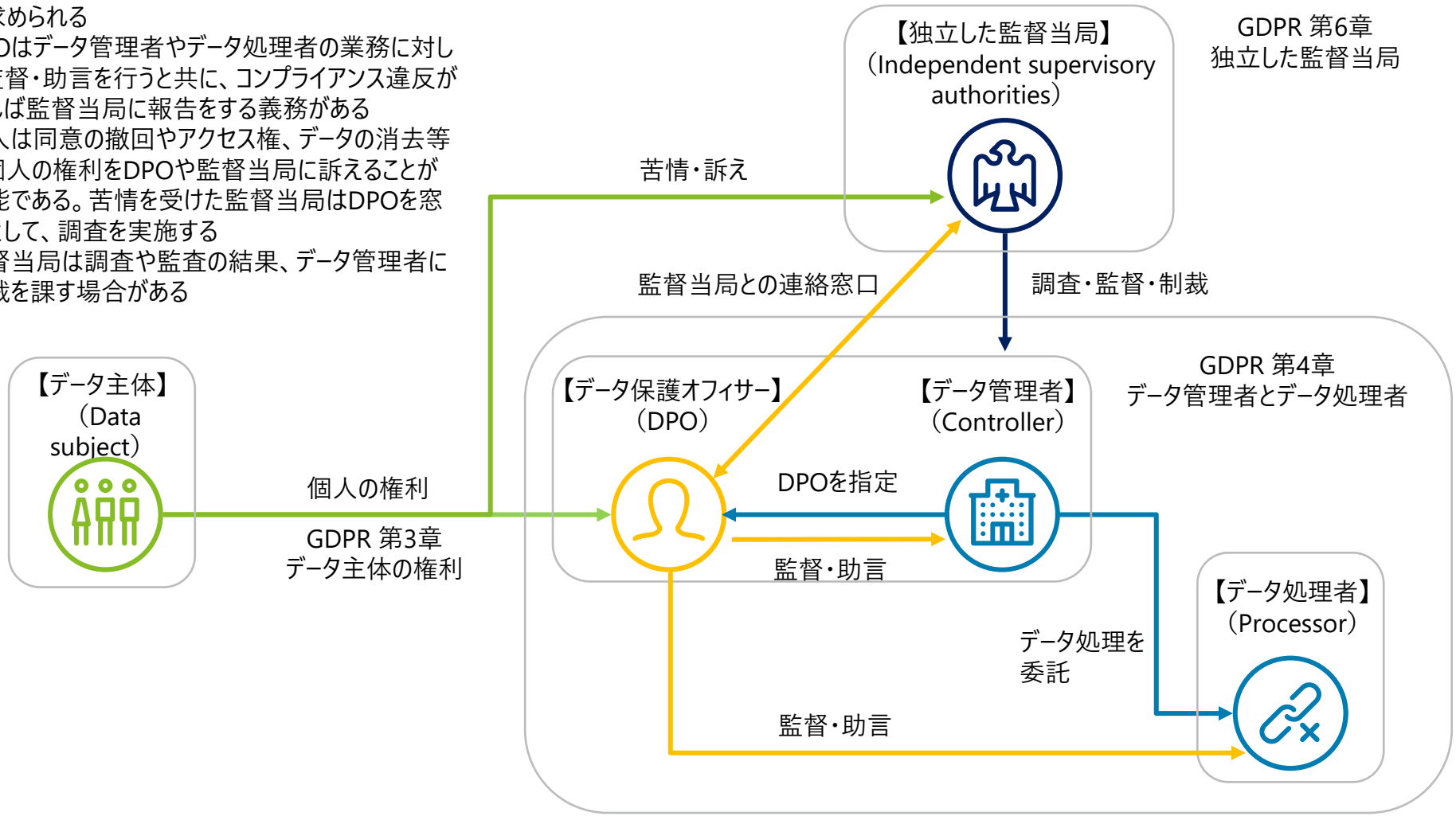
DPOの任務（GDPR第39条）

- データ管理者又は処理者及び本規則及び他のEU又は加盟国のデータ保護規定に従った義務を遂行する従業員への通知、助言を行う
- データ取扱作業に関与する職員の責任の割当て、意識向上及び訓練、監査を含め、データ管理者又はデータ処理者のコンプライアンスの遵守を監視する
- データ保護影響評価（Data protection impact assessment、GDPR第35条）に関する助言をし、その評価の実施を監視する
- 監督機関の連絡窓口として行動し、適宜、監督機関と協議すること

個人の権利、データ管理者とデータ処理者の義務、そしてそれらを監督する機関とDPOの役割を定めることにより個人及び医療情報を保護する体制を整備している

個人及び個人情報の保護の仕組み

① 医療情報を取り扱うデータ管理者はDPOの設置が求められる
② DPOはデータ管理者やデータ処理者の業務に対して監督・助言を行うと共に、コンプライアンス違反があれば監督当局に報告をする義務がある
③ 個人は同意の撤回やアクセス権、データの消去等の個人の権利をDPOや監督当局に訴えることが可能である。苦情を受けた監督当局はDPOを窓口として、調査を実施する
④ 監督当局は調査や監査の結果、データ管理者に制裁を課す場合がある

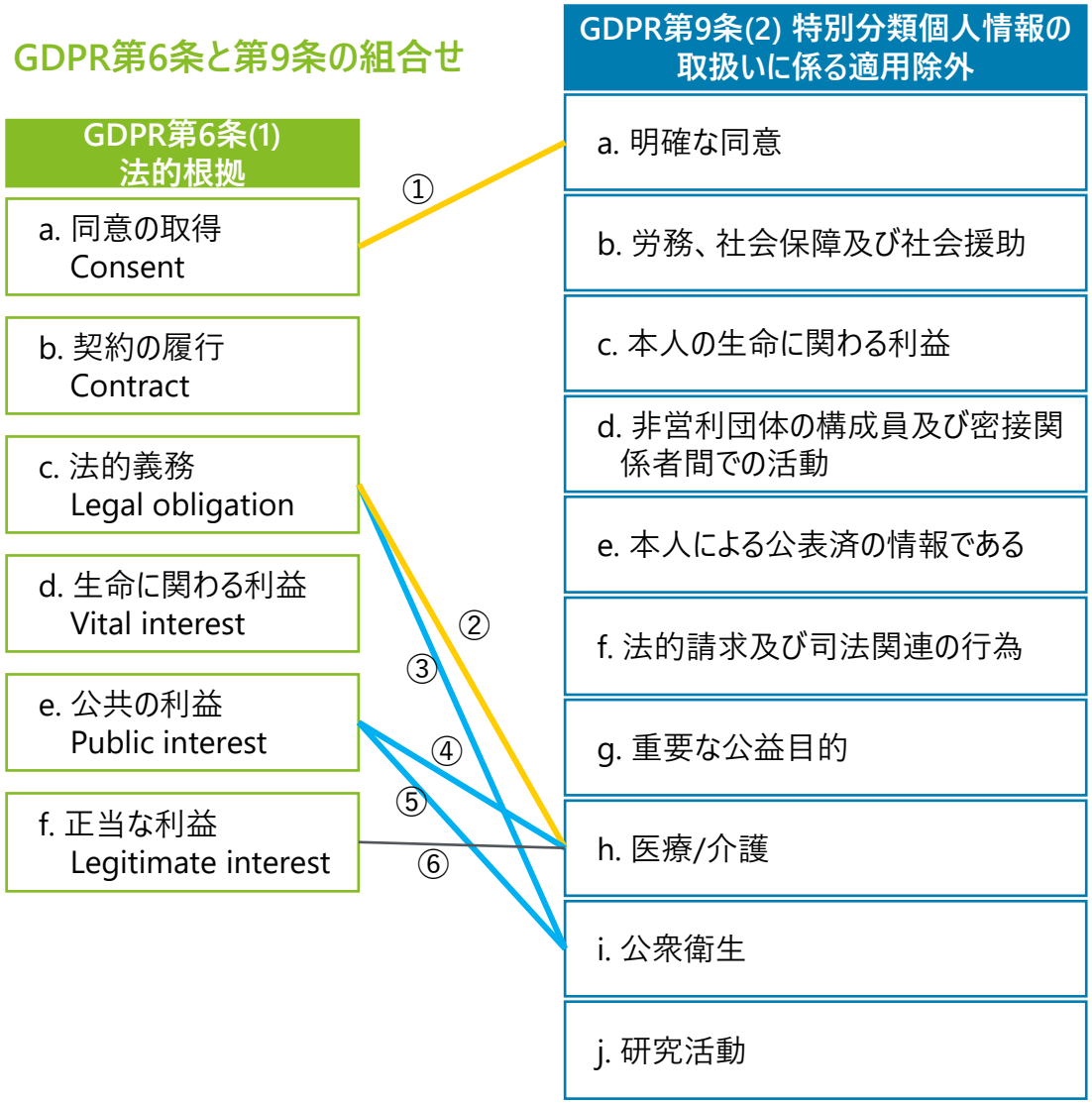


 出所：https://gdpr-info.eu/chapter-3/、https://gdpr-info.eu/chapter-4/、https://gdpr-info.eu/chapter-6/

EU加盟国におけるGDPRの運用実態

【EU調査報告】医療情報の取扱いにおいて、EU加盟国の国内法の基礎となったGDPR第6条(1)と第9条(2)の法的根拠の組合せは各国で異なっているという実態がある

GDPR第6条と第9条の組合せ



EU27加盟国が医療情報の取扱いについて国内法を定めた際の基礎としたGDPR第6条と第9条の組合せとその採用数

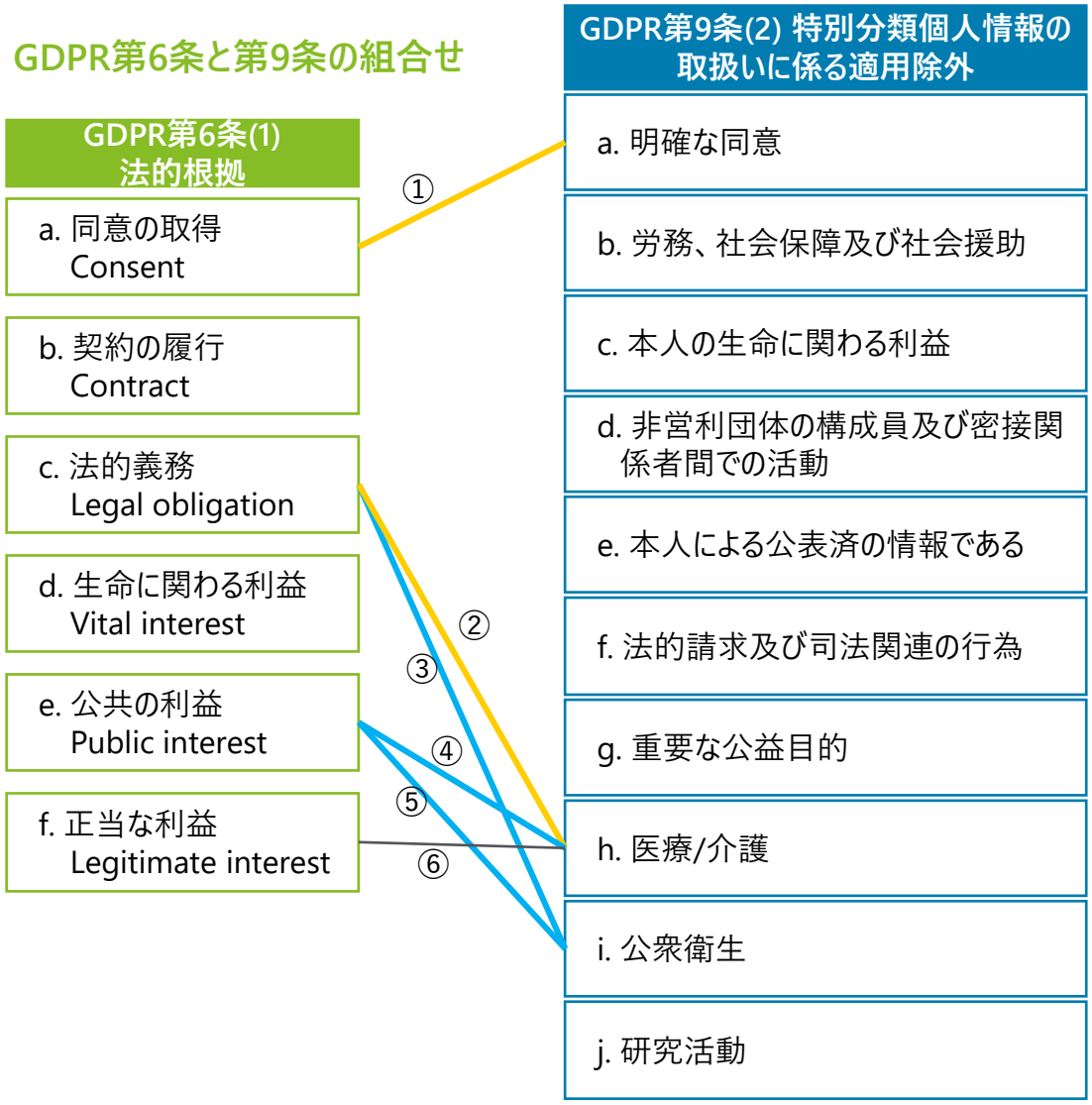
組合せ	一次利用			二次利用（公益目的）		
第6条の法的根拠＋第9条の例外要件	通常の治療	医療従事者間	アプリや機器の情報利用	医療体制整備	疾患登録	医療機器の安全性監督
① 6(1)a+9(2)a	12	17	18	NA	NA	NA
② 6(1)c+9(2)h	21	19	6	9	8	7
③ 6(1)c+9(2)i	9	7	3	16	18	15
④ 6(1)e+9(2)h	12	8	5	13	6	5
⑤ 6(1)e+9(2)i	8	7	1	12	17	6
⑥ 6(1)f+9(2)h	2	3	2	1	1	0
その他	6	4	2	6	5	7
該当する個別法なし	NA	NA	NA	3	3	9

注1) 1か国で複数の組合せを挙げている場合もある
注2) EU離脱をした英国は上記集計には含まれていない

 出所：https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

【EU調査報告】医療情報の取扱いにおいて、EU加盟国の国内法の基礎となったGDPR第6条(1)と第9条(2)の法的根拠の組合せは各国で異なっているという実態がある

GDPR第6条と第9条の組合せ



本調査対象国が医療情報の取扱いについて国内法を定めた際の基礎としたGDPR第6条と第9条の組合せ

組合せ	一次利用			二次利用（公益目的）		
第6条の法的根拠＋第9条の例外要件	通常の治療	医療従事者間	アプリや機器の情報利用	医療体制整備	疾患登録	医療機器の安全性監督
① 6(1)a+9(2)a		NL UK	NL			
② 6(1)c+9(2)h	NL					
③ 6(1)c+9(2)i		UK		NL	UK	
④ 6(1)e+9(2)h	EE UK	EE	EE UK	EE UK		EE
⑤ 6(1)e+9(2)i				EE UK NL	EE UK	EE
⑥ 6(1)f+9(2)h						
その他						
該当する個別法なし					NL	NL UK

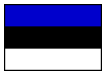
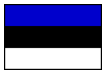
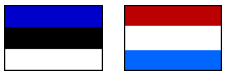
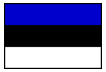
UK：英国　EE：エストニア　NL：オランダ

 出所：https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

【EU調査報告】治療目的で収集したデータを第三者機関に提供して研究をする場合のGDPR第9条第2項の法的根拠は、研究活動の内容やGDPRの解釈により各国で異なる

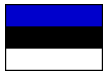
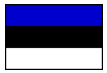
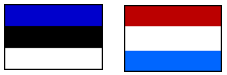
第三者機関（公的）による研究時の法的根拠

治療目的で収集されたデータを第三者機関である公的機関が研究で使用する場合の法的根拠としているもの

GDPR第9条第2項	採用している国	本調査対象国
明示的な同意 9(2)a	6	
明示的な同意 9(2)a ただし、非識別化または仮名化をする	3	
国内法またはGDPR前文33に基づいた包括同意	3	
明示的な同意が原則だが、ある一定の条件下で同意が免除される	4	
公衆衛生分野での公益目的 9(2)I	9	
研究目的 9(2)j	14	
その他	1	
研究の法的根拠を国内法で指定していない	12	

第三者機関（民間）による研究時の法的根拠

治療目的で収集されたデータを第三者機関である民間機関が研究で使用する場合の法的根拠としているもの

GDPR第9条第2項	採用している国	本調査対象国
明示的な同意 9(2)a	7	
明示的な同意 9(2)a ただし、非識別化または仮名化をする	3	
国内法またはGDPR33に基づいた包括同意	3	
明示的な同意が原則だが、ある一定の条件下で同意が免除される	4	
公衆衛生分野での公益目的 9(2)I	6	
研究目的 9(2)j	13	
その他	1	
研究の法的根拠を国内法で指定していない	13	

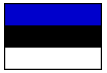
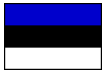
注1) 1か国で複数回答の場合もある
注2) EU離脱をした英国は採用している国の集計には含まれていない

 出所：https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

【EU調査報告】第89条第1項を採用して研究時等のデータの保護措置を定めている国は18か国あり、第89条第2項に基づいて個人の権利の行使制限を定めている国も14か国ある

GDPR第89条第1項により国内法を制定した国

EU27加盟国の内、医療情報を活用した研究のため、GDPR第89条第1項で述べられている保護措置について国内法やガイダンスを策定している国の数

GDPR第89条第1項の採用		採用している国	本調査対象国
No		9	
Yes		18	
Yesと回答した場合の法令の内容	公的機関の科学研究	12	
	民間機関の科学研究	9	
	国家統計目的の研究	12	
	当局の計画目的の研究	9	
	その他	6	

注1) 1か国で複数回答の場合もある
注2) EU離脱をした英国は採用している国の集計には含まれていない

GDPR第89条第2項により個人の権利の行使制限を制定した国

EU27加盟国の内、医療情報を活用した研究のため、GDPR第89条第2項で述べられている個人の権利の行使制限を定めている国の数

GDPR第89条第2項の採用	採用している国	本調査対象国
Yes	14	
Yes（部分的に）	5	
No	6	
不明	2	

- 27のEU加盟国のうち、19か国がGDPR第89条第2項に基づき、国内法で個人の権利の制限を定めている
- 研究が既に進行している場合、データの修正または消去することが既に進行中の研究を妨げることになり、また研究で既に使用されたデータの除去は非常に困難であることから、修正と消去の権利を限定的なものにしている

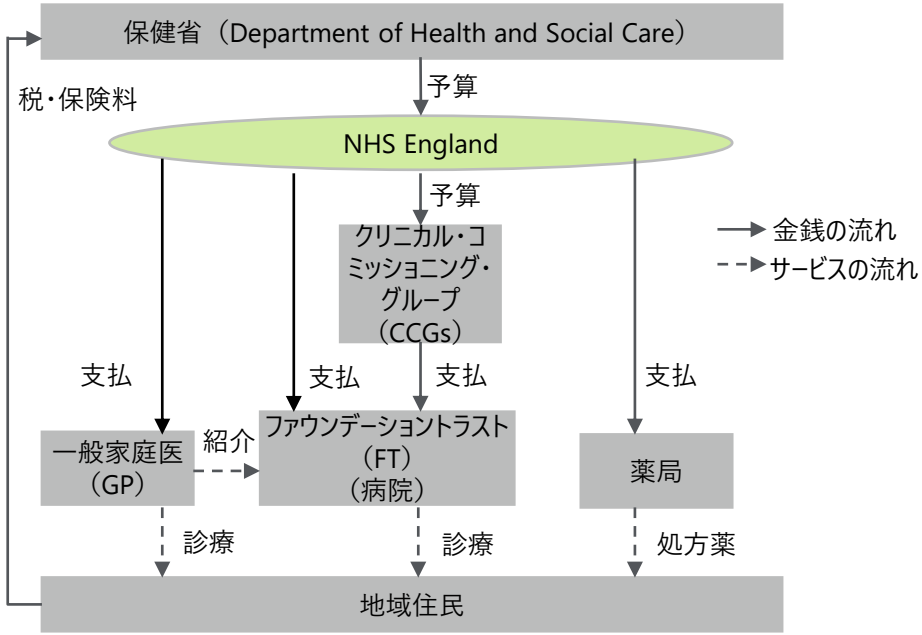
 出所：https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

3.3.3 英国 

英国(UK)

■ 医療制度の概要

制度	概要
医療保険	・全国民を対象とした国営の国民保険サービス（National Health Service : NHS)を政府が提供
医療費	・基本的な医療サービスは原則、国民の自己負担がない ・先端医療や特別な素材を使用した歯科等は自己負担あり
GP制度	・患者が登録した、かかりつけ医(GP)からプライマリケアを受ける ・必要に応じてGPが専門医や病院等の第二次医療へ紹介
診療報酬	・GPへの診療報酬の70％は登録患者数に応じる。残り30％は予防達成度や疾病管理の質のフレームワークに応じて支払われる
医療ID	・NHS番号(NHS digitalが提供するサービスの患者識別に用いる)



■ 健康・医療及び情報保護の法体系

➢ EU法
- ✓ General Data Protection Regulation: GDPR
  2020年末、EU離脱移行期間終了により、2021年1月よりUKGDPR施行

➢ 国内法
- ✓ 一般法　The Data Protection Act：DPA (個人情報保護法　2018）
  英国内の個人のためのデータ保護の強化が目的。英国やEU域外への個人情報の移転も対象
- ✓ 医療法関連
  National Health Service Act 2006
  患者情報の管理及び利用について規定
  The National Data opt-out （2018年5月）
  2020年までにヘルスケアデータを扱う事業者はオプトアウト式の導入を義務化
- ✓ ガイドライン
  ①英国のデータ保護当局であるInformation Commissioner's Office (ICO)がDPAを実務レベルで適用できるように詳細な説明をしたガイドラインを発表
  ②NHS Digital が英国における医療のデジタル化を推進しており、GDPRガイダンス、データセキュリティの実践指針、サービスの標準化などについてガイドラインを発表

■ EHR/PHRの取組み

NHS England、国家情報部(National Information Board : NIB)、医療やパーソナルデータの利活用推進を管轄しているNHS Digital がEHR計画を推進

➢ NHS Spine
- NHS Digitalが提供する医療記録に関するサービスの総称であり、次の7つのサービスを提供している。①患者の人口動態的な情報のデータベース、②GP間の情報転送サービス、③EHR/PHRサービス、④電子処方箋システム、⑤GPから病院へのオンライン紹介、⑥病院間の画像情報交換、⑦二次利用サービス

➢ The Summary Care Record : SCR (EHR・PHRシステム）
- GPの診療システムを介したEHRの仕組みであり、GPのみが入力可能
- 二次医療の医師はSCRの閲覧はできるが入力はできず、二次医療圏で生じた登録事項はGPが把握し、必要に応じてGPがSCRに入力する
- 2018年にSCRがEHRからPHRに発展し、NHSが提供するNHSアプリや、NHSが認証した他のアプリを通じて、患者が自身の情報を閲覧可能となった

➢ Clinical Practice Research Datalink (CPRD)
- GPシステム上の診療情報の患者個人情報を非識別化処理し、NHSが別途収集した二次医療圏情報も付加し、研究に利用可能にする二次利用の仕組み
- 同意取得はThe National Data opt-outに基づいたオプトアウト方式

出所：https://www.mhlw.go.jp/wp/hakusyo/kaigai/20/dl/t3-08.pdf
https://www.kansai-u.ac.jp/Keiseiken/publication/seminar/asset/seminar12/s196_1.pdf

英国における個人情報保護のための法律は、「EU離脱に伴うUKGDPR」と「国内法であるDPA」が存在している

英国における個人情報保護のための法整備の概要

個人情報保護のための法整備の背景

- 英国におけるコモンロー(慣習法)は、そもそもプライバシーという概念を有していなかったため、一般的なプライバシー権を創設しようという動きがあり、DPAが制定され運用が行われてきた
- 1995年のEUのデータ保護指令は、EU加盟各国が個別に個人データ保護のための国内法を制定したため、個人データ保護の範囲等、各国間で差異が生じた状態で運用されていた。また、急速な技術発展とグローバル化は、個人データ保護に対して新たな課題をもたらした(前文第6項)
- そのため、域内市場全域にわたりデジタル経済を発展させることができるようにする信頼を形成することの重要性に鑑み、それらの発展は、強力な執行によって支えられたEU 域内における強力かつより一貫性のある個人データ保護の枠組みを必要とした(前文第7項)
- すなわち、データ保護指令が採択されて以降の環境変化を踏まえた制度としてGDPRが制定された

コモンローによる個人情報保護

1984年　The Data Protection Act 1984(DPA)

1998年　The Data Protection Act 1998(DPA改正)

✓ 1995年のEUのデータ保護指令に基づき英国で指令を運用する規定として制定すると同時に1984年に制定した旧法は廃止

2018年5月　General Data Protection Regulation(GDPR施行) 及びThe Data Protection Act 2018(DPA改正)

✓ いずれも、分野ごとに規制ではなく、個人情報に関することであれば分野にかかわらず適用される

✓ 同年制定のDPAは、GDPR を遵守しつつ、英国内でのGDPR の効果を高めるために規定の修正・追加などを定めている

2021年1月　UKGDPR

✓ EU離脱に伴う制定、移行期間終了時には、個人データの処理に関して、現在のEUのGDPRのルールがそのまま適用された

　出所：一般データ保護規則（GDPR）の前文、JETRO「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）

医療情報の一次利用、二次利用共に、原則本人同意が必要である。ただし、NHS法第251条やDPAで、同意に依拠せず情報の利活用が可能な場合が定められている

■ コモンローでは医療情報の機密保持に対する義務を課し、不正な個人情報の使用・開示を防止する定めがある一方、NHS法において、秘密保持の義務を免除する法令を定めている

同意の法的根拠

ケース	治療・研究目的での情報開示に関する同意	個人情報の取扱いに関する同意
関連規則	• Common Law Duty of Confidentiality • National Health Service Act 2006 (NHS法) • The Health Service (Control of Patient Information) Regulations 2002	DPA 2018 (DPAの第2章にUK GDPRが含まれている)
規制の目的	秘密保持されている個人情報の使用又は開示が不正に行われないよう規制する	• GDPRに準拠しつつ、一部要件を加えている
規制対象	英国の個人データを取り扱う者	英国の個人データを取り扱う者
データ主体から取得する同意	• 黙示の同意（Implied consent） 治療等のためにデータが使用される場合など、患者が自分のデータの利活用を合理的に期待している場合 • 明示的な同意（Explicit consent）	明示的な同意（Explicit consent) (同意の自由、特定の目的や利用されるデータに関する説明、本人の明確な意思表示等要件が定めれている)

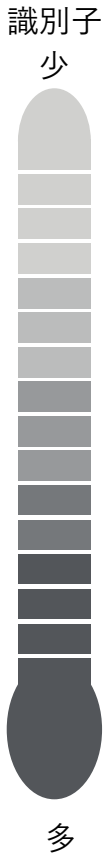
NHS法第251条承認にて、コモンローの守秘義務が免除　された場合、第三者への情報開示が可能である

GDPR第6条及び第9条の要件を満たせば同意による必要はない

研究目的での医療情報の使用・開示

英国では医療情報を第三者が利活用する際に、本人の同意を得る場合と、得られない場合の利用条件がある

研究における個人情報の利活用



本人の同意は不要	匿名化	■ 匿名化された情報は個人情報に該当しない Anonymous data	GDPR 前文 26
	同意以外の法的根拠	■ データの取扱いに関する法的根拠が本人の同意でない場合（Legal obligation, Public Interest, Legitimate interest)	GDPR 第6条
本人の同意の取得が困難な場合	本人の同意の免除	■ 医学研究において、匿名化された情報では不十分であり、本人の同意取得が実現可能でない状況である場合にコモンロー上の守秘義務（Common law duty of confidentiality)が免除される	NHS法第251条
本人の同意	本人の同意	■ 明示的同意(Explicit consent): 研究プロジェクトにデータを含める等の、十分な情報提供を受けた後に、特定の目的のためにデータを使用することに患者が同意した場合にDuty of Confidentialityが適用される	コモン・ロー

仮名化(Pseudonymisation)
- 仮名化は個人情報のセーフガードとして利用が推奨されているが、データの取扱いに係る法的根拠にはならない。
- 仮名加工されていても、個人情報に該当し、GDPRやDPAの適用を受ける

医療情報に関して、オプトアウトでのデータ利活用可能な制度や、研究の将来目的に対しても同意を取得できるように法令が定められている

情報開示に関する同意の柔軟性

【Common Law Duty of Confidentiality】

- コモンローとは裁判所が法律上の論点に基づいて事件を決定し、拘束力のある凡例を作成することによって発展してきた法律。守秘義務(confidentiality)はコモンローの一つであり、判例によって変化する。秘密保持されている個人情報の使用又は開示には、合法的な根拠があることを要求する法律である
- 同意取得場面: 治療等のためにデータを開示する場合（黙示の同意）、研究プロジェクトにデータを使用する場合（明示的な同意）
- 明示的同意(Explicit consent): 研究プロジェクトにデータを含める等の、十分な情報提供を受けた後に、特定の目的のためにデータを使用することに患者が同意した場合にDuty of Confidentialityが**適用**される

【National Health Service Act (NHS法) 第251条】

- 匿名化された情報を利用できない場合及び同意を得る実現可能性がない場合、医学目的での機密の患者情報の利用を可能にするために、コモンロー上の守秘義務(Duty of Confidentiality)が**免除**される
- NHS法第251条に基づいた研究には、ナショナルオプトアウトが適用される(NHS法第251条の適用によりオプトアウトでのデータ利活用が可能となっている）

※ただし、第251条承認は厳密に運用されている

【The Health Service (Control of Patient Information) Regulations 2002】

- 2006年NHS法を親法とする規則であり、NHS法第251条の下で施行
- Health Research Authority (HRA)のConfidentiality Advisory Group (CAG)が識別可能な患者情報への同意なきアクセスへの承認を行う

将来目的の研究に対する同意の柔軟性

【GDPR 前文33】

データの収集時に研究目的が特定されていない場合、本人は研究の分野に対して幅広く同意を与えることや、当初の研究目的部分に限定して同意を与えることも認められている

- 科学研究のための個人情報を収集する際、データ活用の全ての目的を特定することが難しい場合がある
- そのため、科学研究の倫理基準が満たされている場合、本人は特定の研究目的ではなく科学研究の分野への同意を与えても良い
- 本人は意図された目的の範囲の研究や一部の分野のみに同意する機会も与えられる

【Human Tissue Act 2004】

Human Tissue Act 2004は ヒト組織の除去、保管、使用、廃棄に関する活動を規制するための法律である。研究に参加するにあたり、本人は同意(informed consent)を与えることが基本原則であるが、同意する情報の範囲については選択肢がある

- Specific consent: 特定のプロジェクト、治療、使用
- Generic consent: 未定のプロジェクトへのヒト組織保管、使用

英国のHealth Research Authorityのガイダンスでは、データ管理者の組織の属性による、GDPRの法的根拠の違いが示されている

UK Policy Framework for Health and Social Care Researchで実施される医療や介護に係る研究の場合、その法的根拠はデータ管理者である組織の種類によって決まる

医療や介護に係る研究におけるGDPRの法的根拠

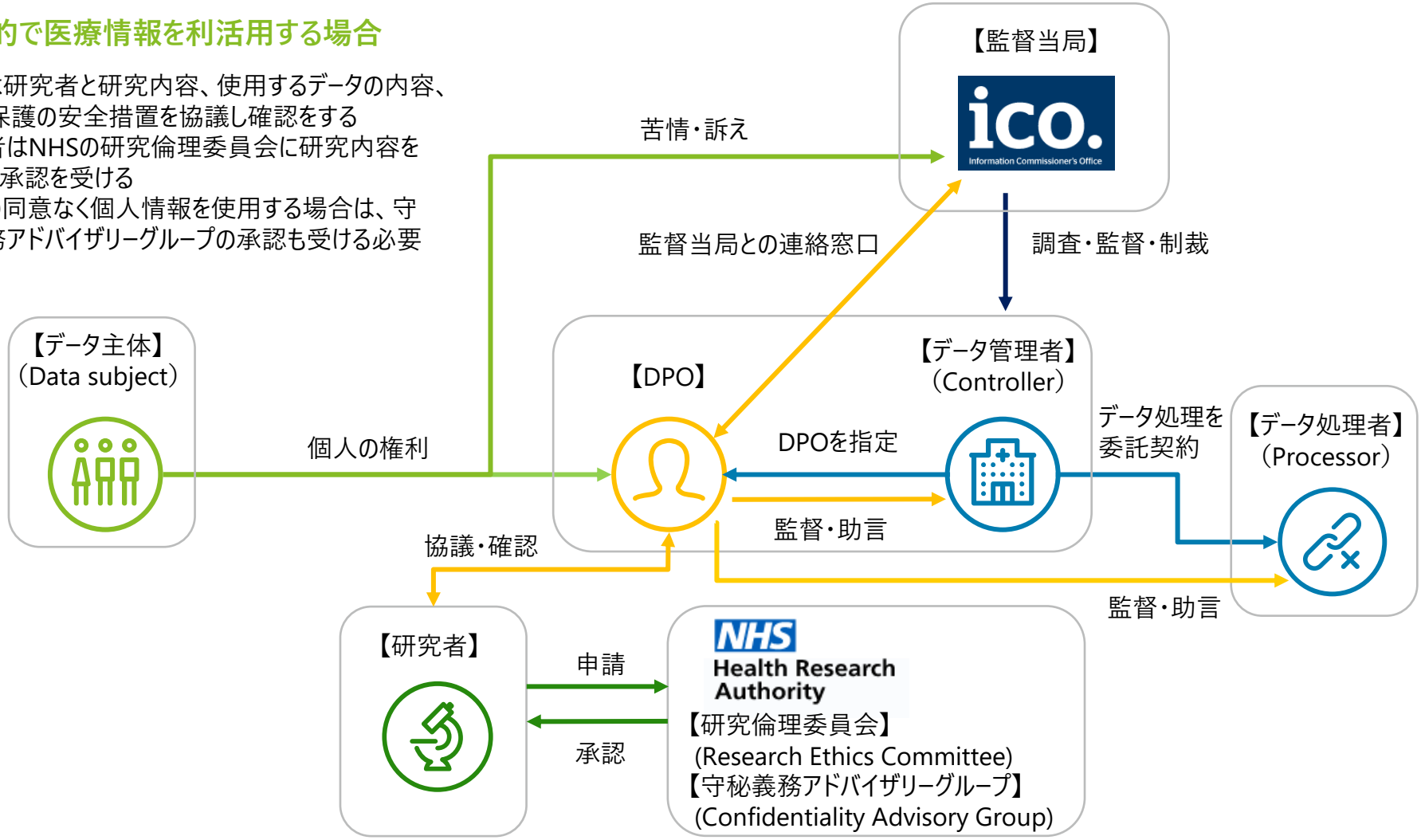
同意 Consent	• GDPRの下で医療情報のデータ処理を合法的に行うためには、①GDPRの法的根拠が確認されていること、②その他関連する法的枠組みを満たす必要があること、という二つの基準を満たしている必要がある。②には研究への参加の同意も含まれ、同意を通じたcommon lawの守秘義務を満たす例もある • 英国において「同意」は、common lawの守秘義務違反を避けるため、治験への参加のため、ヒト組織サンプルの採取と使用のため等に得られてきた。これは、GDPR導入後も変わらない • GDPRは、管理者とデータ対象者の間に力関係の不均衡がある場合、同意は法的根拠として適切でないとしている
公共の利益 Public interest	• 大学、NHS組織、研究評議会機関(Research Council institutes)、その他の公的機関の場合、研究のための個人データの処理は"task in the public interest"でなければならない • データポータビリティの権利は、research under public interestにおいては適用されない
正当な利益 Legitimate interest	• 営利企業や慈善団体の場合は、研究のための個人データの処理は"legitimate interests"の範囲内で行われなければならない • データポータビリティの権利は、research under legitimate interestsにおいては適用されない

出所： https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/

研究者とDPOは研究目的や使用する医療情報の内容、データ保護の安全措置等について検討する。研究者はそれらについて研究倫理委員会に承認申請を行う

研究目的で医療情報を利活用する場合

- DPOは研究者と研究内容、使用するデータの内容、データ保護の安全措置を協議し確認をする
- 研究者はNHSの研究倫理委員会に研究内容を申請し承認を受ける
- 本人の同意なく個人情報を使用する場合は、守秘義務アドバイザリーグループの承認も受ける必要がある



出所： https://www.hra.nhs.uk/approvals-amendments/
https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/what-you-should-do-now/

NHSの組織や患者、医療介護に関わる研究については、RECのレビューを受ける必要がある。また個人の同意を得ずに患者情報を使用する場合はCAGの承認も必要である

研究倫理委員会と守秘義務アドバイザリーグループの承認

IRAS
INTEGRATED RESEARCH APPLICATION SYSTEM

- UKの医療情報・介護情報に係る研究の承認申請はRECやCAGに行う必要がある
- これらの申請はThe Integrated Research Application System (IRAS) を通してオンラインで行うことが可能である

NHS Health Research Authority	Health Research Authority (HRA)	
	研究倫理委員会 Research Ethics Committees (REC)	守秘義務アドバイザリーグループ Confidentiality Advisory Group (CAG)
申請・承認の内容	• NHSの組織や患者、Health and Social Care(HSC)に関わる研究については、RECのレビューを受ける必要がある • RECはデータ保護と研究倫理原則に基づきながら、医療情報の利活用についても研究者に対して助言を行う • 研究で使用される個人情報についてDPA2018への遵守も確認する • RECの構成は専門家（医療専門家、臨床試験統計学者、その他の研究専門家）と、健康研究倫理に関心のボランティアメンバーの混合から成る	• 識別可能な患者情報を、本人の同意なく使用する場合にはCAGに申請して、承認を受ける • CAGへの申請は研究の場合でも研究ではない場合でも必要であり、研究ではない場合はForm251（NHS法第251条の承認）を提出する
研究の場合	○	○
研究でない場合	–	○　(Form251の提出)

出所：https://www.hra.nhs.uk/approvals-amendments/
https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/
https://www.ukdataservice.ac.uk/manage-data/legal-ethical/obligations/research-ethics-review.aspx

GDPRおよびDPAで匿名加工方法についての定めはないが、ICOが匿名加工手法に関するガイドラインを公表している。匿名加工の責任者はデータ管理者である

匿名化・仮名化の定義と要件

■ 匿名化(Anonymisation)の定義

➢ GDPR

- GDPR 前文26において、匿名化とは、識別された自然人又は識別可能な自然人との関係を持たない情報・データ主体を識別できない情報のことであると定義している
- 完全に匿名化された(truly anonymized)情報は個人情報の特性を持たないため、GDPRの適用を受けない

➢ 国内法

- 国内法であるDPAでは匿名化に関する規定はないが、DPA Section 51に基づき、情報独立機関であるICOが匿名加工に関するガイドラインを公表している
- ICOのガイドラインでは、匿名化とは個人を識別することが起こりえない形にデータを処理することと定義している

■ 匿名化要件

- DPAでは匿名化の技術的手法を定めておらず、ICOが公表している匿名加工ガイドラインを参考に右表のような匿名加工をすることになる

■ 仮名化(Pseudonymisation)の定義

- 現実世界(real world)での身元を明らかにしない特有(unique)の識別子を使用し、データセット内の個人を区別する処理

ICOによる匿名化手法の例示

手法	具体例
データ削減	識別子の削除
	記録の削除
	情報粒度の変更
	部分的隠蔽
データ攪乱	マイクロアグリゲーション (個々の数値をグループごとの平均値へ置換)
	データの交換
	ポストランダム化手法(PRAM)
	ノイズ追加
	リサンプリング
非データ攪乱手法	サンプリング
	クロス集計

 出所： https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

ICOはテストやケーススタディを通じて個人再特定のリスクがないか評価することを推奨しているが、米国のようなリスク評価の基準は定められていない

匿名化の評価

■ 評価に関する規定
- ➢ DPAでは再特定の評価方法について言及していない
- ➢ ICOは、完璧に再特定リスクを評価することは不可能であり、ケーススタディを通じて状況に応じてリスクの評価をする必要があるとしている

■ 評価手法
- ➢ ICOでは、以下のテストを通じて再特定リスクを発見することを推奨している

テスト	説明
Motivated Intruder Test	• 個人の再特定を試みる人物が、その対象となる匿名データと他の情報源を組み合わせることによって再特定ができないか判断するテスト • 具体的には、ウェブ、SNS、図書館などの情報を収集して特定を試みる
Re-identification Test	• 個人の再特定が不可能であることを確認するためのテスト • 具体的なステップは以下の通り ①匿名データから、公開しているデータ(もしくは公開予定のデータ)を把握する ②他のデータと匿名データを統合しても、個人が特定されないか確かめる

129 出所： https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

公益目的での医療情報の使用・開示

DPA2018では「重要な公益目的」の項目を列挙し、同意を不要とするケースが定められている

重要な公益目的（DPA2018, Schedule 1, Part2)

同意不要	条	項目	概要
	6	法令及び政府の目的	法により権限を与えられた者、国王、又は英国大臣の機能の行使のために情報を取り扱う場合
	7	司法及び議会の業務	司法業務又は議会の機能の行使のために情報を取り扱う場合
	8	機会び待遇の平等	人種・民族の出自、宗教・思想の信条、健康データ、性的指向といった特別分類個人情報を取り扱う際に、機会や待遇の平等性を確認する場合
○	9	組織の上層部の人種的多様性	特定の組織の上位につく者を識別し、組織の上位につく者のダイバーシティを保つために情報を取り扱う場合
○	10	不法行為の予防	不法行為を検出し、事前に防ぐために情報を取り扱う場合
○	11	国民の保護	不正や組織の不当な管理から国民を保護する場合
○	12	不法行為に対する法的義務	不法行為を行った人物に対して、法的義務を果たすための行為である場合
	13	不法行為に関する報道等	報道、学術、芸術、文学的な目的においてある人物の不法行為や組織の不当な扱いに関する情報を開示する場合
	14	詐欺の防止	ある種の詐欺を防止する目的で、詐欺防止組織による情報開示の場合
	15	テロリストへの資金・マネーロンダリング容疑	2000年テロリズム法や2002年犯罪収益法に基づいた情報開示の場合
○	16	特定の障がいや病状の個人への支援	非営利組織による、特定の障がい又は病を持つ人の支援や啓蒙において、人種・民族、遺伝子・生体データ、健康データ、性生活・性的指向に関する情報を取り扱う場合
○	17	カウンセリング	機密性のカウンセリング又は類似の気密性の高いサービス提供目的で、本人の同意を取得することができない又は同意をとることでサービス提供に偏見をもたらす可能性がある場合

出所：https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted

DPA2018では「重要な公益目的」の項目を列挙し、同意を不要とするケースが定められている

重要な公益目的（DPA2018, Schedule 1, Part2)

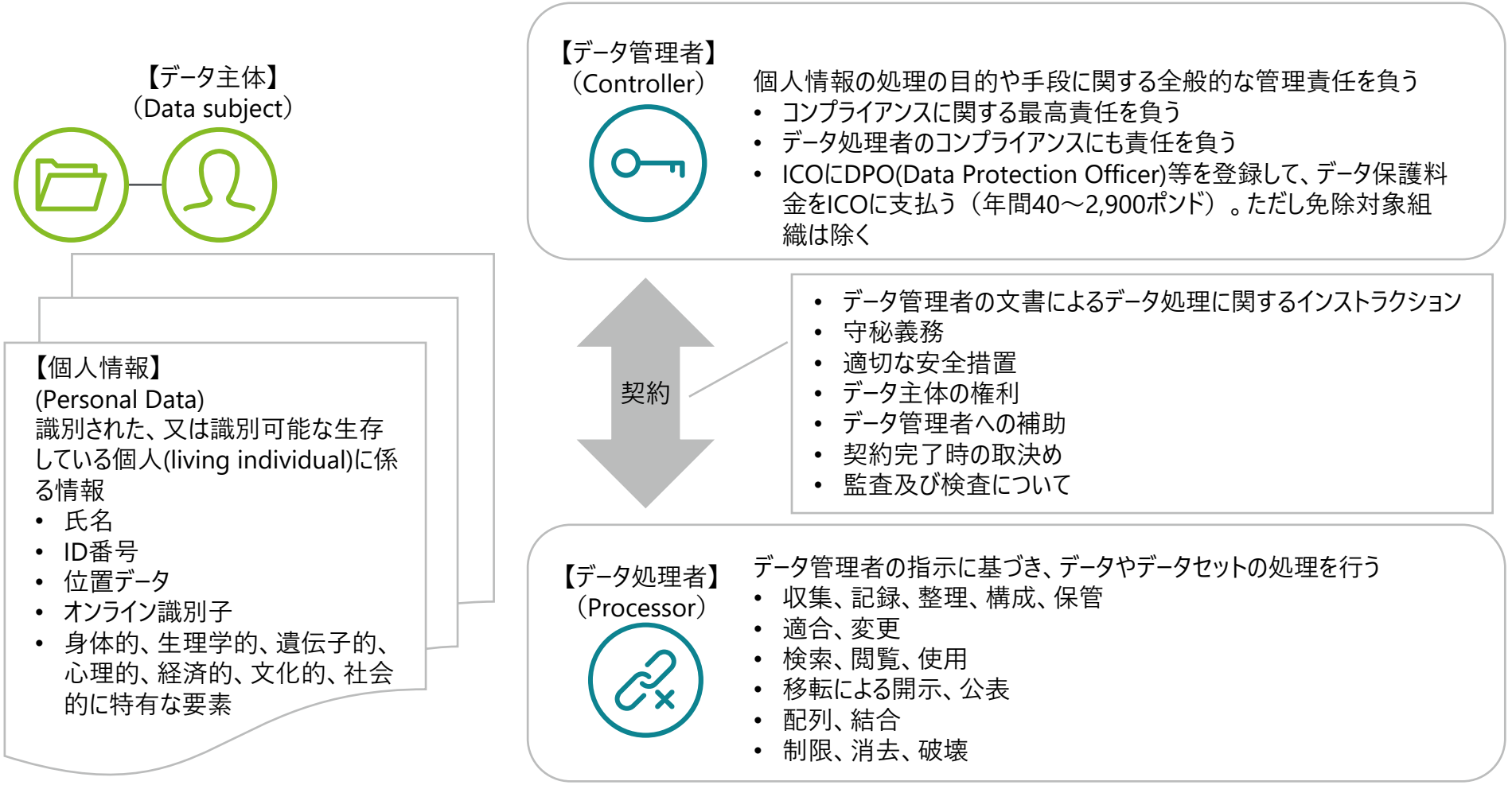
同意不要	条	項目	概要
○	18	子ども及びリスクの高い個人の安全措置	18歳未満の個人又は18歳以上でネグレクトや身体的・心理的・感情的な被害を受けるリスクが高い個人を保護する場合
○	19	個人の経済的健全性の安全措置	身体的・心理的な障がいや病気により、自身の経済的な健全性を守る能力が十分でない個人のための安全措置である場合
○	20	保険	保険契約の権利の執行や義務の履行において、本人の同意取得が困難である場合
○	21	職域年金	職域年金の受給資格や受給額の決定のための、データ主体に関する健康データを取り扱う場合
	22	政党	政治活動や政治的見解の公表にかかる情報を取り扱う場合
○	23	要請に対する議員の応答	議員辞職に関する場合やデータ主体以外からの個人の要請に従って議員が対応する場合
○	24	議員への開示	データ主体以外の個人から議員や当局関係者に開示要求がある場合
	25	囚人について下院等に通達する	囚人に関する情報を下院等の議員に開示する場合
	26	判決の公表	裁判所や法廷の判決やその他の決定事項の公表に関する場合
	27	スポーツのアンチ・ドーピング	スポーツのドーピングを排除する目的でドーピングやその疑いがあるケースの情報開示をする場合
○	28	スポーツにおける行動規範	スポーツやスポーツイベントを不誠実性や不当な行為から守るための措置として必要な場合

出所：https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted

運用の仕組み

DPAの定めでは個人情報のデータ管理者はデータ処理者の業務やコンプライアンスに関しても責任を負い、データ主体やICOは管理者と処理者の両者に対して責任を問える

データ主体・管理者・処理者の関係（DPA2018)



出所：https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

個人情報保護監督機関としてICOがある。またデータ管理者がDPOを個別に任命し組織内の個人情報保護方針の遵守を監視する

法の適切な運用を確保するための機関

	ICO(Information Commissioner's Office)	DPO(Data Protection Officer)
根拠法令等	DPA、GDPR	DPA
選任主体	長官任命は国王、メンバー任命は長官	データ管理者(controller)
役割の範囲	■ 国民議会、政府及びそれ以外の機関・組織に対し、取扱いに関する権利と自由の保護に関する立法・行政措置の助言 ■ 管理者及び処理者の義務の周知（GDPR第57条）	■ 管理者、管理者に従事する処理者、及び個人データの処理を行う管理者の従業員に義務を通知し、助言すること(DPA Section71) ■ データ主体とICOとの連絡ポジション
役割	■ データ取扱いの記録義務の範囲(GDPR第30条) ➢ 管理者は氏名、連絡先、取扱いの目的、データの種類等のデータ取扱活動を記録し保管する ■ データ漏洩時(データ侵害時)の通知義務(DPA Section67) ➢ 管理者は過度な遅延なく、72時間以内に下記を通知 ①データの性質 ②データ保護責任者の名前及び連絡先 ③想定される結果と対処措置	■ データ保護オフィサーの役割(DPA Section71) ➢ 個人情報保護に関する管理者の方針を遵守しているか監視すること ➢ データ処理に関する相談の窓口となること

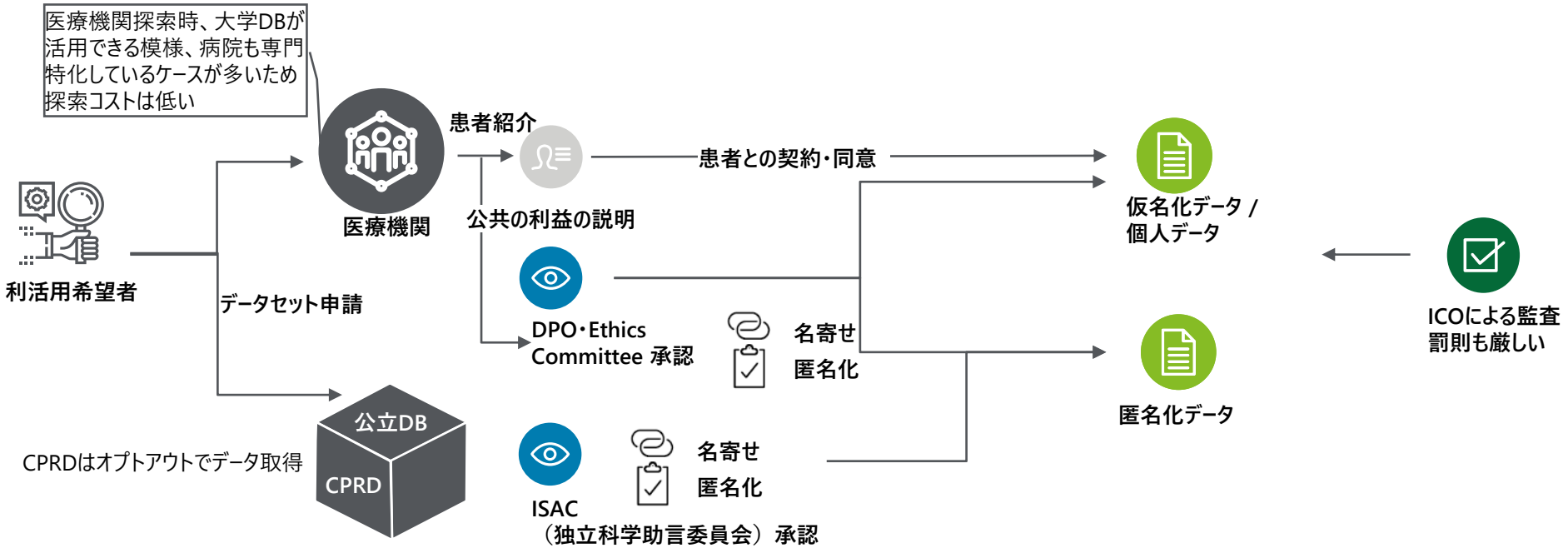
罰則・是正措置
■ 個人の権利、UK外へのデータ移転、安全保障、秘密情報に関する違反：(法人)€2,000万と前年度全世界売上高の4％いずれか高い方、(法人以外)€2,000万以下 ■ 上記以外の違反：(法人)€1,000万と前年度全世界売上高の2％いずれか高い方、(法人以外)€1,000万以下 ■ 実際の罰金事例 ➢ 2019年12月、ICOはロンドンを拠点とする薬局に、データのセキュリティ確保ができていなかったとして£275,000の罰金を課した。薬局は約50万件の氏名、住所、生年月日、NHS番号や医療情報などの個人情報を含む文書に鍵をかけず保有していた

出所：https://ico.org.uk/action-weve-taken/enforcement/doorstep-dispensaree-ltd-mpn/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

英国では、二次利用に関して従来同意か、公共利益の根拠適用が中心であったが、政府の働きかけもあり、GPデータを中心に医療DBの利活用割合が増加している

英国の医療情報二次利用の主要パターン

英国の医療情報利活用関連基本ルール
・一次利用：同意必要なし　※公共の利益6(1)(e) 、医療専門家との契約で健康産業への寄与9(2)(h)の適用【UK GDPR】【NHS法第251条】
・二次利用：同意が基本【DPA】、公共の利益6(1)(e) 、医療専門家との契約で健康産業への寄与9(2)(h) にて活用のケースもある【UK GDPR】※ 製薬会社などが個人情報を利用する場合
・二次利用その他：NHS関連の同意はオプトアウトが基本　【ナショナルオプトアウトプログラム】



多く活用されているCPRD(人口の約2割規模)は全国1,300のGPクリニックのデータをEHRを経由して収集し、ISAC（独立科学助言委員会）が審査した後第三者に提供している

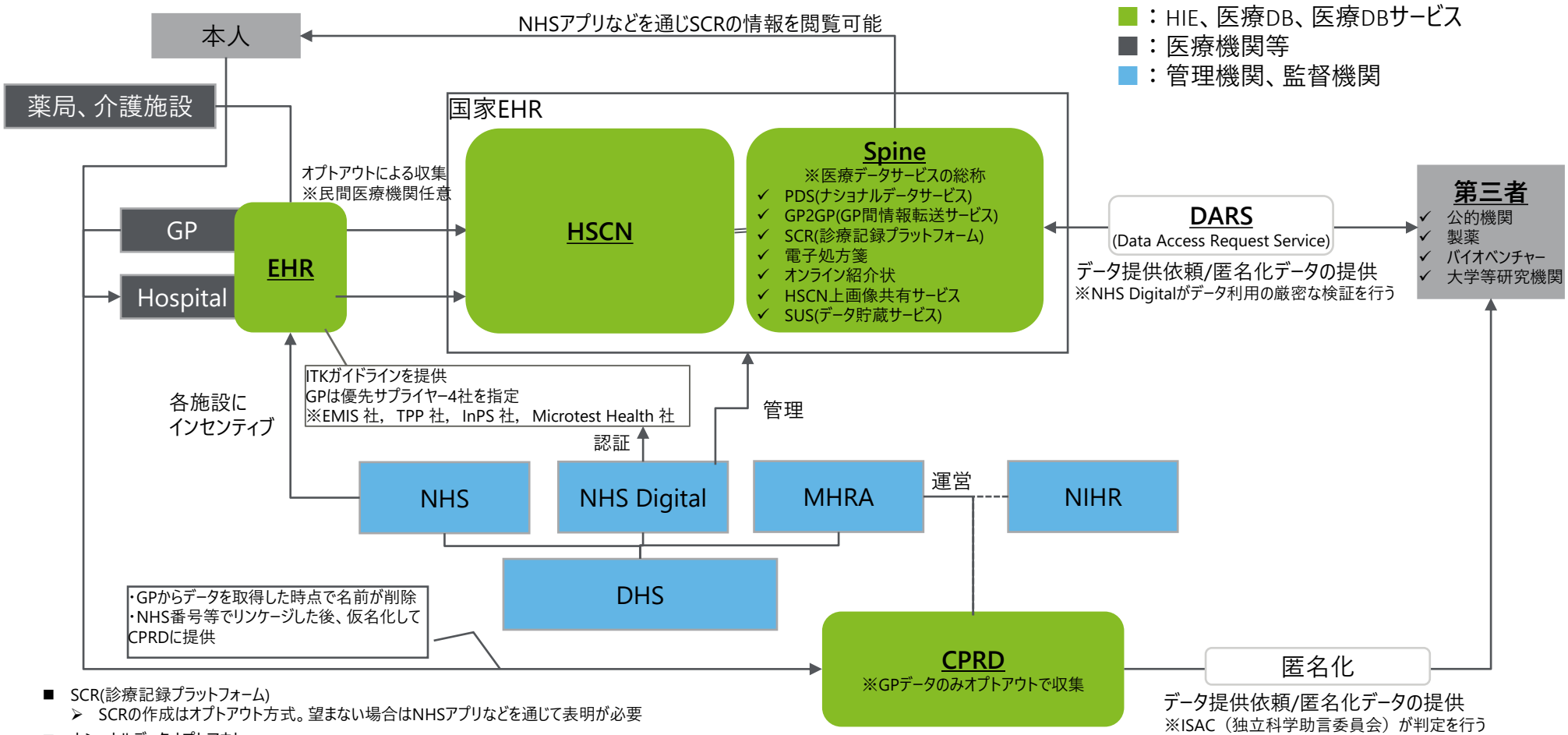
CPRDデータの概要

項目	内容		
管理者・運営者	保健省傘下のMHRA(Medicines & Healthcare products Regulatory Agency)		
規模	11百万人(人口の約2割。英国には約1,300か所のGP診療所があり、現在の登録患者は約35百万人といわれている)		
保有データ ※CPRD GOLD	1	Patient(患者)	患者ID、性別、出生年月、配偶者の有無、家族ID、小児健康診断登録の有無、投薬禁忌、登録日、登録解除日、死亡日 等
	2	Practice(GP診療所)	GP診療所ID、地域、データ登録日
	3	Staff(スタッフ)	スタッフID、性別、役割
	4	Consultation(相談)	患者ID、相談日、システム入力日、相談内容の種別、相談ID、スタッフID、相談日数
	5	Clinical(診察)	患者ID、診察日、システム入力日、相談内容の種別、医療コード(Medical Code)、スタッフID、症状 等
	6	Additional Clinical Details (診察の追加情報)	患者ID、システム入力日、追加情報種別、追加データ
	7	Referral(紹介状)	患者ID、紹介状発行日、システム入力日、紹介状ID、医療コード、紹介者、専門医の種別(NHS分類及びFamily Health Services Authority分類)、入院/日帰りの別、紹介の契機、緊急度
	8	Immunisation(予防接種)	患者ID、ワクチン投与日、システム入力日、相談内容の種別、相談ID、医療コード、スタッフID、予防接種の種別、投与ステージ(回数)、投与の有無、混合ワクチンの有無、投与理由、投与方法、バッチ番号
	9	Test(検査)	患者ID、検査日、システム入力日、相談内容の種別、相談ID、医療コード、スタッフID 等
	10	Therapy(処方せん)	患者ID、処方せん発行日、システム入力日、相談内容の種別、相談ID、製品コード(product code)、スタッフID、投与剤型ID、British National Formularyコード、総処方量、服用期間、投与単位(包数)、単位の種別、継続処方の有無
	※Vision製をもとに作成したシステムをGOLD、EMIS製をもと作成したシステムをAURUMと呼称 ※GP診療所の一次診療データとNHS等から提供された外部データに含まれる二次診療データは、連結しての提供が可能。連結データには、GOLDには411診療所・患者数約10百万人、AURUMには232診療所・患者数約6.5百万人が含まれる		
データ利用可能者	・CPRDの利用申請の対象者は、ISAC(独立科学助言委員会)の審査を経て利用認可を得た組織(研究者個人はNG)。組織の形態は、公共/非公共や営利/非営利の別は問われない ・利用申請者は、ISACの認可を得てから、CPRDとライセンス契約を行う。ライセンス契約の当事者は、保健大臣がLicensor、組織がLicenseeとなる ・ライセンス契約の方法には、契約期間を1年間としてISACの利用認可を得た複数の研究に対してデータを利用できる契約(Multi-study Licence)と、ISACの利用認可を得た研究のために個別のデータセットを利用する契約(Dataset Licence)があり、これらは組織が営利と非営利の場合で異なる契約書面を用いる ・データの利用目的に制限はない		
利用可能データ	・非特定化データ、データ提供サービスあり(有料)		
その他特徴 問題点	・GPシステムは、2019年2月現在、EMIS社、TPP社、InPS社、Microtest Health社の4社がNHS Digitalが要求する基準を満たす優先サプライヤー(principal supplier)の指定を受けている ・2020年2月段階で約3,000本の学術論文に利用されたと報告あり		

出所：NHSホームページ、平成30年度厚生労働省「諸外国における健康・医療・介護分野のデータベースの現状調査」

公的な医療DBとしては、NHS Digitalが管理するSpineとMHRAが運営するCPRDによって情報が集められ、いずれも匿名化したのち第三者提供されている

英国における医療情報(公的DB)の流れ



- SCR(診療記録プラットフォーム)
  - SCRの作成はオプトアウト方式。望まない場合はNHSアプリなどを通じて表明が必要
- ナショナルデータオプトアウト
  - 2018年にスタート、患者識別可能な機密情報を研究や保険医療計画策定の目的で使用する場合はオプトアウト方式にするよう義務付けられている(2021年までに私立医療機関も含め完了)
  - 2019年3月時点でGP登録患者の2.74%がオプトアウトの意思表明
- CPRD
  - CPRD のデータ処理の適法性は，GDPR の 第6条(1)(e)「公共の利益」，及び，第9条(2)(j)（第89条第 1 項に従う必要）を法的根拠とする

3.3.4 エストニア 

エストニア

■ 医療制度の概要

制度	概要
医療保険	・社会保険税を財源としたエストニア健康保険基金が保険サービスを提供
医療費	・基本的な医療サービスは無料（人口の95％をカバー） ・民間の保険も利用
医師・医療機関数	・医師数4,400人、うちGP(かかりつけ医)約800人 ・病院数65か所、うち19か所で公的な医療を提供
IDカード	・誕生時に付番される国民ID ・医療機関の受診の際に患者識別番号として利用される
eIDカード	・15歳以上の国民が保するICカードで患者ポータルへのアクセス時に利用される。PINコードはログインパス、電子署名として機能する

■ 健康・医療及び情報保護の法体系

- EU法
  - ✓ General Data Protection Regulation: GDPR
- 国内法
  - ✓ 一般法　Personal Data Protection Act (一般個人情報保護法)
  - ✓ 医療法関連

Health Service Organisation Act（2001年制定）
保健サービス全般を規制する法令。2008年に第5章を追加し、ENHISの定義、システムへのデータ転送、システムへのアクセス、研究倫理委員会の設置に関する概要を記載

Statute of the Health Information System（2016年制定）
医療情報システムに関わる法令。情報ポータビリティ、処理、開示、個人の情報に係る権利を定めている

The data composition of the documents transmitted to the health information system and the conditions and procedure for their submission
ENHISへの提供が義務付けられる情報項目の詳細が定められている

Human Genes Research Act
2001年に施行されたGene Bankの設立と維持について規制し、必要な遺伝子関連研究を組織することを目的とした法律

■ EHR/PHRの取組み

- EHR　・政府機関HWISCがエストニア中央医療情報システムENHISを運営
  ・医師はENHISへ情報を共有する義務が課されており、全ての医師が既往症、診断経緯といった医療の基本情報にアクセス可能
- PHR　・患者ポータルサイトを通じてENHISに格納されている自分や家族の医療データを閲覧可能

年	経緯
～2000年	・1991年にソビエト連邦から独立。病院、GP等は独自の情報システムを開発し、電子カルテを導入
2005年	・社会省が医療機関や組合・協会と共同でeヘルス財団を設立
2008年	・エストニア中央医療情報システム（Estonian National Health Information System : ENHIS)をスタート
2010年	・電子処方箋が開始
2012年	・eConsultation（オンライン相談）の開始。GPと専門医間で患者の治療についてオンライン相談が可能となった
2014年	・デジタル化された医用画像の共有が義務化 ・Medical certificate serviceを開始。運転免許更新に必要な健康診断結果がオンラインで送信される
2015年	・eAmbulance サービス開始。救急搬送時に救急隊員がタブレットで服薬履歴、アレルギー、血液型等を確認 ・歯科データの共有開始
2017年	・社会省のIT部門とeヘルス財団を統合し、Health and Welfare Information Systems Center (HWISC)を設立 ・国防省の健康委員会に、訓練を受ける市民の健康サマリデータを送り、訓練実施の可否判断に活用
2018年	・E-labサービス開始。E-labサービスを使って公的な機関に検査を依頼し、検査結果がENHISにあがってくる
2019年	・フィンランドとの処方箋の共有開始 ・死亡証明書をENHISに共有

エストニアでは、一般個人情報保護法であるPDPAの他、公共情報へのアクセスや開示に関する法令と、保健医療サービスに関する法令でも個人情報の取扱いを定めている

同意の法的根拠

ケース	個人情報の一般的な取扱い		医療情報システム上の取扱い
関連規則	PDPA	Public Information Act	Health Services Organisation Act
規制の目的	• GDPRの実施基準を規定し、その法令を補足している • 個人情報に関する自然人の基本的権利と自由の保護を目的としている	• 公衆及びすべての者が公共目的とする情報にアクセスする機会を確保し、公衆が公務の執行を監視する機会を創出することを目的としている	• 医療情報システム(ENHIS)を含む保健サービス全般を規制
規制対象	• 個人情報の取扱いに関する官民両方を対象とする	• 官民両方	• 医療情報システム上のデータを取り扱う者
同意の取扱い	• データの処理にはデータ主体の同意が必要 • データ主体の同意は生涯有効 • 機微な個人情報(sensitive personal data)の処理には書面での同意が必要	• 州政府、地方自治体、法務関係者が管理するデータの利用に関する規程であり、本人同意に関する規定はない • 機微な情報の取扱いは組織の内部利用に制限されるが、法的な理由に基づいた、義務の遂行のための医療情報の取扱いは認められている	• 医療従事者が医療サービスを提供するために個人データを処理する際に同意は不要 • 全国医療情報交換プラットフォーム(ENHIS)を経由した医療情報の利活用に本人の同意は不要

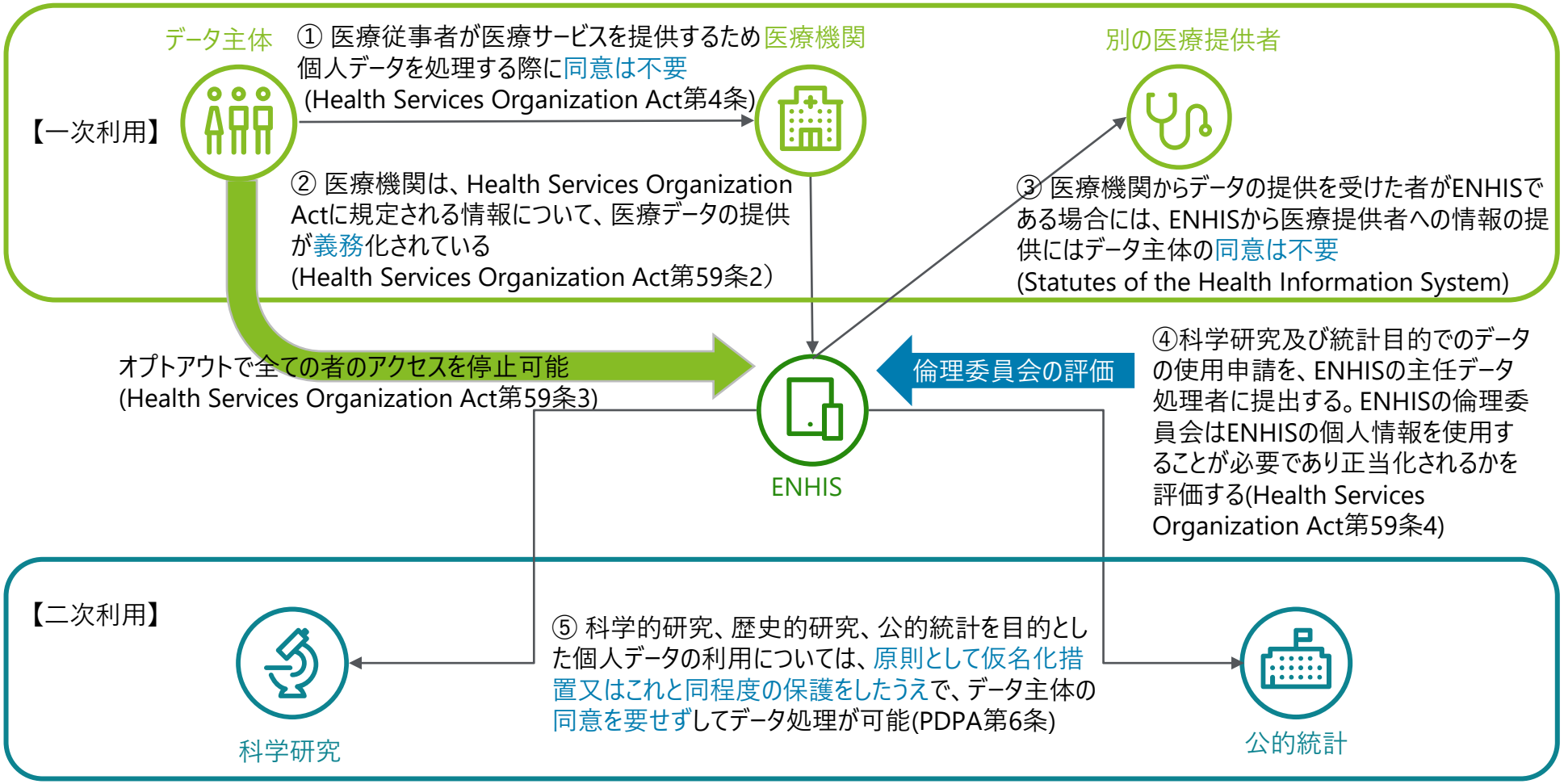
法的手段、報道目的、研究目的等で同意を不要とする場合の規定がある

法的な義務の遂行や生命に関わる場合等の医療情報開示が義務づけられている

本人の同意なく医療情報にアクセス可能であるが、本人はオプトアウト可能

Health Services Organization ActにおいてENHISへの医療情報の登録が義務化されており、ENHISを通して得られるデータは二次利用でもデータ主体の同意が必要ない

医療情報の一次利用と二次利用における本人の同意



出所：Health Service Organisation Act (HSOA)　https://www.riigiteataja.ee/en/eli/508012018001/consolide
PDPA　https://www.riigiteataja.ee/en/eli/523012019001/consolide

PDPAでは科学的・歴史的研究目的、及び公的な統計を作成する場合において、仮名化や倫理委員会等の確認を経てデータ主体の同意なくデータ処理をすることが認められている

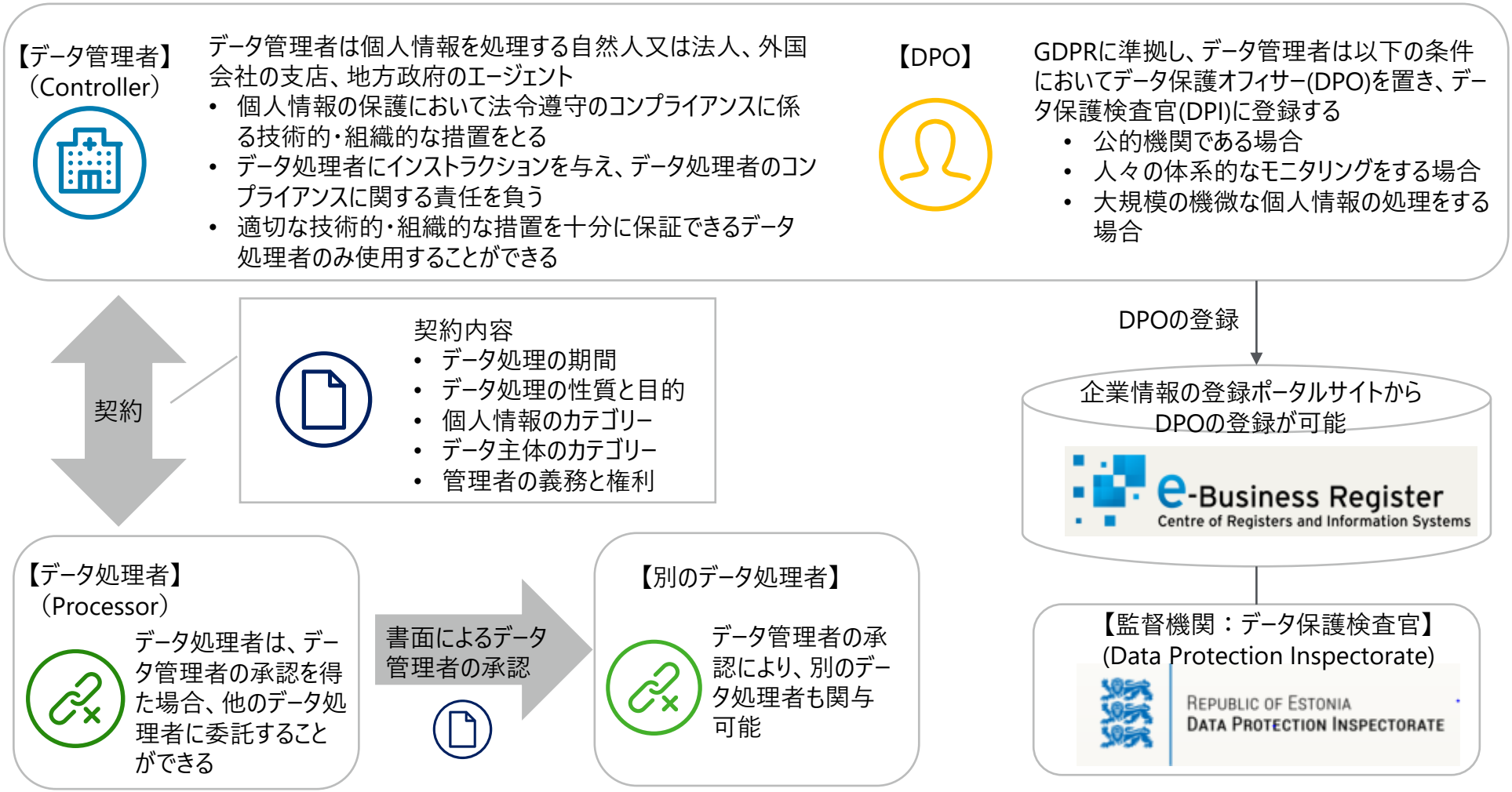
科学的・歴史的研究及び公的な統計目的（PDPA第6条）

仮名化	■ 仮名化(pseudonymised format)又はそれに該当する保護措置がとられている場合で、仮名化や同等の保護措置がデータ処理のためのデータ移転の前に行われている場合 ■ 追加的な科学的・歴史的研究及び公的統計の作成において必要な場合のみ、非仮名化による再識別化が認められる。データ処理者は、仮名化された情報へアクセスできる人物を指名する
仮名化をしない	■ データ主体を識別可能な状態で処理する際には、以下の要件を満たす場合のみ可能である ✓ 識別可能な情報の除去により、データ処理の目的が達成されない場合、又は目的達成が不合理に困難になる場合 ✓ 科学的・歴史的研究を実施する者又は公的統計を作成する者の推定により、公共の利益が勝る場合 ✓ 処理された個人情報によってデータ主体の義務が変わらない場合、又はデータ主体の権利が毀損しない場合
機微な個人情報に関する研究	■ 特別分類個人情報を扱う研究においては、該当分野の倫理委員会が研究目的等についてのコンプライアンスについて確認をする ■ 科学分野の倫理委員会が存在しない場合は、エストニアデータ保護検査官(Estonia Data Protection Inspectorate : DPI)がコンプライアンスについて確認をする ■ 国立公文書館に保管されている個人情報については、国立公文書館が倫理委員会の権利を有する
国の政策策定	■ 本法令における科学的研究には、当局が政策策定のために行う分析や調査も含むとみなされる。当局は別のデータ管理者やデータ処理者に情報を求め、受領したデータの処理が可能である
個人の権利の制限	■ データ管理者及びデータ処理者は、GDPR第15条、第16条、第18条、第21条の個人の権利の執行が研究目的の達成を阻害する場合は、個人の権利を制限することが認められる

出所：https://www.riigiteataja.ee/en/eli/523012019001/consolide

個人情報のデータ管理者はデータ処理者の業務やコンプライアンスに関しても責任を負う。また、監督機関であるデータ保護検査官(DPI)にDPOの登録をする

データ管理者とデータ処理者の関係



出所：https://www.riigiteataja.ee/en/eli/523012019001/consolide
https://ettevotjaportaal.rik.ee/index.py?chlang=eng

GDPRに準拠して、データ管理者はDPOを置き、国はデータ保護検査官(DPI)を監督機関として設置している

データ保護オフィサーと国の監督機関

	データ保護検査官 (Data Protection Inspectorate)	データ保護オフィサー (Data Protection Officer)
根拠法令等	PDPA　第32条、第33条	GDPR
選任主体	法務省からの提案を受け、エストニア政府が任命	データ管理者(Data Controller)
役割・権利	■ PDPAの要件遵守の監督 ■ 個人情報の取扱いに関連するリスクや保護手段、個人データの権利に関して、データ管理者とデータ処理者の認識と理解を向上させる ■ エストニア政府にデータ保護に関する問題への意見の提示 ■ EUの他の監督機関との相互協力(Section56-2) ■ 苦情に基づく監督手続(Section56-3) ■ 倫理委員会が存在しない研究分野において、倫理委員会の役割を担う(Section6(4))	■ データ管理者やデータ処理者のデータ保護方針の遵守を監視 ■ データ保護規定の義務の従業員への通知と助言 ■ データ保護の影響に関する助言 ■ パフォーマンスの監視 ■ 監督当局との協力(第39条)

罰則・是正措置
■ Health Service Organization Actに対する違反：€640 ■ PDPA 第2章に対する違反：最高€2,000万、又は（法人）前年度全世界売上高の4％のいずれか高い方 ■ 実際の罰金事例 ➢ 2020年、個人識別コードへのアクセスに関する同意を得ずに、他人の現在の処方箋データが閲覧可能であったため、DPIは3つの薬局チェーンに€100,000の罰金を課した

出所：https://www.riigiteataja.ee/en/eli/512112013011/consolide
https://www.aki.ee/en/data-protection-officer/data-protection-officer

データ保護検査官(DPI)は、2012年～2018年までの監督機関としての活動内容と件数をホームページ上で公表している

データ保護検査官(DPI)の活動報告件数 (統計より抜粋)

項目	内容	2012	2013	2014	2015	2016	2017	2018
コミュニケーション	問合せ、情報の自由に関する要求事項	817	1,370	1,144	1,369	1,417	1,520	2,384
	ヘルプラインの電話	1,160	1,344	1,141	1,136	1,419	1,527	2,556
監督業務	苦情受付	404	550	413	446	390	462	462
	データ保護違反の通知 (IMI *)	–	–	–	–	–	–	479
	監督下における現場視察	23	15	48	35	33	45	17
	監督下における提言・提案	–	–	–	299	56	125	10
	仲裁のケース（和解）	43	29	11	16	16	9	23
	軽犯罪の罰金刑と監督下における強制罰金	39	22	8	15	16	4	9
ライセンス・法的手続	登録申請（機微な個人情報の取扱い申請又はDPOの登録）	608	602	902	540	547	641	192
	データベースの承認（構築、使用、データ構成の変更、終了）	84	89	115	167	139	99	36
	データ主体の同意がない科学的研究のためのライセンス申請	13	17	13	29	18	54	61
	データ保護の十分性がない外国へのデータ移転へのライセンス申請	7	6	13	8	18	22	3
	シェンゲン圏、欧州刑事警察機構、その他の越境データベースにある自身のデータに関する申請	4	6	6	10	10	8	21

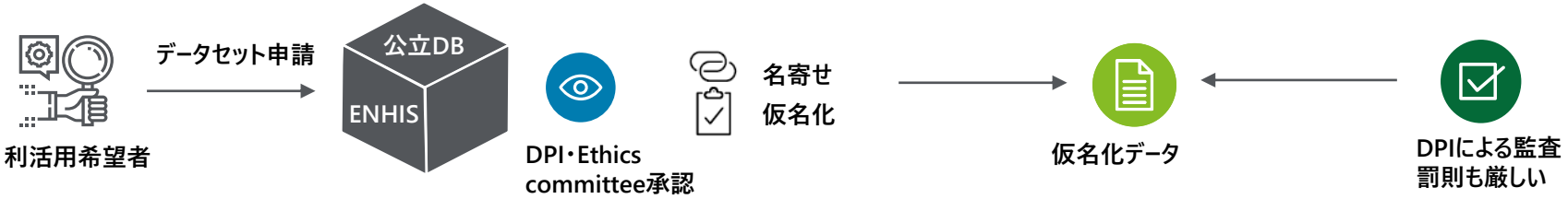
＊IMIはEUのInternal Market Information Systemであり、データ保護当局が情報交換を行い、苦情、説明請求、法の侵害通知、覚書を提供する

 出所：https://www.aki.ee/en/inspectorate/statistics

エストニアでは、国民の健康増進と医療費の適正化のためにほぼ完全な電子化を進めてきたが、研究目的等の二次利用に関しては必ずしも積極的ではない

エストニアの医療情報二次利用の主要パターン

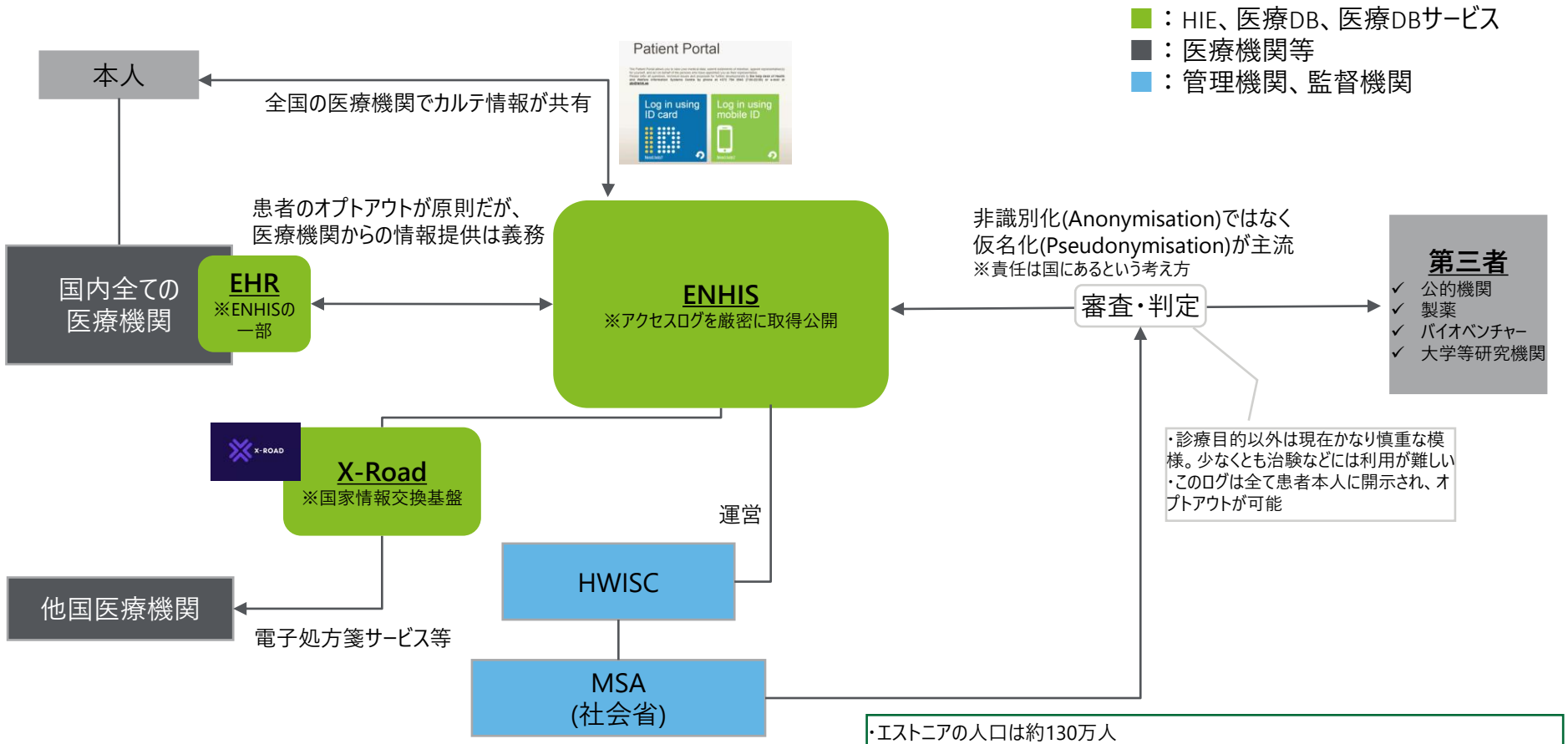
エストニアの医療情報利活用関連基本ルール
・一次利用：同意必要なし　※法的義務6(1)(c)、法的義務9(2)(i)の適用　【GDPR】　【Health Services Organization Act第4条】
・二次利用：　仮名化してあれば本人の同意不要　【PDPA第6条】
　　※Legitimate interestによる活用実態ありとの情報もあり　【GDPR】※製薬会社などが個人情報を利用する場合
・二次利用その他：ENHISへはオプトアウトでデータ収集



※研究目的等の二次利用のケースは少なく、基本仮名化データでの利用が中心
政府機関が作成するデータなのでリスクは政府にあるという認識

2008年に政府がENHISを開発して以来、国民の医療情報を集約すると共に、診療目的に限らず、周辺サービスの展開を行っている

エストニアにおける医療情報(公的DB)の流れ



- X-Road
  - 政府と民間のDBをセキュアに接続した全国的情報交換基盤(接続500機関のうち150が公的機関)
  - フィンランドとX-Road技術の活用に関して協力体制にあり、両国で電子処方箋の活用が可能
- 本人同意
  - ENHISへの登録はオプトアウトが原則であり、医療機関には情報提供義務がある
  - 公的(判断はMSAが行う)な研究以外は本人同意が基本となり、データベース(全てのログが取られている)の不正閲覧には罰則があるなど厳しい制限がある

3.3.5 オランダ 

オランダ

■ 医療制度の概要

制度	概要
医療保険	・国民皆保険であり、民間保険会社が国の規制を受けて定められた保険を提供している（保険会社は民間だが非営利運営） ・オランダの居住者及び納税者が加入を義務づけられている
医師・医療機関数	・医師数 GP(かかりつけ医)約9,000人、専門医18,000人(2013年) ・病院数 90か所、薬局 約2,000か所
国民ID	・BSN(Burger Service Number) が国民IDとして、全国民に発行されている
DigiD	・オランダ政府管轄のオンラインサービスを受ける際に使用する個人識別IDであり、上述のBSNと紐づけられている ・ポータルサイトから自身のEHR及びPHRへアクセスする際に必要

■ 健康・医療及び情報保護の法体系

➢ EU法
- ✓ General Data Protection Regulation: GDPR

➢ 国内法
- ✓ 情報保護法　The Dutch GDPR Implementation Act
- ✓ 医療法

The client right at electronic processing of data processing (WCZ)
2016年に制定された一部改正法。これにより電子ファイル作成やケアプロバイダーによるデータ交換における患者の権利を拡大するために、以下の既存法令が改正された

①Medical Treatment Contracts Act
医療機関に対する義務（医療行為記録等）、患者の権利（医療記録への情報アクセス等）等を規定

②The Citizen Service Number Use in Healthcare Act
国民IDの医療への活用や医療データの取扱いを含む患者の権利を規定

③The Healthcare Market Regulation Act (2006年制定）
②に違反した場合の罰則などが追加された

- ✓ 行動規範・規格

Code of Conduct Electronic Data Exchange in Health Care
データ保有者の権利、合意の有無、医療機関による認証や情報セキュリティ

Code of Conduct for Medical Research
医療データの研究目的利用における研究者の義務

■ EHR/PHRの取組み

➢ EHR
- LSP（ナショナルスイッチポイント）というネットワークを通して医療情報を参照
- 保健福祉スポーツ省が管轄であるが、運営は民間団体のVZVZ（ヘルスケアコミュニケーションのためのヘルスケアプロバイダー協会）
- 運営費用は、政府と保険会社が負担
- 患者データを一時的に集約し、閲覧が終わったら削除を繰り返すため、LSPにデータは集積されない
- LSPによって自身の医療情報を医療従事者間で共有する際の患者の同意はオプトイン方式であり、約1,700万人のオランダ国民のうち約1,400万人が同意
- LSP以外にも各州レベルで様々な民間のEHRが構築されており、LSPで交換できない画像や血液検査結果などの情報交換がなされている

➢ PHR
- MedMij(メッドマイ)という政府、Nictiz、患者会、民間保険会社、ヘルスケアプロバイダーで構成される組織が、PHR事業間のシステムの標準化や互換性の確保に取り組んでいる
- 患者は原則全ての情報を閲覧可能であり、誰がいつデータにアクセスしたかという情報を閲覧又は要求できる

年	近年の動向
1997年	・EHRイニシアチブ公開
2002年	・National Program for IT策定、Nictiz発足
2006年	・AORTA（医療情報交換システム）実証事業開始
2011年	・AORTA法案不成立 ※この間に、国主導での中央集権型のデータ管理を採用した点、患者情報の登録と共有をオプトアウト方式で進めようとした点が国民の反感を買い、メディアも反対の立場を取ったことから廃案につながったとされる
2012年	・LSP設立、翌2012年VZVZに譲渡
2016年	・Client Rights Law in Electronic Process of Data公布、MedMij発足

オランダでは、医療情報の取扱いに関する国内法が、医療機関と医療情報交換システムのそれぞれに規定されている

同意の法的根拠

ケース	データを提供する場合	治療、研究目的でデータを使用する場合	患者の情報を医療情報交換システムで共有する場合
関連規則	The Dutch GDPR Implementation Act	Medical Treatment Contracts Act	The Citizen Service Number Use in Healthcare Act
規制の目的	国内におけるGDPRの適用や管理体制を規定	国内の医療機関に対する義務、患者の権利を規定	医療におけるBSN(国民ID)の管理と使用可能な業務範囲等を規定
規制対象	EU域内の個人データを取り扱う者	国内の医療機関	医療情報交換システム上のデータを取り扱う者
同意の取扱い	明示的な同意	書面(Medical treatment agreement)への同意が必要	明確な同意: 同意の記録保管、有効期間の記録が求められる

GDPR第6条及び第9条の要件を満たせば同意による必要はない

公益目的の統計・科学研究では本人の同意なくデータの利用が可能

システムへ登録しているクライアントの損害を防ぐために必要な場合は第三者提供が可能

公衆衛生の分野における公益目的の統計又は科学研究が必要とされる場合や、個人情報が特定できないような形で情報開示する場合は本人の同意が不要である

研究目的の場合　Dutch Medical Treatment第458条、第467条

患者のプライバシーの保護	第458条第1項a又はbをみたす場合には、患者の同意なしに、公衆衛生の分野における統計的又は科学的研究の要請に応じて、患者情報が他者に提供される a. 許可を求めることは合理的に不可能であり、研究の実施に関して、患者のプライバシーが不相当に損なわれないという予防手段がある場合 b. 研究の性質と目的を考慮して、許可を求めることを合理的に要求することができず、かつ、care providerが、個々の自然人への遡及が合理的に防止されるような形で情報が提供されることを保証した場合	Dutch Medical Treatment 第458条第1項
公益目的	第458条第2項において、第1項に従った情報提供は、以下のaからcの全てを満たした場合にのみ可能と規定している a. 研究は公益のために資する b. 関連するデータがなければ研究を行うことはできない c. 関係する患者が情報提供に明示的に反対していない	Dutch Medical Treatment 第458条第2項
身体から分離された匿名データ	1. 身体から分離された匿名の物質(anonymous substances)及び部分は、当該人体組織の元となった患者が当該研究に反対せず、かつ必要な注意を払って研究が行われる限り、医学統計又は他の医学科学研究に使用することができる 2. 身体から分離された匿名の物質や部分を使った研究とは、研究に使用する人体組織とそこから得られるデータから、当該個人に遡ることができないことが保証されている研究を意味する。関係する患者が情報提供に明示的に反対していない	Dutch Medical Treatment 第467条 第1項、第2項

　出所：http://www.dutchcivillaw.com/civilcodebook077.htm

個人データの処理を監督する国の機関としてDutch Data Protection Authorityがあり、データ管理者はGDPRに基づきDPOを設置する必要がある

法の適切な運用を確保するための機関-オランダ

	DPA (Dutch Data Protection Authority)	DPO(Data Protection Officer)
根拠法令等	The Dutch GDPR implementation Act	GDPR
選任主体	法務安全保障大臣の指名に基づき国王が任命	データ管理者(controller)や処理者(processor)
役割の範囲	■ 個人データ処理の監督 ■ 苦情の処理 ■ 個人情報保護に関するアドバイスや情報の提供 ■ EUの他の監督機関との相互協力	■ 管理者や処理者のデータ保護方針の遵守を監視 ■ データ保護規定の義務の従業員への通知と助言 ■ データ保護の影響に関する助言 ■ パフォーマンスの監視 ■ 監督当局との協力(第39条)

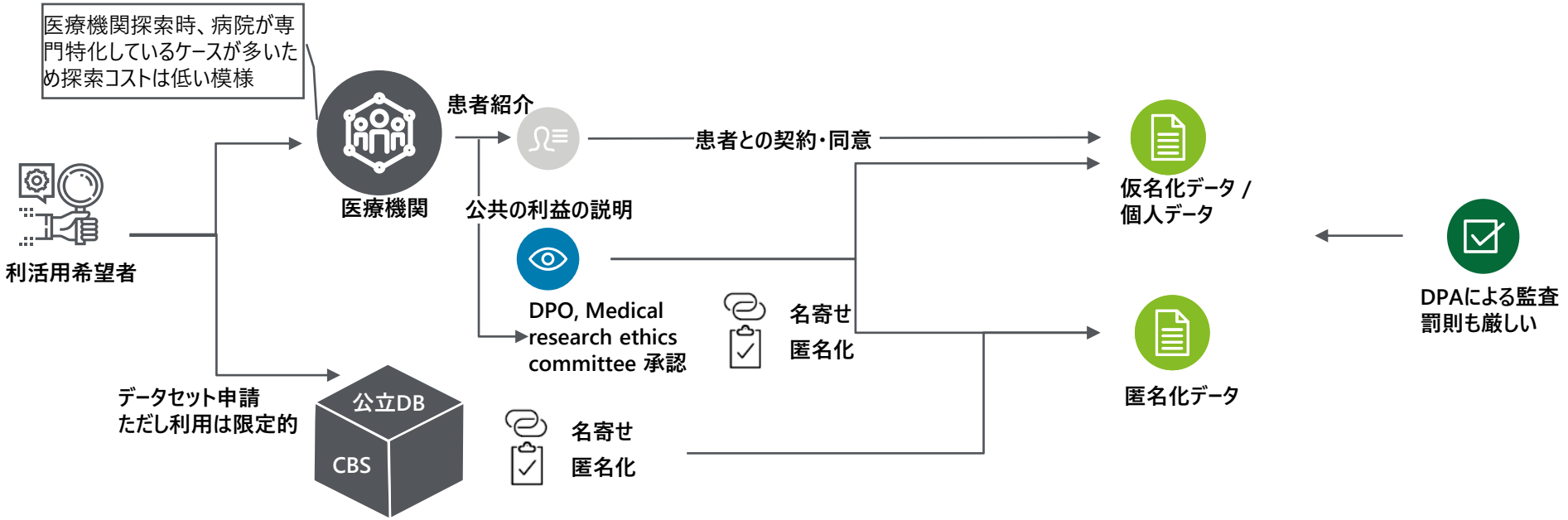
罰則・是正措置
■ The Citizen Service Number Use in Healthcare Actに対する違反：最大€50万又は売上の10％ ■ 実際の罰金事例 ➢ 2019年、個人データの取扱いに十分注意していなかった健康保険会社に€50,000の罰金を課した。DPAは健康保険会社に取扱いを改善する期間を設けたが、期間内に改善されなかった。 ➢ GDPR違反では、同じく2019年、不十分な内部管理で患者のデータを保持していた病院にDPAが€460,000の罰金を課した

出所：https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa
https://iapp.org/news/a/dutch-dpa-hits-medical-insurer-with-50k-euro-gdpr-fine/#:~:text=The%20Dutch%20data%20protection%20authority,its%20processing%20of%20personal%20data
https://blogs.dlapiper.com/privacymatters/the-netherlands-first-gdpr-imposed-eur-460000/.

オランダは、EUの中でも一次、二次利用ともに同意を重視する意向が強く、HIEもオプトインでの活用となっている

オランダの医療情報二次利用の主要パターン

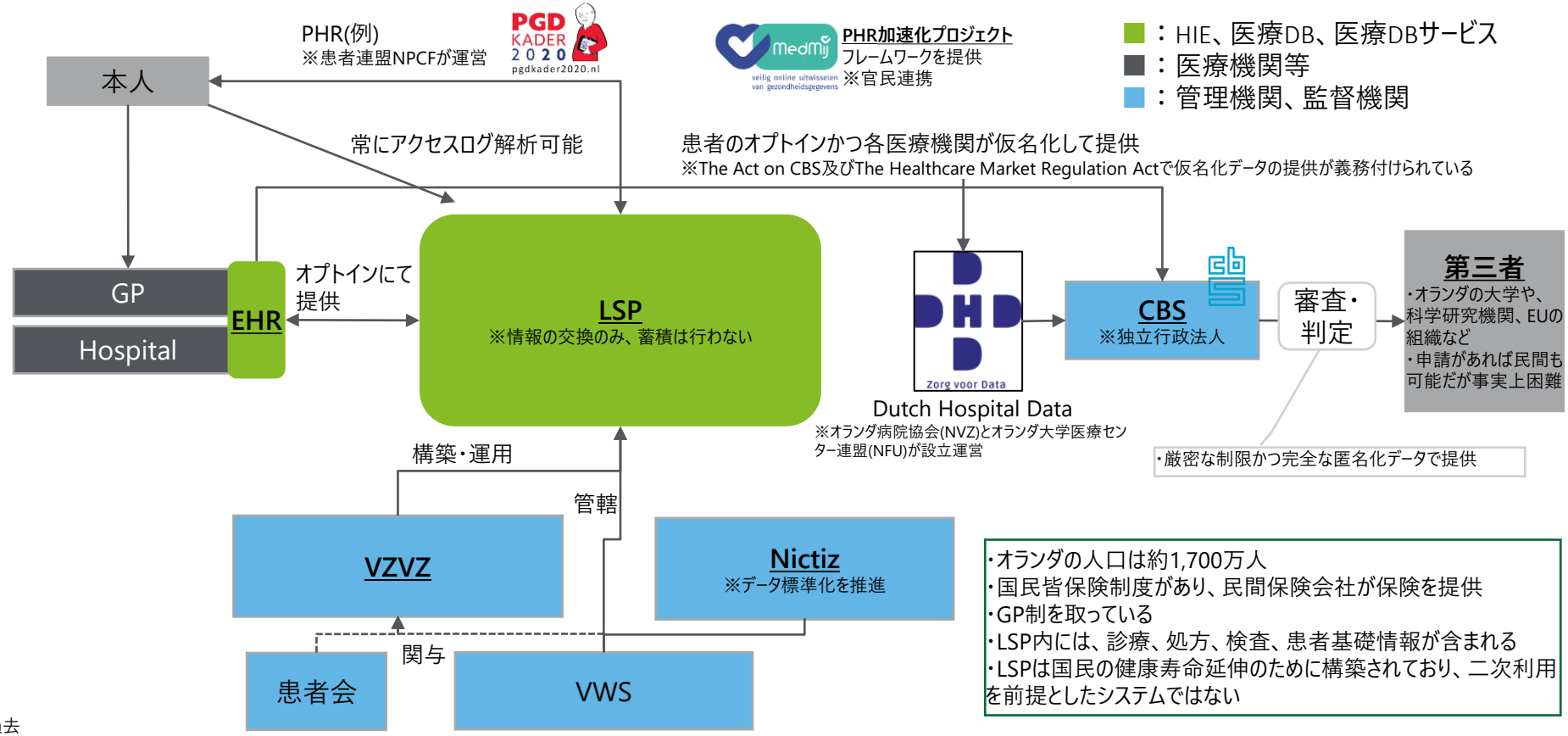
オランダの医療情報利活用関連基本ルール
・一次利用：同意が基本。※ケア目的であっても他の医療者等にデータを提供する際には同意が必要【Medical Treatment Contracts Act 450】
・二次利用：①公衆衛生目的：公共の利益6(1)(e) 、医療専門家との契約で健康産業への寄与9(2)(h)
②研究目的(公的、公的外)：同意が基本　※Medical Treatment Contracts Actにて4つの例外規程あるも適用は厳密
・二次利用その他：LSP等HIEへの同意はオプトインが基本



出所： https://english.ccmo.nl/investigators/guide-to-the-review-procedure

オランダは、民間主導でHIE（LSP)を構築し、患者約1,400万人(人口の8割)がオプトインでLSPにデータを提供しており、PHRや医療機関間の連携のために活用されている

オランダにおける医療情報の流れ



・オランダの人口は約1,700万人
・国民皆保険制度があり、民間保険会社が保険を提供
・GP制を取っている
・LSP内には、診療、処方、検査、患者基礎情報が含まれる
・LSPは国民の健康寿命延伸のために構築されており、二次利用を前提としたシステムではない

■ 過去
- Nictizで医療情報交換のために「AORTA」という標準策定し、これに基づいた仕組みを構築するも必要な法案が、国民とメディアによる強い反対により上院を通過できず、2011年に廃案。中央集権型でオプトアウト方式であったことが、不安を感じさせた模様
- この結果VZVZを中心としてLSPの構築が進んだ

※ 欧州委員会の調査によると、オランダにおいて、患者の医療情報を別の医療機関と共有する場合は、患者の同意が必要であるが、患者が別の医療機関への紹介に同意している場合には、医療情報の提供に対する同意も推定される。これを「プッシュ型（push）」という。一方、（同意の際想定していない）新たな医療機関の情報閲覧が可能な場合、患者の同意が必要となる。これを「プル型（pull）」という。
この考え方に従い、LSPのようなHIEシステムを運用する場合に170以上の同意が必要とされる法律があったが、非現実的であることから施行されておらず、現在、緊急事態の際の同意の必要性など更なる審議がなされている

 出所：:https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf

3.3.6 シンガポール 

シンガポール

■ 医療制度の概要

制度	概要
医療保険	・国民健康保険が存在せず、政府の補助金と個人負担 ・Medisave：個人負担として所得の6-8％の積立を義務化 ・Medishield Life：Medisaveでは賄えない多額・長期にわたる医療費の支出に対応するために自動的に加入 ・Medifund：低所得者向けに政府が国庫で設立している基金
医師・医療機関数	・GP診療所（一般開業医　民間施設） 1,700施設 ・ポリクリニック（公立の診療所） 20か所 ・総合病院 19か所（公立8 民間11） ・専門医療センター 8か所 ・公的なコミュニティ病院 7か所　（2018年3月時点）
国民ID	・出生時に付番される出生証明番号が、15歳到達時に国民登録番号(National Registration Identification Card: NRIC)になる
個人認証	・全ての官公庁サイトで共通の個人認証番号であるSingPass（Singapore Personal Access)を2003年に導入

■ 健康・医療及び情報保護の法体系

➢ 国内法

✓ 一般法

民間部門

Personal Data Protection Act: PDPA (個人情報保護法）

民間企業・団体(organization)を適用対象とした個人データの収集、使用、開示に関する個人情報保護法として制定(2012年)

公的部門

Statutory Bodies and Government Companies (Protection of Secrecy) Act

政府機関による統計の収集及び利用について規定

✓ ガイドライン

Advisory Guidelines for the Healthcare Sector

ヘルスケアセクターにおける個人情報取扱いについて記したガイドライン（取得に際しての利用目的の通知義務、個人情報の開示・訂正義務、情報の保護、正確性、保持に係る義務）

■ EHR/PHRの取組み

➢ EHR

- 全国をカバーするEHRとして2011年The National Electronic Health Record (NEHR)というシステムを構築
- NEHRは保健省が所有しているが、保健省傘下の企業であるMinistry of Health Holdings (MOHH)が運営に取り組んできた。その後2016年11月にMOHHの子会社Integrated Health Information System Pte Ltd (IHiS)が運営を引き継いだ
- NEHRへのデータ登録は義務化されておらず、データ提供施設数は142施設（2018年IHiS発表）。2020年2月時点、1,384施設がアクセスしている
- NEHRにはサマリー情報のみが格納され、詳細データは各医療機関に保存されている電子カルテのデータを読み出す仕組みである
- 医療従事者は専用のポータルサイトから患者情報にアクセスできるが、その際に患者の同意は不要である
- 患者はNEHRへのデータ登録をオプトアウトで拒否できる。指定されたいくつかの医療機関でオプトアウトフォームを入手して提出する。また、オプトアウトの撤回はいつでも可能。2019年7月時点、オプトアウト患者数は417名、オプトアウト撤回者は31名

➢ PHR

- 2015年10月、Health Hubという患者向けポータル（モバイルアプリ）を開始
- 保健省、Health Promotion Boardが提案し、IHiSと公立医療機関が支援
- 2018年7月までにアプリは356,000回ダウンロード、27万人が利用登録を実施

■ 医療情報漏洩インシデント

- 2018年7月20日、保健省管轄の公的医療機関SingHealthが不正アクセスを受け、2015年5月～2018年7月にかけて患者に関する個人情報150万件が流出したと発表。約16万件については氏名、住所、生年月日、電話番号、人種、調剤情報も流出
- 2019年1月、保健省はHIV検査陽性者1万4,200 人の氏名や連絡先がインターネット上に流出していたと発表

- 2019年3月に首相の諮問機関としてデータセキュリティ検討委員会を設置し、公的セクター94機関の300超の情報システムのデータ管理状況を調査し、2019年11月に提出された報告書の中で情報漏洩防止策を提言している

シンガポールの個人情報保護の一般法であるPDPA2012は2014年に施行されて以来、2021年2月に改正法が施行された

シンガポールにおける個人情報保護と利活用の歴史

1973年	Statistics Act施行
1983年	Statutory Bodies and Government Companies (Protection of Secrecy)Act施行
	法定機関や政府系企業のメンバー又は旧メンバーが役職を理由に入手した機密文書や情報の開示を禁止
2009年4月	EHRの開発開始
2012年	Personal Data Protection Act 2012 (PDPA2012)を議会承認
2013年1月	PDPC(個人情報保護委員会)の設置
2014年	PDPAの施行
2015年	患者向けポータルサイト、HealthHubの使用開始
2018年7月	公的医療機関「SingHealth」の医療情報インシデントの発表
	SingHealthが不正アクセスを受け、2015年から2018年にかけて患者の個人情報150万件が流出
2019年1月	HIV検査で陽性となった1万4,200人の氏名や連絡先等の情報が流出
2019年3月	公的セクターデータセキュリティ検討委員会を設置
2020年11月	PDPA改正法を議会承認
2021年2月	PDPA改正法施行

出所：https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
一般データ保護規則（GDPR）の前文、JETRO「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）

シンガポールの個人情報保護法(PDPA)では、個人情報の収集・使用・開示にかかる同意について、「みなし同意」や「通知によるみなし同意」を認めている

同意の法的根拠

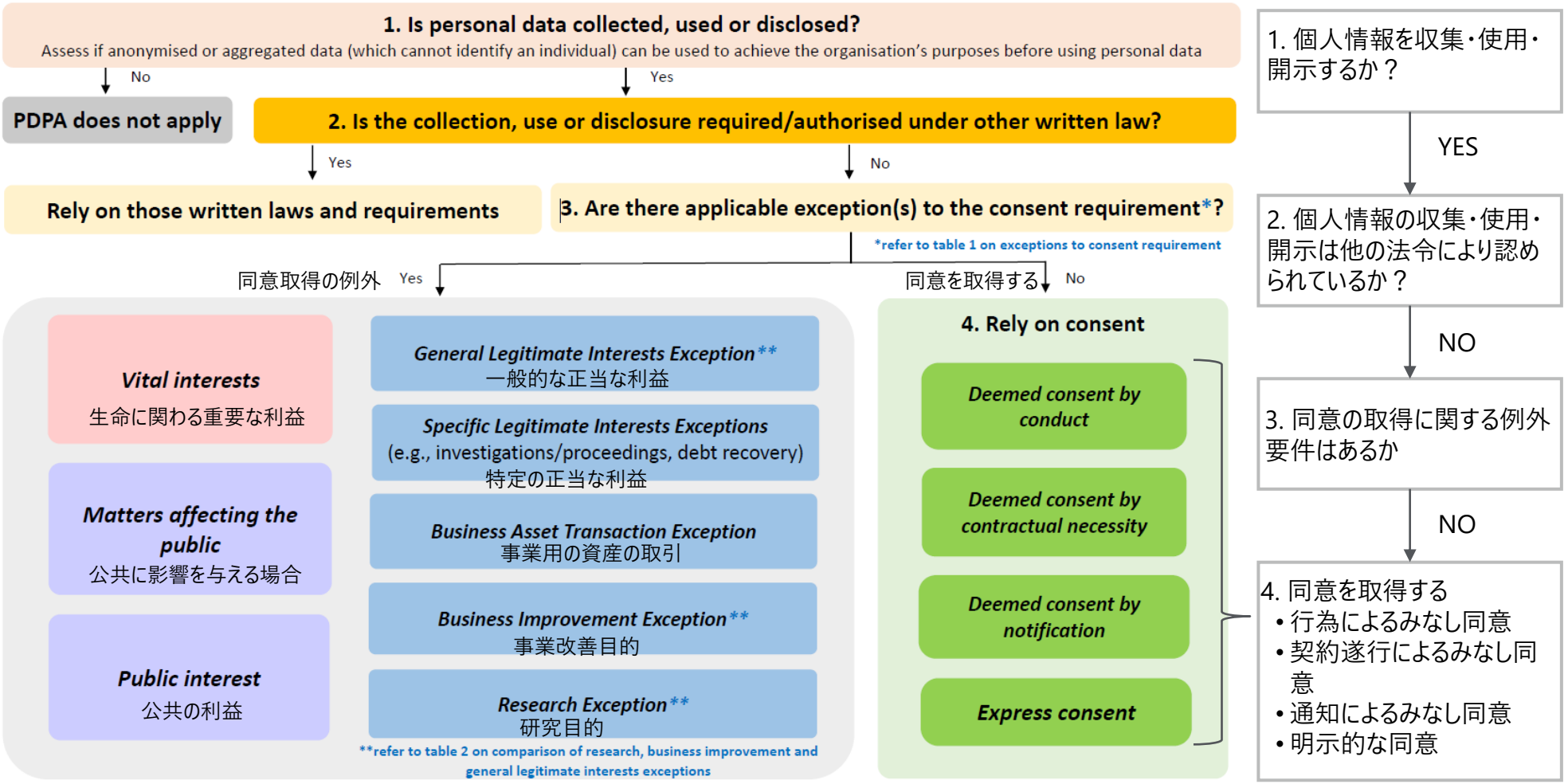
同意に関する規制	内容
個人情報の取得場面	治療を受ける場合、研究目的でデータを提供する場合のいずれも同様
関連規則	Personal Data Protection Act 2012 Advisory Guidelines for the Healthcare Sector (PDPAの解釈指針として、保健省とPDPC※がガイドラインを提示している)
規制の性質	個人情報を保護するための国内法
規制対象	シンガポールで活動するすべてのOrganisation(事業者)
同意の種類	• 同意(Consent) • みなし同意(Deemed consent) • 通知によるみなし同意（Deemed consent by notification)⇒オプトアウト

※PDPC：PDPAの監督機関（個人情報保護委員会）

出所：https://sso.agc.gov.sg/Act/PDPA2012?ValidDate=20210201
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf

匿名化、又は個人を識別できないように集約したデータでは目的が達成されず、個人情報の収集・使用・開示が必要な場合に、取得すべき同意の種類と例外要件が示されている

同意の取得又は同意の適用除外に係るフローチャート



出所：https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-A--PDPAs-Framework-for-the-Collection-Use-and-Disclosure-of-Personal-Data-1-Feb-2021.pdf?la=en

個人情報の収集・使用・開示に関する目的を本人に通知した上で同意をとることが原則であるが、情報の使用・開示が合理的である範囲において「みなし同意」が認められる

一定の目的で本人が自発的に個人情報を提供したと認められ、特定の機関との契約締結及び当該機関による契約の履行のために合理的に必要となる場合はみなし同意(Deemed Consent)が認められる

医療機関でのみなし同意の例 (PDPA第15条)

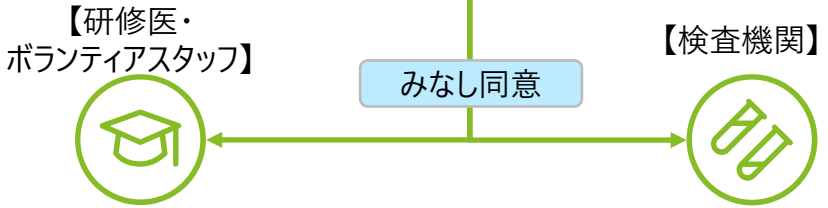
患者が受診受付票に氏名、ID番号、電話番号等の個人情報を記載して提出する。この行為は自発的(Voluntary)に個人情報を提供したと捉えられる

受診の結果、医師は検査や他の医療機関への紹介を検討。本人に確認の上、該当する機関に連絡を取る。後にトラブルになるケースに備え、本人の承諾を口頭でとった旨を記録に残しておくと良い

医療機関Aの医師から患者の紹介を受け、医療サービスや介護サービスを提供する。なお、患者本人が紹介状を持参してきた場合は、みなし同意ではなく、本人が個人情報を開示していると捉えられる

以下の場合は「みなし同意」は認められず、別途同意の取得が必要

- 研修医の教材開発のために匿名化されていない患者情報を使用する
- 患者のマネジドケアプロバイダーへの受診状況等の情報開示
- マーケティング目的での患者情報の利用



医療機関A内の、患者のケアに係る活動については、みなし同意が認められる

医療機関Aと契約を締結している検査機関に患者情報を提供する際も、みなし同意が認められる

出所：https://sso.agc.gov.sg/Act/PDPA2012?ValidDate=20210201
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf

個人情報の収集・使用・開始に関する通知に対して、本人が指定された期限までに同意に反対の意思を示さない場合も「みなし同意」と認められる

医療機関が個人に対して診療目的による個人情報の収集・使用・開示を通知し、個人がこれに同意しない旨を述べるべき期間に同意しない旨を述べなかった場合、診療目的での当該個人情報の収集・使用・開示に同意したものとみなされる

通知によるみなし同意(オプトアウト)を適用する際の措置 (PDPA第15条A)

1. 影響の評価

- 組織は、予定している個人情報の収集・使用・開示について、個人に対する悪影響がないかを評価する
  - 個人情報の収集・使用・開示により、個人に与える可能性がある悪影響を識別する
  - 悪影響を除く、悪影響が発生する可能性を軽減する又は悪影響を軽減する措置をとる

2. 通知

- 以下の情報について、個人の注意を喚起する適切な措置を行う
  - 組織の個人情報の収集・使用・開示に関する組織の意思を示す
  - 個人情報の収集・使用・開示の目的を示す
  - 個人が個人情報の収集・使用・開示に同意しない旨を知らせることができる合理的な期間を設ける

3. その他

- その他、法令の要求事項を満たす

4. 本人の否定の有無

- 組織が上記の要件を満たした上で、通知期間の期限内に、本人から個人情報の収集・使用・開示に同意しないという意思表示がない場合は、本人が「みなし同意」を与えたと認められる
- ただし、PDPC(個人情報保護委員会)は、オプトアウトの意思表示がないことが直ちに同意とみなされるわけではなく、個別の事情を踏まえる必要があるとしている

PDPCは通知によるみなし同意に依拠して良いかを評価するチェックリストを作成し、ガイドラインと共に公表している

出所：https://sso.agc.gov.sg/Act/PDPA2012?ValidDate=20210201
https://www.pdpc.gov.sg/FAQ-Listing?persona=dp-professional&topic=collection--use-and-disclosure&page=1
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-B--Assessment-Checklist-for-Deemed-Consent-by-Notification-1-Feb-2021.pdf?la=en

生命に関わる場合や、個人の利益を上回る正当な利益がある場合、公益、研究目的において、本人の同意が不要な場合が認められている

同意が不要な場合 (PDPA・Schedule1-3)

個人の重要な利益になる場合	■ 適時の同意取得が困難又は同意拒絶が合理的に予想困難な場合、生命又は身体の安全のために緊急の必要性が認められる場合等、個人の利益を保護すべき場合
公共に影響を与える場合	■ 公に取得可能な個人情報の収集・使用・開示で、①国家の利益となる個人情報の場合、②芸術と文学の目的に限定した場合、③過度に機微でない個人情報のアーカイブや歴史的な目的の場合、④報道目的の場合
正当な利益	■ 組織が個人に与える悪影響を評価し、悪影響を最小限にした上で、①組織や他人の利益が個人への影響に勝る場合、②調査や裁判で必要な場合、③個人又は組織による負債を回収する場合や組織による負債を個人に支払う場合、④信用調査所のクレジットレポート（信用状況報告）を準備する場合、⑤雇用、事業、職業に関する文書作成目的の場合 等
事業用資産の取引	■ X社とY社の間で事業用資産の取引を行う場合に含まれる個人情報
事業改善目的	■ 製品やサービス向上のために関与する目的で、対象となる企業の顧客情報を別の企業が使用する場合
公的利益	■ 政策の策定目的で、①現在又は過去の学生の個人情報を教育機関に開示する場合、②現在又は過去の患者の情報を医療機関やHealth Service Act2020に基づいてライセンスを取得している者へ開示する場合
研究	■ 歴史的又は統計的研究目的で、①個人情報が個人識別可能な形で使用されないと研究目的が合理的に達成されない場合、②研究目的の個人情報の利用が明らかに公共の利益に資する場合、③研究結果が個人に影響を与える決定に使用されない場合、④研究結果を公表する際に個人が特定されない形で公表する場合

出所：https://sso.agc.gov.sg/Act/PDPA2012?ValidDate=20210201#Sc1-

PDPAに匿名化に関する規定はないが、個人情報保護委員会(PDPC)が個人情報の匿名加工に関するガイドラインを公表している

匿名加工と再識別化のリスク評価

- 匿名化の定義
  - PDPAでは匿名化に該当する規定が無く、同法のガイドラインであるAdvisory Guidelinesにおいて「PDPAで定義されている"Personal Data"の文脈で理解する必要がある」と説明されている
  - Advisory Guidelinesによると、匿名化(Anonymisation)とは個人データを個人を特定できないデータに変換するプロセスを指す。当データは、データ自体・他のデータを組み合わせることによっても、個人を再特定(re-identification)できないものである
- 匿名化要件
  - PDPAでは匿名化の技術的手法を定めておらず、PDPCの公表するAdvisory Guidelinesを参考に右表のような匿名化加工をする
- 匿名加工の主体
  - Advisory Guidelines 3.11の匿名化の注意事項説明においてOrganisationsが匿名化をすることを想定しているが、匿名加工をする主体についての詳細説明はない
- 評価に関する規定
  - Advisory Guidelinesでは、再識別のリスクを評価することで匿名化されているかを判断することを推奨している
  - Advisory Guidelines 3.15において、Organisationsが再識別リスクの評価を行うことを想定している
  - 評価方法として、英国のICOが公表している"Code of Practice Anonymisation: Managing Data Protection Risk Code of Practice"で示されているテストを参考にしている

ガイドラインによる匿名化手法の例示

手法	具体例
仮名化	個人の名前をランダムに生成した参照番号に置き換える
集合化	個人8人の異なる年齢を、8人の合計値だけに置き換えて表示する
数値の置き換え	15,18,20歳の個人がいた場合、全てその平均値の17歳に置き換えて表示する
不要識別子の除外	個人情報のうち、「民族」など目的上不要と考えられる識別子を除外
リコーディング及び一般化	「中学二年生」を「中学生」に置き換える
シャッフリング	顧客の名字を別物と置き換える
マスキング	'S1234567A'を'#####567A'に置き換える

個人の再識別リスクの評価のテスト

テスト	説明
Motivated Intruder Test	個人の再識別を試みる人物が、その対象となる匿名データと他の情報源を組み合わせることによって個人を再識別ができないか判断するテスト 具体的には、ウェブ、SNS、図書館などの情報を収集して個人の特定を試みる

出所:：https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-9-Oct-2019.pdf?la=en

監督機関として、個人情報保護委員会であるPersonal Data Protection Commission (PDPC)があり、各組織でもデータ保護責任者を設置している

法の適切な運用を確保するための機関

	個人情報保護委員会 PDPC　(Personal Data Protection Commission)	データ保護オフィサー Data Protection Officer (DPO)
根拠法令等	PDPA第50条	PDPA第11条(3)
選任主体	政府	組織（organization）
役割と義務	■ データ処理問題におけるシンガポール政府の代表 ■ 組織がPDPAを遵守しているかの調査の実施と措置の指示 ■ 苦情に基づく調査 ■ PDPA遵守のためのガイドラインの作成 ■ PDPAに基づき任命されるThe Data Protection Advisory CommitteeがPDPCに個人データ保護のフレームワークのレビューや管理に関する問題についてアドバイスを行う	■ 個人情報管理体制の確認 ■ 個人情報取扱いについての情報管理規則の作成・改正・従業員への周知 ■ リスク及び対策の検討 ■ 社外からの問合せ対応や苦情に対応する体制の整備 ■ データ漏洩時の通知義務 ➢ 通知可能であるかを評価する義務があり、通知可能な場合に委員会と影響を受ける個人に通知する義務がある

罰則・是正措置

■ PDPAに違反した場合：SGD10,000以下の罰金又は３年以下の懲役、又はその両方
➢ 違反を続ける場合には, 毎日又は有罪判決の後に違反が続いた期間、追加でSGD1,000以下の罰金

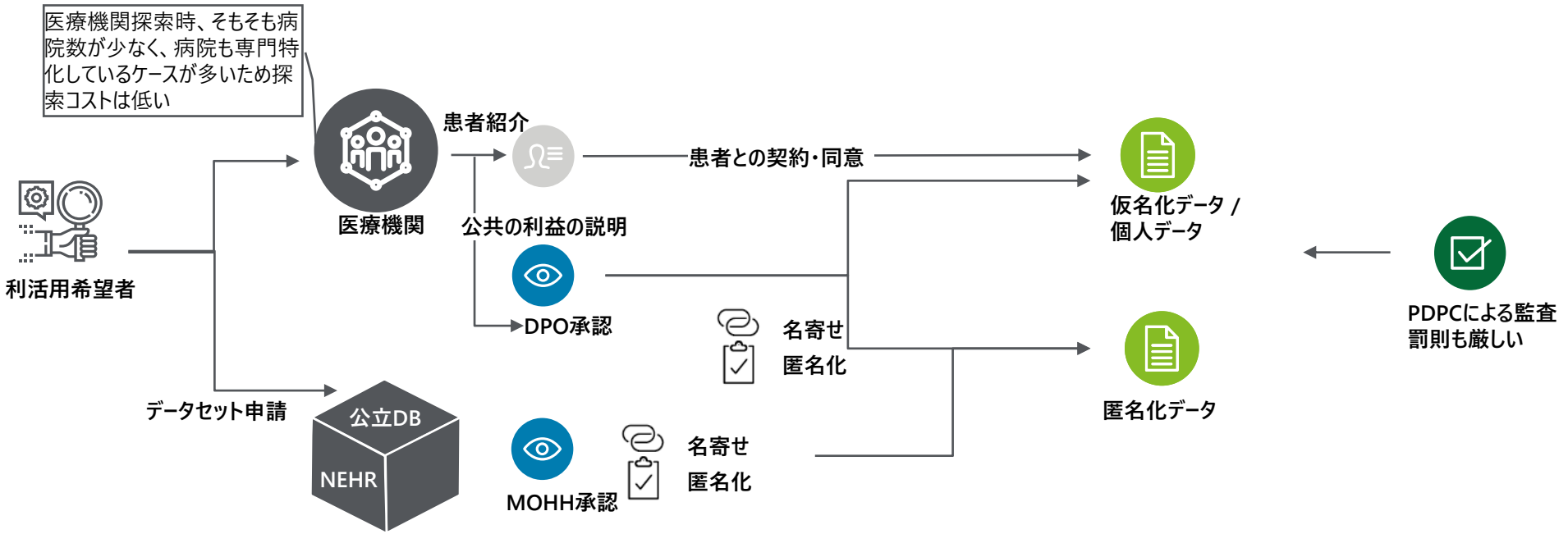
■ 実際の罰金事例
ヘルスケア関連の違反事例は5件報告されており、うち3件に罰金が課されている。罰金額は、サイバー攻撃により約150万人（2015～2018年）の患者データと約16万人（2019年）の外来患者の処方記録を流出させたことにより、関与した2つの組織それぞれにSGD250,000（前者の組織）とSGD750,000（後者の組織）が課された

出所：https://www.pdpc.gov.sg/All-Commissions-Decisions?keyword=&industry=healthcare&nature=all&decision=all&penalty=all&page=1
https://www.pdpc.gov.sg/Who-We-Are/Advisory-Committee

シンガポールでは、国民の健康増進のために公的DB（NEHR）の構築に熱心だが、研究目的等二次利用への活用に関しては、現在様々な議論が行われている

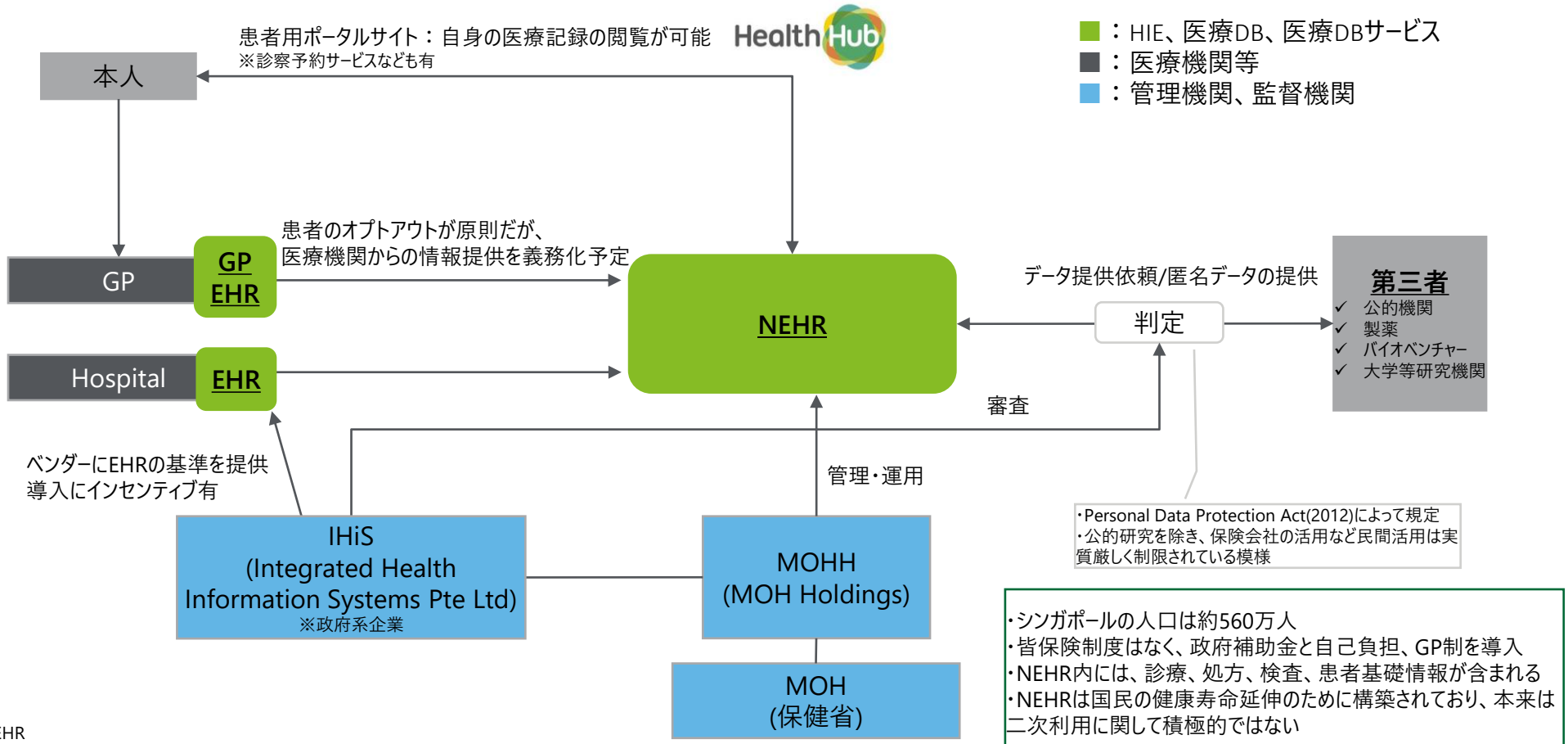
医療情報二次利用の主要パターン

シンガポールの医療情報利活用関連基本ルール
・一次利用：同意必要なし、みなし同意が成立　【Personal Data Protection Act 2012】
・二次利用：同意が基本　　【Personal Data Protection Act 2012】
・二次利用その他：NEHRへはオプトアウトでデータ収集



政府主導でNational EHRを開発し、政府として段階的に情報の集約化を進めている最中であり、患者向けポータルサイトの運用に力を入れている

シンガポールにおける医療情報の流れ



■ NEHR
- 2020年時点で、国立病院はほぼ100％でEHRの導入が進んでいる
- GPクリニック、及びプライベート医療機関にはGP EMRの導入が進められているがまだ6割程度の導入にとどまっている
- NEHRにはオプトアウトでデータが集まるが、自国民に限らずEHR導入医療機関の全データが収集されている

■ サイバーアタックインシデント(2018)
- 2015年5月1日～2018年7月4日にSingHealthが運営する専門外来医院や総合病院を訪れた患者150万人の個人情報にアクセスされ、コピーされた。流出したデータには、患者の氏名、国民登録番号、住所、性別、人種、生年月日などが含まれていた
- 2019年3月には献血者約80万人分の個人情報流出が明らかになるなどの事件が相次いだ。これを受け、リー首相は3月31日、公共機関が管理する個人情報保護のあり方を見直すため、「公共セクター・データセキュリティー再検討委員会」を設置した

3.4 ヒアリングによる各国の実態調査

米国、英国、エストニア、オランダ、シンガポールにおける医療情報の保護と利活用の実態に関して文献調査で不明であった点について海外の個人情報専門家に確認した

運用実態に関するヒアリング質問項目

大項目	No	詳細項目	質問内容
医療情報の利活用	Q1	医療情報の収集手段	• 本人の同意に依拠しない情報収集手段はあるか • 研究目的で医療情報を収集する際、主にどのような手段が採用されているか
	Q2	データベースの活用	• 医療情報が集約されているデータベースがあるか • それらのデータベースはどのように活用されているか
	Q3	研究主体別の制限	• 研究目的で医療情報を活用する場合、公的機関と民間組織との間で制限の違いがあるか
	Q4	匿名加工	• 非識別化・匿名化に関するガイドラインや、非識別化・匿名化された状態に関するクライテリアは存在するか • 匿名加工における責任者は誰であり、再識別化のリスク評価はどのように行われているか
個人情報の保護	Q5	個人の権利	• 同意の撤回など、個人の権利はどのように尊重されているか
	Q6	倫理審査委員会	• 倫理審査委員会は医療情報の保護と利活用の観点で研究内容等の審査を行っているか • 倫理審査委員会の構成員に個人情報保護に関する専門家が含まれているか
	Q7	監督機関	• 個人情報保護委員会のような政府機関はどのように機能を果たしているか
個人情報の保護と利活用のバランス	Q8	情報保護と利活用の現状と今後の展望	• 医療情報の保護と利活用に向け、実態とそれにまつわる政策動向がどうあるか

注）回答内容には個人の見解が含まれる場合もある

GDPRでは個人情報を取り扱う法的根拠に同意以外の根拠も定められているが、研究では「同意」を法的根拠とする傾向が強い。また匿名化の基準も米国以外は曖昧である

ヒアリング結果サマリー①

	1. 医療情報収集の法的根拠	2. データベースの活用	3. 研究主体別の制限	4. 匿名加工の実態	5. 個人の権利の執行
米国 (HIPAA)	Limited Data Setの利用、または De-identification (非識別化)	医療機関のHIEへの参加を政府が推奨し、研究データへのアクセス向上を目指している	なし	セーフハーバー方式であれば、個人の再識別がされても匿名加工の責任を問われない	常に情報開示を求めることができる。同意の撤回もいつでも可能
英国 (UK GDPR、DPA)	Consent （同意）	いくつかデータベースが存在するが、政府は連携を推奨	なし	ガイドラインはあるが、厳格な規則が定まっておらず、匿名加工は各実施機関に委ねられている	データ主体の情報を直接収集するわけではない場合は、データ収集機関はデータ主体に通知する努力が必要
エストニア (GDPR、PDPA)	Consent（同意） または Legitimate Interest （正当な利益）	ENHISを社会省が管轄。研究者も申請によりアクセス可能	なし	ENHIS上で仮名化されているため、加工は国の責任であるとの認識	本人がENHIS上で研究者からのアクセスを制限することが可能
オランダ (Dutch GDPR Implementation Act等)	Consent （同意）	データベースは存在するが研究目的への活用に十分なものではない	なし	完全匿名化と言える技術はないので、匿名化には触れないようにしている	権利はあり、十分な説明を受け、同意をした上で研究に参加しているので同意を撤回するケースはほぼ見られない
シンガポール (PDPA2012)	Consent （同意）	研究者もNEHRのデータの活用が可能	なし	ガイダンスはあるが匿名加の状態の基準はあいまい	公益目的であっても個人の消去権が勝る。2021年2月の法改正でデータポータビリティ権を導入

諸外国ではデータ主体が個人の権利を主張する傾向が高まってきており、それに対してデータ保護当局が調査や監査を実施して、個人情報を保護しながら利活用を推進している

ヒアリング結果サマリー②

	6. 倫理委員会の構成や審査内容	7. 監督機関の活動	8. 医療情報保護と利活用のバランス	9. 医療情報の利活用に向けた政策動向
米国 (HIPAA)	本人の同意なく研究を実施するために医療情報を第三者提供する場合は、IRBまたはプライバシー委員会が審理	OCRの活動内容は過去10年で変化している。OCRは監査を実施しているが、対象の選定基準は非公表	医療分野では個人の権利がより頻繁に請求されるようになってきている	HIPAAによる制約を受けない医療情報や個人情報の制約に向けた動きが活発である
英国 (UK GDPR、DPA)	倫理研究者、統計学者、データサイエンティスト、弁護士、臨床の専門家等で委員会を構成することが多い	ICOがNHSの部署や警察等の公的機関の監査を実施。民間機関に対しても任意で監査を実施	データ主体が権利主張するケースが増加しているため、各組織はDPOを雇用・設置し、アカウンタビリティを強化	英国では医療情報の利活用が必ずしも進んでいるとは言えないため、課題は山積している
エストニア (GDPR、PDPA)	研究者がENHISのデータを利用する場合はENHISの倫理委員会に申請。研究内容そのものについては、各研究分野の倫理委員会が審査	DPI(Data Protection Inspectorate)が、特に焦点を当てた分野で調査や監査をすることがある	患者は医療サービス提供者以外に対して、自身の医療情報へのアクセスを禁止する権利を持つ	eHealth 戦略計画2020で2025年までのビジョンを掲げ、ENHISに集約されたデータの更なる利活用を計画
オランダ (Dutch GDPR Implementation Act等)	Ethics Review Committeeを医療機関内に設置。Ethics Review Committeeの構成メンバーには法務と倫理の専門家を含む	DPA(Dutch Data Protection Authority)に組織や個人が直接苦情を訴えることが可能である。当局の活動は活発であり厳格な調査を実施	DPAは医療情報に対して厳格な姿勢を示しつつも、リスク評価をした上で医療情報の活用に投資をしていく考え	データエコノミーを推進する動きもある
シンガポール (PDPA2012)	医療機関が倫理審査委員会(IRB)を設置。構成員は科学者や非科学者を含む	PDPC(個人情報保護委員会)は特に営利目的の分野で監査や調査を実施	本人の権利に関する対応と監査により、規則を遵守するような体制を整備	2021年2月にPDPAの法改正

米国の研究では主にリミテッドデータセットや非識別化されたデータを活用している。リミテッドデータセットは、CEとのBusiness Associates合意書を締結することで利用可能になる

研究における医療情報の保護と利活用の実態（米国）

大項目	No	詳細項目	回答内容
医療情報の利活用	A1	医療情報の収集手段	• 本人の承認なく医療情報を使用・開示できる手段として①非識別化、②IRBやプライバシー委員会の書面による承認、③データ利用契約締結によるリミテッドデータセットの利用といった方法があるが、それら採用実態は以下の通り（ヒアリング回答者の業務上の印象である） ✓グループ病院内での本人の治療目的外のデータ利活用　①15％、②25％、③60％ ✓製薬会社やIT企業のデータ利活用　①50％、②20％、③30％
	A2	データベースの活用	• 多くの製薬会社や医療機器メーカーは自身が収集した研究データや第三者が収集してまとめて非識別化したデータを利用している • Health Information Exchanges (HIE)に参加することを促し、組織をまたいで患者を治療する能力の強化、治療結果（アウトカム）の向上、研究データへのアクセスの向上を目指している
	A3	研究主体別の制限	• 公的機関と民間で異なる制限は存在しない。ある組織が研究目的で本人の同意を得て収集した情報を他の組織と共同で活用することは求められない • しかし、最近のいくつかの医療機関では研究目的のために患者情報を非識別化して集約する動きがある。これは非識別化データを研究目的で販売し、新たな収入源とするためであり、研究主体の制限があるからではない
	A4	匿名加工	• HIPAAで示された専門家の統計分析による非識別化の方法と18の識別子を除外するセーフハーバー方式がある • 組織がセーフハーバー方式を採用した場合、個人が再識別化されても責任を問われない • 統計的な匿名加工を行い個人が再識別化された場合は、組織（または統計分析を実施した専門家）は採用した手法が健全であったことを示すことが求められる。この場合、法的審理により裁決をくだされるケースになり得る

医療分野では個人の権利の主張が強くなってきている傾向がある。また非医療情報の保護法令の制定に向けた動きも活発になっている

研究における医療情報の保護と利活用の実態（米国）

大項目	No	詳細項目	回答内容
個人情報の保護	A5	個人の権利	• データ主体は、いつでも同意を撤回できる。これは被験者となった治験の同意の撤回も、それ以外の研究活動への利活用への同意の撤回も含む • HIPAAに基づいて医療情報を利用・開示している組織は、医療情報が研究目的で活用されることについて本人に通知し、本人が知る権利を有することを知らせる必要がある • 個人は研究目的で情報を使用しないように求めることも可能であり、また、研究目的で活用された情報内容について開示要求することもできる。例えば、HIPAAに基づき本人の同意なく研究を行った場合、本人は情報開示の説明を求める権利(Right to an accounting of disclosures)を有する。具体的には誰が自身のどの情報に、いつ何の目的でアクセスしたかについての説明を求めることができる
	A6	倫理審査委員会	• HIPAAに基づいて医療情報を第三者提供する場合、ビジネスアソシエイツ合意書(BAA)により制約を受ける。BAAを締結する前の審査はないが、ビジネスアソシエイツは合意書を遵守する責任がある • 本人の同意なく研究を実施するために医療情報を第三者提供する場合は、IRBまたはプライバシー委員会がデータ提供について審理する。これらの構成員は医療機関によって直接招集される場合もあれば、提携組織から招集される場合もある（例：大学附属病院は大学の関係者からIRBを組成する場合など）
	A7	監督機関	• 保健福祉省(HHS)の人権保護局(OCR)がHIPAAの執行の監督機関であり、活動内容は過去10年で変化している。OCRは監査を実施しているが、対象の選定基準は公表されていない
個人情報の保護と利活用のバランス	A8	情報保護と利活用の現状と今後の展望	• 個人の権利の執行はライフサイエンスや保険セクターではほとんど発生しないが、医療分野ではより頻繁に執行されるようになってきている • HIPAAの執行は厳格である • HIPAAが適用されない領域の医療情報については、個人情報の制約に向けた動きが活発である。カリフォルニア州は非医療情報の保護を規定した最初の法律である「カリフォルニア州消費者プライバシー法」を制定した。他の州のこれに倣う動きがある

英国の研究では、インフォームドコンセントの取得と同時に、データ処理に係る同意を取得し、それを個人情報の取扱いに係る法的根拠とする傾向が強い

研究における医療情報の保護と利活用の実態（英国）

大項目	No	詳細項目	回答内容
医療情報の利活用	A1	医療情報の収集手段	• 同意の話をする際はインフォームドコンセントとデータ処理に関する同意の違いを明確にすべきである • データ処理では同意の取得、正当な利益等の法的根拠等に基づいて医療情報の収集が行われるが、実際にはほとんどの機関が同意の取得による情報収集を行っている • 科学的研究目的の場合はいずれにせよインフォームドコンセントによる情報収集を行わなければならないため、データ処理に関する同意も合わせて取得するのことが最も主流な法的根拠となっている • 「正当な利益(Legitimate Interest)」も法的根拠となり得るが実際にはほとんど使われていない。正当な利益を示すまでのテストが複雑なこと、未だに体系化されていない根拠であること、継続性が難しいことが理由として挙げられる • COVID-19に関する研究の場合は、公益目的としてデータ処理が正当化されている • 同意取得では目的の特定等の要件は定められているものの、研究目的での同意取得は比較的柔軟性がある
	A2	データベースの活用	• 目的別に様々なデータベースが存在しているが、NHSは組織間でのデータ共有を推薦している • 腫瘍学・遺伝子学のデータベースのリアルワールドデータは医療研究における需要が増している • ある特定の疾病以外では統合されたデータベースはなく、公的機関と民間機関で分離しているが、NHSと民間機関の連携などは進めている
	A3	研究主体別の制限	• 日本のように学術研究機関との共同研究であるべきといった制限はないが、公的資金と民間資金の違いはある • 民間研究機関は独自で研究を進めることも可能だが、公的機関と共同研究を行うことにより、研究資金をより多く得られる。政府は公的機関と民間機関の連携を推奨している
	A4	匿名加工	• ICOが匿名化に関するガイドラインを発表しているが、厳格な規則が定まっている訳ではなく、匿名化手法は各実施機関に委ねられており、実質的に基準はない状態である • 遺伝子データ等、個人情報に該当するデータの種類も増加しているため、それに伴ってガイドラインも追加されていくことが予想される • 真の匿名化を定義することは困難である中で、匿名加工の責任はデータ管理者が負う。データ管理者は定期的に、データが匿名化されているかリスク評価をし、匿名化の状態を確認する義務がある

ICOによる個人情報保護のコンプライアンスに係る外部監査もあるが、データを取り扱う各組織で自主的に内部監査を行いアカウンタビリティやコンプライアンスを外部に示す動きがある

研究における医療情報の保護と利活用の実態（英国）

大項目	No	詳細項目	回答内容
個人情報の保護	A5	個人の権利	• 説明を受ける権利（Right to be informed) について、データ主体の情報を直接収集しない場合は、データ収集機関はデータ主体に通知するよう努めなければならない • データのアクセス権や消去権は、医療に関するデータを研究目的で処理する場合は特別扱いされるため、これらの権利の請求に応じる必要はない • GDPR第89条でも同様に、科学的研究目的であれば権利の請求対象外と規定している
	A6	倫理審査委員会	• 倫理委員会、研究倫理委員会といった組織が、研究目的等を審査する。 • 委員会を構成するのは倫理研究者、統計学者、データサイエンティスト、弁護士、臨床の専門家等である。データ保護専門家を含むことは必須とはされていない
	A7	監督機関	• ICOは小さな組織だが、ガイダンスの作成、問合せ対応、公的機関への監査等の業務を行っている • ICOは制裁を直ちに課すことよりも、個人情報保護に関する支援を提供している • ICOはNHSの部署や警察等の公的機関の監査を実施し、政府の活動にも意見を行っている。民間機関に対しても任意で監査を実施しており、指摘や忠告を行っている • また企業のアカウンタビリティのために製薬企業などは内部監査も実施している。データ保護は重要項目として捉えられており、コンプライアンスについて自ら示す努力をしている
個人情報の保護と利活用のバランス	A8	情報保護と利活用の現状と今後の展望	• データ主体が意見（権利の主張等）を述べるケースが増えてきたため、各組織は法律を遵守していることを示すためにDPOを雇用・設置し、アカウンタビリティを強化している。各組織でコンプライアンスを確実にするための意識改革が進んでいる • 英国では医療情報の利活用が必ずしも進んでいるとは限らないため、課題は山積している

エストニアの研究では、Legitimate Interestや同意を法的根拠とする場合がある。国がENHISデータを仮名化しており、オプトアウトによるデータ利用制限が可能である

研究における医療情報の保護と利活用の実態（エストニア）

大項目	No	詳細項目	回答内容
医療情報の利活用	A1	医療情報の収集手段	• 研究においては同意の取得か正当な利益(legitimate interests)を法的根拠として、医療情報の収集を行っている • 同意を取得しない場合は、仮名化(Pseudonymised format)またはそれに匹敵するレベルの保護措置をとる • 次の3つの条件を満たした場合も、同意なしでの個人情報の利活用が認められる ①個人を識別するデータを除外するとデータの活用の目的が達成されない ②科学的・歴史的研究または公的な統計の作成による「公益目的」が上回る ③データ主体の義務や権利が、データの利用によって変わることがない
	A2	データベースの活用	• 国家のENHISがあり、3種のレベルのデータに分類されている。レベル１とレベル2は治療に関するデータであり、レベル３は研究目的に使用可能な仮名加工データである • データ主体はデータベースへのアクセスが可能であり、同意を与えることもデータベース上で可能である • 警察や州政府もデータベースにアクセス可能であるが、患者（本人）はアクセスを制限することが可能である。警察の権限でデータへのアクセスが必要な場合は、提訴する必要がある
	A3	研究主体別の制限	• 特になし
	A4	匿名加工	• GDPRでは匿名化(Anonymisation)と仮名化(Pseudonymised)という言葉が使われているが匿名化データは個人情報に該当しない • 研究ではPseudonymised formatであれば同意がなくても医療情報の利活用が可能であるが、仮名化に特定のルールは設定されていない • 仮名化は安全な手法で行われ、鍵となる情報(Key code)へのアクセスがある人物のみが再識別化することが可能である • 仮名加工を実施する人物はIT専門家とは限らない • ENHISは社会省の管轄であるため、仮名加工に関する責任は社会省の責任となる

研究者はENHISの倫理委員会の審理を受け、データ主体の同意を得ずにENHISのデータを利用できるが、データ主体は誰がデータにアクセスしたかの確認やアクセス制限が可能である

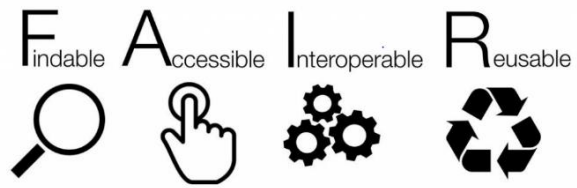
研究における医療情報の保護と利活用の実態（エストニア）

大項目	No	詳細項目	回答内容
個人情報の保護	A5	個人の権利	• ENHISの中の医療データは本人の同意なく使用されることがあるが、本人はその制限をコントロールすることが可能である。例えば、自身の医療データを誰が閲覧し、誰がどのような使用したのかといった記録も閲覧可能であるため、次回よりそれらを制限したければ、他者のアクセスを制限することが可能である。 • 情報の訂正権を有し、またデータの消去を請求することも可能である
	A6	倫理審査委員会	• 研究目的でENHISのデータの利用を求めるものは倫理委員会に申請する。申請の際には、医療情報の保護措置を述べる必要がある • 倫理委員会は医療情報へのアクセスに正当な理由があるか、どのような種類のデータを必要としているのかを分析するという役割を果たす。その分析に基づき、本人同意を得ないで研究利用が可能か否かを決定する • ただし、倫理委員会の検討事項にデータ保護の評価等は含まれていない
	A7	監督機関	• DPI(Data Protection Inspectorate)は人材不足であるが、監督機能を果たしている • DPIは特定分野に焦点を当てて調査を進める事があり、過去には銀行や学校を調査を進めていた
個人情報の保護と利活用のバランス	A8	情報保護と利活用の現状と今後の展望	• 患者は医療サービス提供者以外に対して、自身の医療情報へのアクセスを禁止する権利を持つ • 医療サービス提供者も同様に、患者の要望に応じてデータへのアクセスを禁止する権利を持つ • ヒアリングでは質問を行っていないが、eHealth 戦略計画2020では2025年までのビジョンを掲げ、ENHISに集約されたデータの更なる利活用に向けた計画を策定している

177 出所：https://www.sm.ee/sites/default/files/content-editors/sisekomm/e-tervise_strateegia_2020_15_en1.pdf

オランダは研究において、本人同意を唯一の法的根拠とするほど重視している。医療目的のデータベースは存在するが、セキュリティ管理等の懸念から研究での活用に至っていない

研究における医療情報の保護と利活用の実態（オランダ）

大項目	No	詳細項目	回答内容
医療情報の利活用	A1	医療情報の収集手段	• 本人の同意をとることが唯一の手段と言えるほど同意を重視している。Legitimate Interestを法的根拠とすることはまずない
	A2	データベースの活用	• 一般的な医療情報を管理するためのデータベースはあるが、研究目的で利用しやすい状態にはない。研究のために政府レベルで集約されているデータベースもない。そのため、研究者は独自に情報収集を行っている。複数の医療機関で「同じ言葉(same language)」で情報交換をする試みはあるが、標準化されておらず難しい。データセキュリティに関する懸念、法的または技術的な課題もあり、研究目的ではデータベースは活用できていない
	A3	研究主体別の制限	• 研究主体の制限はないが、機微な個人情報に関する取扱いには制約がある ✓ ISO27001（情報セキュリティマネジメントシステムに関する国際規格）が適用される ✓ NIS指令 (Network and Information Systems Directive)の適用 ✓ 評価委員会（Assessment Committee)の評価 ✓ FAIR基準(オランダの保健省が制定した原則であり、学術研究に良く適用される） • Findable 見つかる • Accessible アクセスできる, • Interoperable 相互運用ができる • Reusable 再利用できる 
	A4	匿名加工	• 匿名化(anonymisation)を確実に行う技術はないので、誰も触れたがらず、匿名化基準もない • 研究では匿名化ではなくAggregated data（集計データ）を利用する • 匿名化基準がないため、匿名加工する者（Data controller and Data processor) の責任となる • データ管理者は責任を課されたくないため、匿名加工をしないという実態がある

178 出所：https://www.maastrichtuniversity.nl/research/open-science/fair-principles

評価委員会、倫理委員会、DPA等の監督が厳格に行われている一方、リスク評価をした上で、医療情報の活用に投資を行い、データエコノミーを推進していく動きが見られる

研究における医療情報の保護と利活用の実態（オランダ）

大項目	No	詳細項目	回答内容
個人情報の保護	A5	個人の権利	• GDPRでにある全ての個人の権利が認められている • 研究目的でも消去(Erasure)の要求は認められる。ただし、本人は研究内容や目的について実際十分な説明を受け、研究に参加することで新しい薬ができるなど、自身の治療にメリットがあるという考えで同意をしているので、消去や撤回(withdraw)をすることはまずない • 個人情報を入手してすぐにAggregated Data(集約された統計データ)に加工すれば、個人情報に該当しないため、データ元の個人情報を消去したとしても、Aggregated Dataを消去する必要はない。そのため、研究者は個人情報を入手すると、直ちにAggregated Dataに加工している
	A6	倫理審査委員会	• 病院全体の情報管理に関する評価委員会(Assessment Committee)があり、更に研究に焦点を当てた倫理委員会(Ethics Review Committee)が医療機関の中にある。倫理委員会の構成メンバーには法務と倫理の両方の専門家がいる
	A7	監督機関	• データ保護当局(Data Protection Authority : DPA)が１つあり、組織や個人が苦情を訴えることが可能である。DPAの所属人数は多くはないが、当局の活動は活発であり厳しい。（苦情等があった場合）全件は調査しないが、調査内容は厳しく、罰金が課されたケースも何件もある。
個人情報の保護と利活用のバランス	A8	情報保護と利活用の現状と今後の展望	• DPAは医療情報に対して厳格な姿勢を示しているが、リスク評価をした上で利用をしていくという考えである(Risk based approach) • データエコノミーの推進する動きが見られる。保険会社などはマーケティング目的で医療情報を求めており、医療機関も利益になるのであれば関心がある。グーグルやフィリップスは、データベースの活用により研究費の削減に成功している

シンガポールの研究も、原則本人の同意の取得に基づいているが、後向き研究では同意が不要な場合や、匿名化情報の再識別が認められる場合もある

研究における医療情報の保護と利活用の実態（シンガポール）

大項目	No	詳細項目	回答内容
医療情報の利活用	A1	医療情報の収集手段	• ヒト生医学的研究条例や臨床試験に関する条例に従い、要件を満たす同意の取得によって医療情報の収集が可能となる • ただし、後向き研究の場合で、過去の情報を匿名化できず、またデータ主体の連絡先が不明で連絡をとることが不可能であるか連絡を取ることにコストが非常にかかる場合は、本人の同意なくデータの利用が可能である • 匿名化加工がされている場合は、本人の同意は不要である • 再識別化が許容されるケースもあるが、限定的である
	A2	データベースの活用	• PDPAが適用されるのは民間企業であり、政府機関はPDPAに準拠した公的サービス条例やPublic Sector (Governance) Act(PSGA)が適用される • 本人(患者)はNEHRにある情報のアクセス、訂正、同意の取消しを請求することが可能。ただし、患者自身が医師の意見等の情報を直接変更することは不可能。また同意を取り消して治療を拒否することも可能である • 製薬企業等も申請により、データへのアクセスが正当化された場合にNEHRへのアクセスが可能
	A3	研究主体別の制限	• 研究主体の制限はない • 経済発展のため、医療研究ハブの構築など投資が進んできた • 官民連携による研究も推奨されている
	A4	匿名加工	• ガイドラインは公表されているものの、具体的な匿名化手法については述べていない • ガイドラインに従い、再特定化のリスク評価を行う必要がある

出所： https://sso.agc.gov.sg/Act/PSGA2018#legis
https://www.straitstimes.com/politics/parliament-public-agencies-not-governed-by-pdpa-because-of-fundamental-differences-in-how

欧州のGDPRでは公益目的の法的根拠では本人の同意は撤回できないが、シンガポールでは国の利益が個人の利益に勝るとするのは難しく、本人の同意の撤回が可能である

研究における医療情報の保護と利活用の実態（シンガポール）

大項目	No	詳細項目	回答内容
個人情報の保護	A5	個人の権利	• インフォームドコンセントを与える上で、その目的と開示先についての説明を受ける権利が認められている。また、インフォームドコンセントは署名が求められる • 本人に、同意の撤回権が認められている。例えば1月に同意を行い、2月に撤回した場合、2月以降のデータは取り扱うことができなくなる • 欧州のGDPRでは公益目的などの法的根拠があると同意を撤回できないが、シンガポールでは国の利益が個人の利益に勝るとするのは難しい。基本的には同意に基づいているので、撤回が可能である • 2020年11月にはデータポータビリティ関連の法案が可決した
	A6	倫理審査委員会	• 全ての医療機関は倫理審査委員会を設立しなければならず、そのメンバーは科学者に加えて、非科学者も含む • 倫理審査委員会はプライバシーに関する事項に、回答しなければならない • 倫理審査委員会にDPOを含むことは義務化されていないが、倫理審査委員会の中で研究の財源や予算、データ保護に関する検討を行う
	A7	監督機関	• PDPC(個人情報保護委員会)は10人の委員から構成される。大きな規模ではないが、監督機関として全ての調査を行っている • 欧州は任意で監査を実施するが、シンガポールは苦情を受けた際に監査を実施している • 調査や監査対象になり得るセクターは特に営利目的の分野であり、非営利分野と差がある • ガバナンスや安全措置を徹底していれば、高額な罰則となるケースは少ない。ガバナンスを徹底させるために、重要なセクターには認証を与えたり、中小企業には補助金を出している • 医療研究に関して制裁金が課されたケースはこれまではないと思われる
個人情報の保護と利活用のバランス	A8	情報保護と利活用の現状と今後の展望	• 本人の権利に関する対応と監査により、確実に規則を遵守するような体制ができている • データを処理する際の根拠となるのは、おおむね同意の取得であるため、保護措置の一つとして同意の撤回がいつでも可能である。また、同意の撤回を行う際は、撤回をすることで発生するデメリットについても説明を受ける。同意の撤回は、7日以内に実施される必要がある • 2021年2月にPDPAの法改正が行われた

3.5 海外調査参考情報

米国

【参考】Meaningful useは、HITECH法の制定後、2011年EHR導入インセンティブが開始される前に3ステージに分けて設定された

Meaningful Use概要

STAGE	1	2	3
目的	データの収集と結合	収集プロセスの改善	アウトカムへの活用
時期	2011年～	2014年～	2016年～
要件	• 医療情報の電子化および標準化 • 主要臨床記録 • ケアサービスの調整過程におけるコミュニケーション • 医療の質評価および公衆衛生に関する報告書作成への取組み • 患者および家族への関わり合いに向けた利用	• HIEの活性化 • 電子処方箋および診断結果を含むEHR要件拡大 • 患者情報を複数の第三者機関への電子送信 • 患者による自己管理データへ拡大	• 治療効果向上につながる医療の質および安全性の向上と効率化 • 国家重点疾患に関する判断サポート • 患者のための自己管理ツール • 患者を中心とした包括的な医療情報交換 • 社会全体の健康向上への貢献

出所：ONCホームページ（https://www.healthit.gov/）、NRI「米国ヘルスケア産業の構造変化と医療機器業界への影響」

【参考】HIPAA Privacy Ruleに関して、HHS（U.S. Department of Health & Human Services）が特定項目に関する用語の定義と事例を挙げている

HIPAAで用いられる用語の定義と具体例①

用語	定義・説明	具体例（一部抜粋）
偶発的な使用と開示 (Incidental Uses and Disclosures)	・CEが個人のプライバシー保護のための措置等を適切に行っている場合、特定の偶発的なPHIの使用と開示を許容している	・医療機関のレベルに合わせて適切な措置が取られている中で発生した事象に関しては許容されるが、「病院の職員が患者の情報について話しているのを、他の職員が聞いてしまった場合」等に関しては偶発的な使用や開示とは認められない
必要最小限の要件 (Minimum Necessary)	・PHIへの不必要又は不適切なアクセスや開示を制限するため、必要最小限の基準を設け実践の評価や保障措置の強化を行うこと	・PHIの開示を要求された場合、その要求内容に沿い必要最小限のものに限定して開示を行わなければならない
個人代表者 (Personal Representatives)	・医療関連の意思決定を行う際に個人を代表して行動する権限を与えられたもの	・個人が未成年者の場合、その個人代表者は親、後見人又は未成年の子どもに代わって健康管理の決定を行う法的権限を持つ親権者
ビジネスアソシエート (Business Associates : BA)	・PHIの利用や開示に関わる特定の役割や活動を、CEに代わりに行う、又はCEにサービスを提供する個人又は事業体のこと	・BAの例: 医療提供者への会計サービスにPHIが含まれる公認会計士事務所
治療、支払い、関連手続等に関する使用と開示 (Uses and Disclosures for Treatment, Payment, and Health Care Operations)	・治療、支払い、関連手続に関しては、PHIを（一定の制限と保護の下で）使用・開示することをCEに許可している	・治療、医療費の支払い、医療提供者のための品質評価及び改善の取組み、クリニカルガイドラインの策定等のヘルスケア業務において、特定のPHIの使用・開示が可能
マーケティング (Marketing)	・製品やサービスの購入や利用を促すようなコミュニケーションのこと	・元患者に対して、病院側から「心電図を$39で提供できる施設がある」と説明すること
公衆衛生活動 (Public Health)	・公衆衛生局が病気、怪我、障がいを予防又は制御するための活動	・CEは虐待やネグレクトの恐れがある時に、当局に対してPHIの開示を行う
研究 (Research)	・一般化が可能な知識の開発又は貢献を目的とした、研究開発、試験及び評価を含む体系的な調査のこと	・PHIの利用に関して研究参加者の承認を取得し、臨床試験等の研究を行う ・本人の承認が得られない場合も、正当性が認められた上で、IRBかプライバシー委員会の認可を受ければPHIの使用が可能

【参考】HIPAA Privacy Ruleに関して、HHS（U.S. Department of Health & Human Services）が特定項目に関する用語の定義と事例を挙げている

HIPAAで用いられる用語の定義と具体例②

用語	定義・説明	具体例（一部抜粋）
労働者補償 (Workers' Compensation Laws)	・労災関係会社等は、労災制度下での手当てを行うために個人の医療情報にアクセスする必要がある ・HIPAA Privacy Ruleではその正当な必要性を認識し、労災目的での医療情報の開示を許可している	・労災時、労働者に提供された医療費支払いに関して関係者にPHIの提供を行う
通知 (Notice)	・通知は、プライバシーの問題や懸念事項について個人に焦点を当て、医療計画や医療提供者との話し合いを持ち、その権利を行使するように促すことを目的としている	・CEが、カスタマーサービス等に関する情報を提供するウェブサイトに、通知事項を目立つように掲示し、利用可能な状態にしておく
政府のアクセス (Government Access)	・HIPAA Privacy Ruleにおいては、政府運営の医療保険と医療提供者は、個人特定が可能な医療情報を保護するため、民間の医療計画と実質的に同じ要件を満たす必要がある	・政府運営の医療保険(ex. Medicare, Medicaid Plans)は、民間の医療保険と実質的に同じ手順を踏んで、顧客から受け取る請求書や医療情報を保護管理する
死亡者 (Decedents)	・HIPAA Privacy Ruleでは、死亡人の死亡日から50年間、死亡人に関する個人特定可能な医療情報を保護する	・死亡してから50年以上経過した個人特定可能な医療情報等は、PHIとはみなされないためHIPAA Privacy Ruleの適用を受けずに使用・開示することが可能である
学生の予防接種 (Student Immunization)	・PHIのプライバシー保護を行う一方、公衆衛生等の目的のためにPHIの開示を認める必要があり、学生の予防接種情報の開示はその一例である	・学校は保護者に予防接種の記録を要求し、保護者が医療機関に子どもの予防接種記録を要求することで、入学法(所定の予防接種を受けていることを証明できなければ、登校が禁止される法律)の条件を満たす
マーケティング: 処方薬等の継続服薬リマインダー (Marketing: Refill Reminders)	・治療等サービスの奨励や助言と、マーケティング活動はやむを得ず重なってしまう部分が存在する ・必要不可欠な治療等サービスが妨げられないようにマーケティングとみなされない例外項目を規定しており、個人に定期処方されている薬剤等の継続服薬のリマインダーがその一例である	・「継続服薬リマインダー」に該当する項目として、現在処方されている薬の継続案内、薬のジェネリック同等品に関する案内、薬を指示通りに服用するよう促す、過去90日以内に失効した処方箋に関する案内等が挙げられる

出所：HHS, Guidance on Significant Aspects of the Privacy Rule
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/significant-aspects/index.html

GDPRで定められた有効な「同意」の要件

【参考】同意が「自由意思に基づいた（選択・支配権がある）」ことの判断要素として「力の不均衡」「条件性」「粒度」「不利益」の4項目がある

■ GDPRで規定する「自由」とは、データ主体に真の選択と支配権があることを意味している
■ データ主体が真の選択をせず、同意を強制されたと感じる、又は同意しなければ不利益な結果に直面すると感じるならば、同意は有効ではない

自由意思に基づいた (Freely given)

以下の 4 要素を含む場合は同意の自由（任意性）が否定される

要件	説明	各要件の事例	
力の不均衡 Imbalance of power	データ管理者が公的機関や雇用者である場合、データ管理者とデータ主体の関係において力の不均衡や従属関係があるため、データ主体の自由意志が否定される	（力の不均衡としない例）ある市町村が道路の補修工事を計画している。長期にわたる工事のため、住民に対して最新情報を受け取れるメーリングリスト登録機会を提供する。参加する義務がないこと、目的外利用はしないことを明らかにし、同意又は拒否が自由にできるようにする	○
条件性 Conditionality	データ主体が同意しない限り、データ管理者のサービス提供が受けられない場合、データ主体の自由意志が否定される	ある銀行が、第三者がダイレクトマーケティング目的のために顧客の支払い内容を利用することについて顧客に同意を求める。この取引行為は、顧客に対する契約履行にも口座サービスの提供にも必要ではない。この同意に拒否することで銀行サービスの拒否、口座の閉鎖等につながる	✕
粒度 Granularity	データ管理者が複数の業務を行うにあたり、別個に同意を取るのではなく包括的に同意を取る場合、データ主体の自由意志が否定される	ある小売事業者が、同じ同意の要求の中で、顧客にeメールでマーケティング情報を送付し、またグループ内の他の企業とその内容を共有するため、その顧客に対してデータ利用に同意するよう求める。この同意は個別の目的に対する個々の同意ではないため、粒度が揃っていない	
不利益 Detriment	データ主体が同意しない場合等に費用負担などの不利益がデータ主体に生ずる場合、データ主体の自由意志が否定される	あるヘルスケア・モバイルアプリをダウンロードする際、アプリから電話の加速度計へのアクセスのための同意を求める。これはアプリの動作には不要だが、ユーザーの活動レベルを学習しようとするデータ管理には役に立つ。ユーザーが後にその同意を撤回すると、アプリが限定的にしか動作しない	

出所：一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関するガイドライン

【参考】同意は個別に特定の目的に関して与えられる必要があり、目的の変更があった場合には新たに同意を取得する必要がある

■ データ主体の同意は「一つ又は複数の特定の」目的に関係して与えられなければならず、それら個々に関して自由に選べられるようにしなければならない

特定された (Specific)

「特定された（specific)」の要素を満たすためには、データ管理者は以下を適用しなければならない

要件	説明
目的の詳述 (*1) Purpose specification	• 本来の目的のための機能が他の目的にも拡大流用されること(function creep)に対するセーフガードとして、目的の詳述が求められる • データ管理者が当初の目的と別の目的のためにそのデータの取扱いを希望する場合、データ主体に対して追加の同意を求める必要がある
粒度 (*1) Granularity	• データ管理者が異なった目的のために同意を求める場合、特定の目的に対してデータ主体が同意を与えることができるように、各目的について個別のオプトインの機会を提供すべきである
同意取得に関する情報の分離 (*1) Clear separation of information	• 同意取得に関係した情報を、他の事項についての情報から、明確に分離する

事例	✖	○
追加同意 (*1)	あるケーブルTVネットワーク事業者が加入者に対して視聴習慣に基づいた映画を提案するため、同意に基づいて加入者の個人データを収集する。その後、第三者がその視聴習慣に基づいた広告を送付する	ケーブルTVネットワーク事業者は第三者がその視聴習慣に基づいた広告を送付できるようにすることについて決定した場合、この新しい目的には別途同意が必要となる
個別同意 (*2)	マーケティング業務の説明を1段落で説明し、その一部にメールアドレスやIPアドレスの利用について触れ、段落の末尾にまとめて同意を得る	それぞれのデータの利用目的を述べ、データ主体が各項目に同意できるようにする

出所：*1 一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関するガイドライン
*2 https://gdpr.eu/gdpr-consent-requirements/

【参考】「説明を受けた同意」とは、データ管理者がどのデータを何の目的で使用するかについてデータ主体が理解した上での同意である。またデータ主体はいつでも同意を撤回できる

説明を受けた（informed)

データ主体に説明すべき内容	具体例
データ管理者の身元 Controller's identity	• データ管理者の組織名 • 代表者及び情報保護責任者名 • 連絡先
目的 Purpose	• 同意が求められるそれぞれの取扱業務の目的
データの様式 Type of data	• 収集され利用されるデータ(そのタイプ：紙・電子など)
同意の撤回 Right to withdraw consent	• 同意を撤回する権利があること • どのように撤回できるか
自動化された意思決定のためのデータ Automated decision-making	• 第22条(2)Cに基づき個人に対する自動化された意思決定のためのデータ利用についての情報 【例】オンラインでの融資額の決定
リスク Possible risks	• 十分性認定及び第46条で述べられる適切な保護措置がないことによるデータ移転の起こりうるリスクについて

説明の仕方

要件	✖	○
明確かつ平易な用語の使用	二重否定や矛盾する表現といった紛らわしい言葉による同意	データ主体にとって理解可能なものにすべきである
同意の要求の明確な区別	同意が(紙の)契約書の一部として要求される	同意の要求は他の事項と明確に区別されるようにすべきである

出所：一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関する ガイドライン
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what3

【参考】同意はデータ主体の「不明瞭でない意思表示」として、積極的行為により取得される必要がある

■ GDPRは、データ主体からの声明又は明らかな積極的行為による同意を定めている

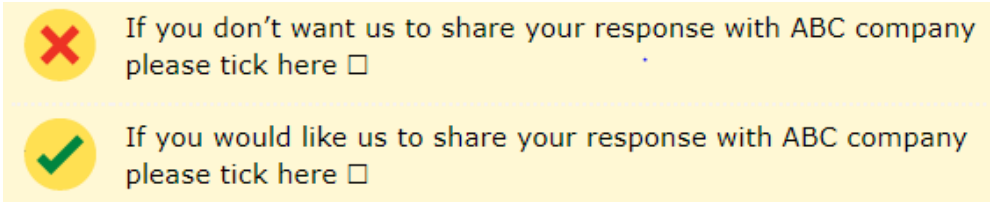
不明瞭でない意思表示 (Unambiguous indication of wishes)

「不明瞭でない意思表示」の要件の一例として、以下のものが挙げられる

要件	説明
積極的な同意 Affirmative action (consent)	同意においては、陳述又は明白な積極的行為（statement or by a clear affirmative action)による明確な意思表示を必要とする

事例	✖	○
明確な意思表示	• 事前にチェックが記入されたボックス • オプトアウトの仕組みの提供	• ウェブサイトのサービス設定に関して自身でチェックボックスに✓を入れる • オプトインボックスの提供

オプトアウトボックスは、行動を起こさないという点を利用して(advantage of inaction)、より多くの同意を得やすいため、同意の質に問題がある。
そのため、オプトインボックス(又は他のオプトインの手法)により同意を得る必要がある。



✖(否）オプトアウトボックス
ABCカンパニーにあなたの回答を共有して欲しくない場合はここにチェックを入れてください

✓(可）オプトインボックス
ABCカンパニーにあなたの回答を共有して欲しい場合はここにチェックを入れてください

出所：一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関するガイドライン
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

【参考】有効な同意を得るための追加的条件として、データ主体の同意を証明できるようにすること、またデータ主体が同意をいつでも撤回する権利が与えられていることが必要である

同意の条件(GDPR第7条第1項)

条件	概要
同意の証明 Demonstrate consent	■ 管理者は、本人(データ主体)が自己の個人データの取扱いに同意していることを証明できることが求められている ➢ 同意取得の仕方(口頭や書面など)については、GDPR上の規定はない ■ 同意の証明義務は、該当する個人データの取扱業務が継続する限り管理者側にある ➢ GDPRは同意がどの位の期間継続するかについて示していない。取扱業者や同意の範囲が拡張された時には新たな同意の取得が必要になる
同意の撤回 Withdrawal of consent	■ 本人(データ主体)は、いつでも同意を撤回する権利があり、管理者は撤回する権利の情報提供が求められている ➢ データの取扱い(例えば、追加の保存)を正当化する他の法的根拠がないならば、そのデータは管理者により消去されなければならない ➢ ただし撤回前の個人データの取扱いは違法にならない ■ 同意の撤回が制限されることはない ■ 管理者は、データ主体による同意の撤回が、同意を与えたときと同様に、簡単にまたいつでも可能であることを確保しなければならない

事例	✖	○
同意の証明	• データの取扱業務に対して同意を得たことを証明できない • 同意の期間が変更されたにも関わらず、新たな同意を取得しない	• 電話を通じて同意を取得する際、その陳述を録音しておく • データの法的義務の遵守又は提訴のため扱い行為が終了した後もデータを保持する
同意の撤回	• オンラインチケットのキャンセル方法が、平日の就業時間帯に電話で問い合わせする以外にない ⇒予約時はオンラインで同意をしているのに、撤回はオンラインでできない	• オンラインチケットのキャンセルが、週7日24時間可能なマウスクリック1回で可能である • 不利益を被ることなく同意を撤回できる

出所：一般データ保護規則（GDPR）の前文、一般データ保護規則（GDPR）、同意に関するガイドライン

GDPR 正当な利益 (Legitimate Interest)

【参考】正当な利益（Legitimate interest）は、法的根拠の中で最も柔軟性があるが、適用の可否の判断が難しい

GDPR第6条(f)正当な利益（Legitimate interest）の適用

■ Legitimate interestの特徴

- Legitimate interestは 6 つの法的根拠の中で最も柔軟性が高いが、適用の可否の判断が難しい
- 特定のデータ利用目的に焦点を当てていない

■ どんな場合に適しているか

- データ処理が法的に求められていないが、データ管理者又はその他の人々にとって明確なベネフィットがある場合
- 個人のプライバシーに関する影響が限定的である場合
- 個人が、その情報を活用されることが合理的であると思える場合（reasonably expect)
- 事前に個人の完全なコントロール（例：同意）を与えることができない、又は与えたくない場合。又はデータ処理に反対することがないと思われる場面で、同意の手間をかけさせたくない場合

■ Legitimate interestが適用可能な場合（例）

- 顧客又は従業員のデータ利用
- マーケティング分析
- 不正防止
- 同組織間でのデータ移転
- ITセキュリティ

→ 本人がデータの利用を合理的に予測できる

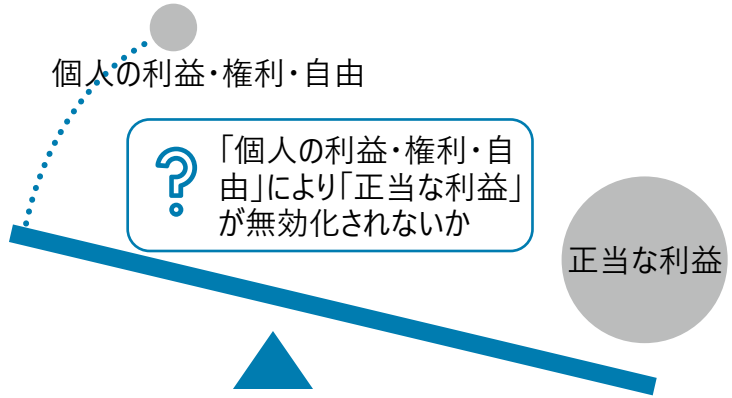
Legitimate interestを適用した事例

【背景】
分割払い契約をしている顧客が金融機関に転居先を届け出ずに引っ越しをしたため、連絡がつかなくなり、支払いが滞った

【目的 Purpose】
金融機関は借金回収のために、エージェントを介して顧客を見つけたい。そのために、顧客の個人情報をエージェントに開示する必要がある

【必要性 Necessity】
借金回収のためにエージェントを使う必要がある

【バランス Balance】
顧客は金融機関が借金を回収するためにとるべき手段を想像し得る。顧客自身の利益（interest）は借金の支払いを回避することかもしれないが、金融機関の借金回収の利益（interest)が支持される



出所：https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

【参考】Legitimate interestを情報処理の法的根拠にするためには、データを取り扱う前に3つのテストを実施し、「正当な利益」を正当化できると結論づける必要がある

3 つのテスト：Legitimate Interests Assessment (LIA)

テスト	概要	テストの内容
目的 Purpose Test	目的の特定を行いそれが正当な利益として妥当かを検討する 目的は可能な限り具体的にする	■ データ処理に伴いどのような利益が発生するのか ■ 関連法・ガイドラインを遵守しているか ■ 特定の目的の場合、即座に正当な利益であると決定される(ex. 不正行為の防止、情報セキュリティetc.)
必要性 Necessity Test	目的達成のために該当するデータの取扱いが必要かを検討する	■ 目的に適った処理であるか ■ 処理せずに目的を達成することは可能か ■ より効率的な処理方法はないか
バランス Balancing Test	「データ主体の権利と利益」と「情報管理者の正当な利益」のどちらが重視されるかを検討する	■ データの質：データの性質上個人が特定されやすいか ■ 予測可能性：客観的指標として、データを使用することについて人々が納得しその行為に期待するか(Reasonable expectations) ■ データ利用による影響及びセーフガード：処理により個人の権利と自由に対するリスクをもたらす可能性があるか、またそのリスクを軽減するセーフガードは存在するか

出所：https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/
https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

【参考】米国では、個人の権利の拡大や緊急事態時の情報取扱いの柔軟性向上など HIPAAの改正方針が示されている。欧州委員会はEU域内での連携強化に言及している

HIPAA Privacy Rule改正提案

2020年12月10日、HHSのOCRは、「調整されたケアと個人の参画を支援し障害を取り除くためのHIPAA Privacy Rule改正提案」と題する文書を公表した。以下の5点が主な方針とされている

- ✓ 個人が自分自身の保健情報（電子情報を含む）にアクセスする権利を強化する
- ✓ 個人のケア調整とケースマネジメントのための情報共有を向上させる
- ✓ 緊急事態または健康の危機を経験する個人のケアにおける家族および介護者の関与拡大を促進する
- ✓ 緊急事態または脅威の存在する環境での情報開示に係る柔軟性を強化する
- ✓ 個人の保健情報のプライバシー権益を継続的に保護する一方、HIPAAの適用対象となる医療提供者および医療保険者の管理上の負荷を低減する

FOR IMMEDIATE RELEASE
December 10, 2020

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Proposes Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) announces proposed changes to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to support individuals' engagement in their care, remove barriers to coordinated care, and reduce regulatory burdens on the health care industry.

The Notice of Proposed Rulemaking (NPRM) is part of HHS's Regulatory Sprint to Coordinated Care, initiated under HHS Secretary Alex Azar's value-based transformation agenda and led by HHS Deputy Secretary Eric Hargan, which seeks to promote value-based health care by examining federal regulations that impede efforts among health care providers and health plans to better coordinate care for patients.

出所：https://www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html

欧州委員会による加盟国の医療情報取扱い実態調査

2021年2月12日、欧州委員会は、「医療情報に関するEU加盟国のGDPR上の規則評価に関する研究」結果を公表した

この中で、欧州委員会は以下の点に言及している

- ✓ GDPRの解釈について各国に分散がある
- ✓ このことがEU域内での医療情報の利活用を阻害する要因になりえる
- ✓ 今後この業界においてEU域内統一ルールを検討する可能性がある
- ✓ 法や運用面に限らずインフラの相互運用性を高める必要がある
- ✓ データの品質、デジタルスキルの開発などを通じた一次利用二次利用のスキルアップも調和を図る必要性がある

European Commission

e-News
12/02/2021

Health and Food Safety Directorate General

Twitter Food | Twitter Health

Public Health

Commission publishes study on Assessment of the EU Member States' rules on health data in the light of GDPR

Today, the Commission published a study on the "Assessment of the EU Member States' rules on health data in the light of GDPR". The study finds that while the General Data Protection Regulation (GDPR) lays down horizontal directly applicable rules in all Member States, there remains variation in the range of national-level legislation linked to its implementation in the area of health. This, the study suggests, has led to a fragmented approach in the way that health data processing for health and research is conducted in the Member States. This can negatively impact cross-border cooperation for care provision, healthcare system administration, public health or research.

To ensure that European healthcare systems can make the best possible use of health data and to support the development of the European Health Data Space, a number of legal and operational issues need to be addressed in a multi-faceted approach. The study identified potential future EU level actions, including stakeholder-driven Codes of Conduct as well as new targeted and sector-specific EU level legislation. In addition to legal requirements and governance, the study also points to the need for a more harmonised approach across the Member States when it comes to technical infrastructure, technical and semantic interoperability. Data quality and acquisition, digital skills and capacity-building for primary and secondary use of health data were also areas identified where a harmonised approach could be beneficial.

The study goes on to highlight that co-operation between the EU, Member States and relevant stakeholders is important, with a particular focus on the interests of patients. The study specifies that they should be supported as active agents in their own health and care, with full capacity to exercise their health data related rights. In conclusion, the development of the European Health Data Space, including specific legislation to be adopted to complement the proposal for a Data Governance Act, is believed to offer the ideal opportunity to build upon the suggestions outlined in the study. In addition, it is believed to ensure that health data can be used to promote better patient care, more resilient healthcare systems and stronger collaborative public health protection and healthcare research across the European Union.

European Commission

DG Health and Food Safety

Assessment of the EU Member States' rules on health data in the light of GDPR

Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03

出所：https://www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html

4. 諸外国との相違点

国内における現行制度の課題である「第三者が研究目的で医療情報利活用を行うこと」に対して、積極的な取組みを行っている米国と英国を対象として日本との比較を行った

比較対象とする諸外国の整理

調査対象国	人口 (日本:約127百万人)	医療情報の利活用の実態	日本との比較
米国	約328百万人	■ 数千万人規模の医療DBが複数存在し、主に医療DBを用いた利活用が行われている ■ 医療データの標準化や統合を政府が主導しているため、情報の集約化がさらに進むことが予想される	■ 大規模医療DBが官民で発達 ■ 政府主導による情報の集約化がさらに進むことが予想される
英国	約67百万人	■ NHS Digitalが管理するSpine及びMHRAが管理するCPRDによって医療情報が集約されている ■ 政府の働きかけにより、近年はGPデータを中心に医療DBの利活用が増加している	■ 政府が医療領域において、ジタル化を進めている ■ GPを中心とした医療DBの構築にも注力している
エストニア	約1百万人	■ 政府主導でENHISを用いて国民の医療情報を集約すると共に、診療目的による周辺サービスへの展開を行っている ■ 国民の健康寿命延伸、医療費の適正化を目的として構築されているため、診療目的以外の利活用は難しい模様である	△ ■ 日本と人口規模が異なる ■ 日本の課題である研究目的を想定した仕組みとなっていない
オランダ	約17百万人	■ 民間主導でLSPというHIEを構築して、人口の8割がオプトインでデータ提供を行い、PHRや医療機関で利活用されている ■ 国民の健康寿命延伸を目的として構築されているため、民間の利活用は厳しい模様である	
シンガポール	約6百万人	■ 政府主導でNEHRを開発して、段階的に情報集約を進めている ■ 国民の健康寿命延伸を目的として構築されているため、公的研究を除き、民間の利活用は制限されている模様である	

4.1 日本の現行制度に対する課題との比較

米国、英国では研究目的において主体による制限は無く、米国における匿名(非識別)加工の考え方は、リスクをゼロにすることを目指していない

【日本の課題に対する諸外国の状況】法律面

課題分類	課題の主要因	日本の課題	米国における取扱い	英国における取扱い
法律面	2000個問題	医療情報の取扱い主体ごとに適用ルール及び解釈権が異なるため、データの取扱いが困難である	■ HIPAAは連邦法であり、取扱い主体ごとにルールは異ならない	■ EU共通のGDPRと国内法であるDPAが適用される。取扱い主体ごとにルールは異ならない
	適用除外規定(学術研究目的)	「学術研究目的」の利活用でも、「研究主体」により個人情報保護法の適用範囲が異なるため、利用の障害となることがある	■ 研究目的において、主体により制限される規定はない	■ 研究目的において、主体により制限される規定はない
	同意を得ずに利用可能な方法	研究目的で利活用する場合、同意と匿名加工以外の方法がない(学術研究目的を除く)	■ HIPAA Privacy Ruleでは、4項目に関して、本人の同意や承認を得ずにPHIの使用・開示が可能である ➢ 本人への利用又は開示(§164.502) ➢ 治療、支払い、ヘルスケア業務(§164.506) ➢ 研究、公衆衛生、ヘルスケア業務のための匿名化されたデータセット(§164.514) ➢ 公共の利益やベネフィットにつながる場合(§164.512)	■ GDPRではデータの処理が適法であるとする法的根拠(lawfulness)6つのいずれか一つを満たすことが求められており、同意の取得はその内の1つである ➢ 同意の取得(Consent) ➢ 契約の履行(Contract) ➢ 法的義務(Legal obligation) ➢ 生命に関わる利益(Vital interest) ➢ 公益の利益(Public interest) ➢ 正当な利益(Legitimate interest)
	仮名加工情報の取扱い	現状、仮名加工情報の第三者提供は行えない	■ 特定個人の識別リスクがゼロでなく、復元可能性もある非識別化（De-identification）データが広く用いられている	■ 研究目的でのデータベース化における適切な保護措置として、GDPR第89条に基づく仮名化が利用されるが、一方で、仮名化データは個人情報として保護対象であり、その利用は同一管理者内に限られる

米国、英国共に医療DBの活用を前提とした仕組みを構築している。また政府の監督機関によるコンサルテーションが有効に働いている

【日本の課題に対する諸外国の状況】運用面

課題分類	課題の主要因	日本の課題	米国における取扱い	英国における取扱い
運用面	ルールの複雑さ	2000個問題に加え、研究倫理指針等が難解であり、解釈・理解の統一を図ることが困難であるため、病院からのデータ提供が慎重となる	— (比較は困難)	— (比較は困難)
	責任主体	データ漏洩等のリスクが医療機関に集中しており、データ提供が消極的となる	■ 大規模な医療DBへの活用が主流で、その際に医療機関は責任を負わない	■ 大規模な医療DBへの活用が増加しており、その際に医療機関は責任を負わない
	インセンティブ	医療機関が外部へデータ提供することに対するインセンティブが乏しい	■ EHR導入の際に、ONCが設定したシステム・モジュールの要件を満たした機器・システムを導入することで、インセンティブが発生する	■ 推奨されたEHRを導入する際に、インセンティブが発生する
	丁寧なオプトアウト(次世代医療基盤法)	実質的にオプトインと同様の手続が想定されており、現場の負担感が大きい	■ HIEは、Business Associateとして扱われるため、個々の同意(承認)の取得義務はない	■ CPRDには、オプトアウトでデータ収集される
	匿名加工基準が不明確	匿名加工基準が不明確であり、各病院に判断が任されているため、加工手法に分散が大きい	■ 非識別加工は、下記2パターンにより加工基準の明確化がなされているため、判断の分散は少ない ➢ 「専門家」が判断し、個人の識別化リスクを小さくする ➢ 18個の識別子を取り除く	■ GDPR及びDPAで、匿名加工の定めはない ■ ICOが、テストやケーススタディを通じて個人再特定のリスクがないことの評価を推奨しているが、リスク評価の基準などは定められていない
	倫理審査委員会(個人情報保護審査会)	倫理審査委員会（又は個人情報保護審査会）の委員の専門性にばらつきがあり、個人情報保護法に詳しいメンバーがいないケースもあるため、判断の分散が大きい	■ IRBが該当 ➢ IRBは、5名以上のメンバーで構成され、幅広い専門知識や経験を有する者を含む必要があるとされている。実態として、法的専門家や統計学専門家が加わっている事が多い	■ DPOが該当 ➢ DPOに明確な資格要件はないが、組織の代表者となり、ICOとの連絡窓口となる。データ保護法制や実務に関する専門的な知識が必要であり、実態として専門家が任命されることが多い
	判定主体	取扱いの判断に迷う場合に、問合せできる外部機関が不明瞭であり、仮に個人情報保護委員会に問い合わせたとしても個別事例に合わせた具体的な回答が返ってこず、判断が難しい	■ OCRがコンサルテーションを行っている	■ 直接ICOに問合せをすることも可能だが、DPOを通じてICOがコンサルテーションを行う事が多い

米国、英国共に政府主導で医療DBの構築・運用を行っている。特に米国においては、公的な医療DBに加え、民間の大規模な医療DBも発達している

【日本の課題に対する諸外国の状況】インフラ

課題分類	課題の主要因	日本の課題	米国における取扱い	英国における取扱い
インフラ	標準化	電子カルテ等のフォーマットが異なり、データを結合することが困難な場面がある	■ Meaningful Useにて、ONC主導によるデータの標準化を進めている	■ NHSがNHS clinical information standardsとして定めている (GPはほぼ統一されている)
	データ結合	匿名加工後は、同じ患者の情報であったとしても名寄せは不可能である	■ 大規模な医療DBに情報が集約されており、医療DB内で名寄せが行われている	■ 大規模な医療DBに情報が集約されており、医療DB内で名寄せが行われている
	医療DB	主体や目的が限定された医療DBが多く広範な利活用を行う上で課題が多い	■ 大規模な医療DBが官民共に発達しており、情報が集約されている	■ 主に、NHS Digitalが管理するSpineとMHRAが運営するCPRDに情報が集約されている

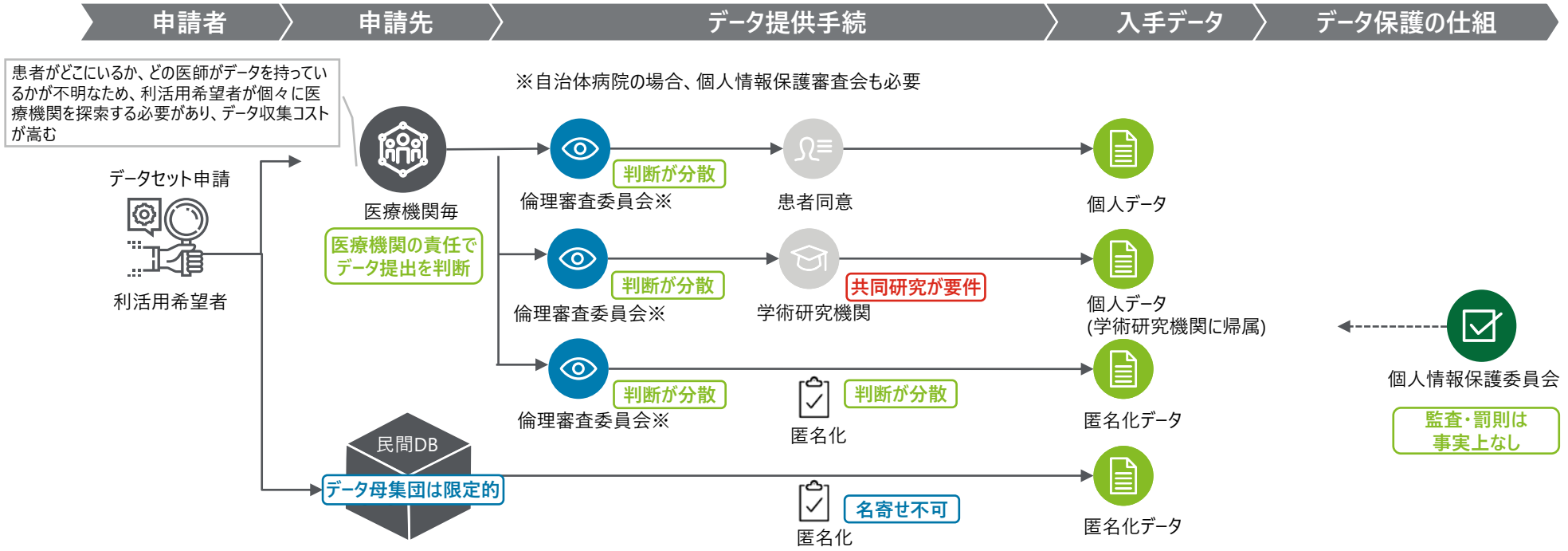
4.2 民間事業者における主要な利活用パターンとの比較

日本は、医療機関ごとにデータ提出の判断を行うこと、個人情報の保護を同意又は匿名化で行う必要があることから、収集コストが嵩む、名寄せができない等の課題がある

【民間事業者における主要な利活用パターン】日本における主要パターン

xxxx：法律面の課題
xxxx：運用面の課題
xxxx：データベースの課題

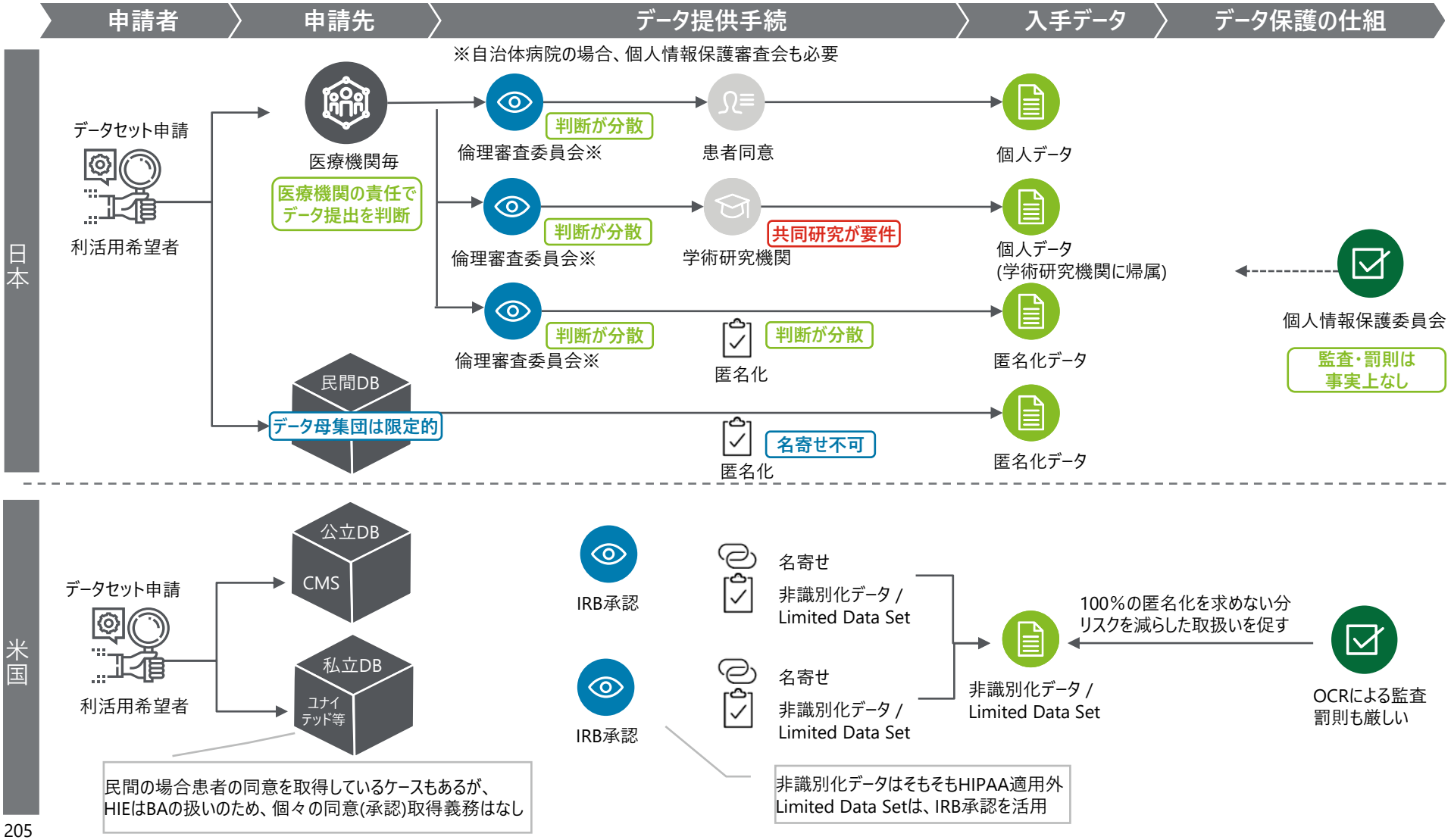
日本の医療情報利活用関連基本ルール
・一次利用：黙示の同意　【個人情報保護法・ガイダンス】
・二次利用：基本同意が必要　　【個人情報保護法】
・二次利用その他：学術研究目的では同意なく利活用可能



米国は、官民の医療DBが発達していることから、医療DBを用いた医療情報の利活用が中心である。また日本と比較して、情報の取扱いにおける監査や罰則は厳しい

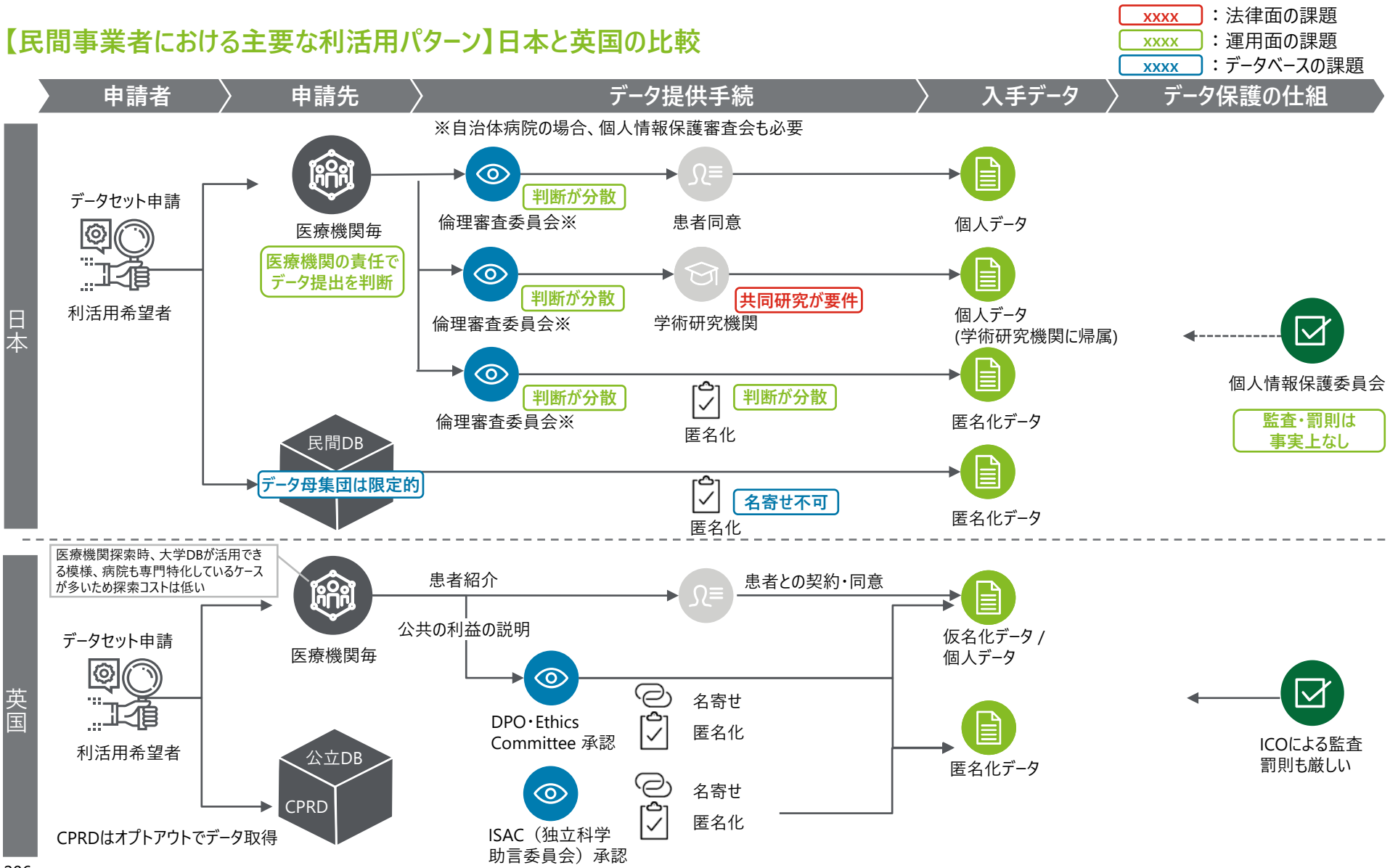
【民間事業者における主要な利活用パターン】日本と米国の比較

xxxx：法律面の課題
xxxx：運用面の課題
xxxx：データベースの課題



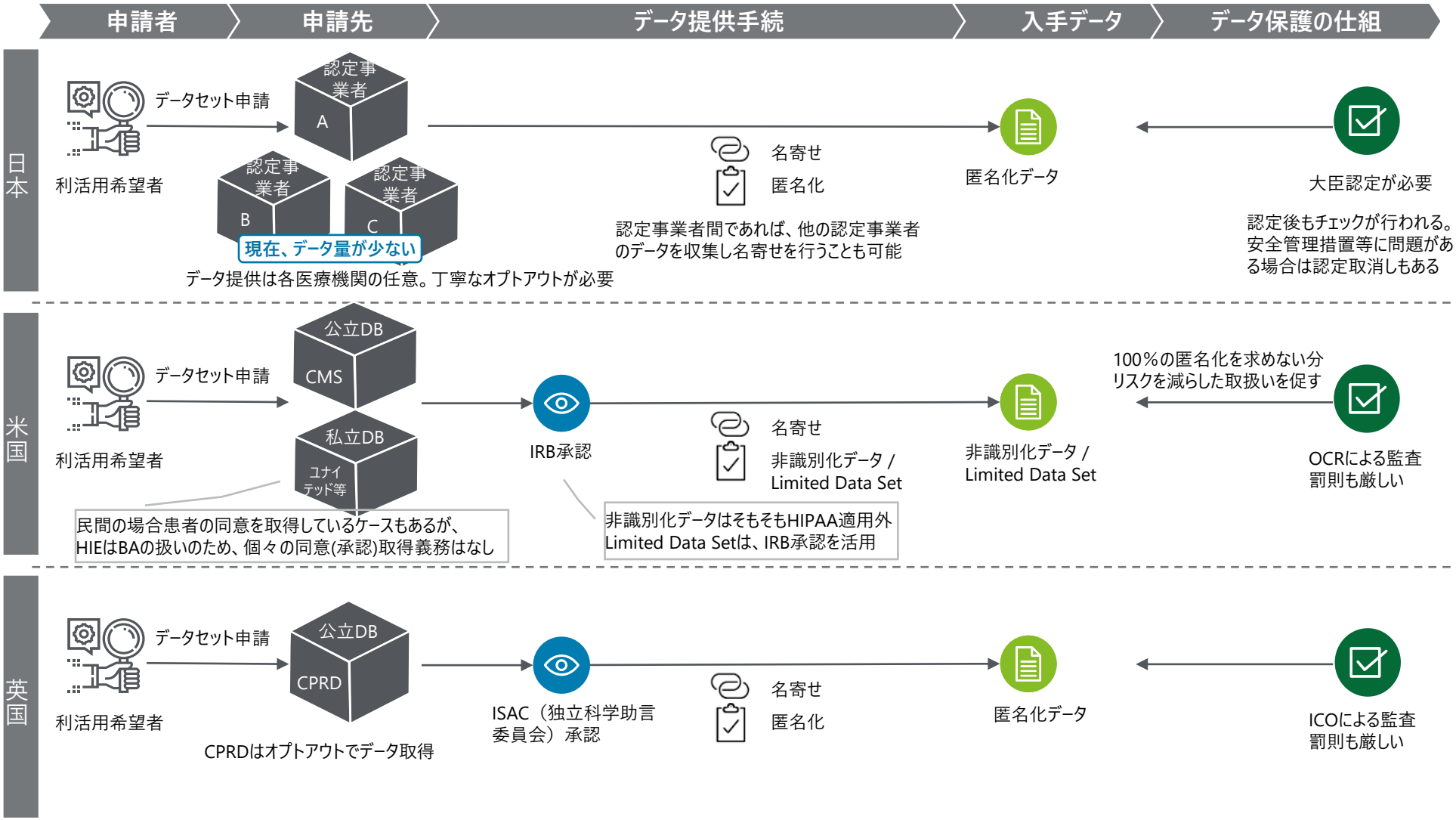
英国も、官民の医療DBが発達していることから、医療DBを用いた医療情報の利活用が中心である。また日本と比較して、情報の取扱いにおける監査や罰則は厳しい

【民間事業者における主要な利活用パターン】日本と英国の比較



日本には、米国や英国同様、次世代医療基盤法による医療DBがあるものの、現状ではデータ量が少なく、利活用が進まないという課題がある

次世代医療基盤法によるスキームを用いた場合の各国比較



【参考】NDBやMID-NETなどに加え、次世代医療基盤法による医療DBの利活用が可能であるものの、NDB以外の医療DBではデータ規模が小さい傾向にある

日本の代表的な医療DBの概要

	NDB	MID-NET	次世代医療基盤法
管理者・運営者	厚生労働省	PMDA （独立行政法人 医薬品医療機器総合機構）	認定匿名加工医療情報作成事業者 （認定事業者）
収集されたデータの規模	約1.2億人（レセプトデータ）	約500万人（2019年時点で10拠点、43病院）	約1万人（2021年2月時点のヒアリングによる）
保有データ	・レセプトデータ ・特定健診、保健指導データ	・電子カルテデータ ・レセプトデータ ・DPCデータ ・検体検査データ	・法律では、医療情報が対象とされている (ex.診療行為のアウトカムに関する医療情報など)
データ利活用可能者	① 国の行政機関 ② 都道府県 ③ 研究開発独立行政法人（PMDA含む） ④ 大学（大学院含む） ⑤ 医療保険者の中央団体 ⑥ 医療サービスの質の向上等をその設立目的の趣旨に含む国所管の公益法人 ⑦ 提供されるデータを用いた研究の実施に要する費用の全部又は一部を国の行政機関や研究開発独立行政法人等から補助されている者等	・医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に基づく医薬品の市販後安全監視やリスク・ベネフィット評価を含めた安全対策を目的とする者 ・行政機関、製薬企業又はアカデミアが実施する公益性の高い調査・研究を目的とする者	・制限はない
利活用可能データ	・集計表 ・特別抽出 ※匿名化データ	・匿名化データ	・匿名化データ
その他の特徴や問題点	・2009年から運用、2018年3月までに157件を提供 ・レセプトデータのため、アウトカムや患者重症度などの情報は無い。 ・死亡個票などとの連結は不可能である ・他のデータベースとの連結は禁止されている ・ 医療機関をまたいだ症例追跡が可能である ・厚労省から個票レベルの情報提供が行われる	・2011年から、審査は1年に数回である ・処置、転帰及び患者背景等の詳細な情報を得ることができる ・検査値変動を捉えることで有害事象を検出できる ・電子カルテデータは１週間ごとに更新される	・丁寧なオプトアウトが求められるため実質的なオプトインと変わらず、情報が収集が難しいとの指摘がある

 出所：https://biostatistics.m.u-tokyo.ac.jp/wp-content/uploads/2019/09/pdf/20181127symp01.pdf

5. 総括

①日本の課題のまとめ：データ利活用のフローに則って日本の課題を再整理すると、「データ収集」「匿名化」「判断・判定」時において課題が大きいことが分かった

「法律」、「運用」、「インフラ」領域にまたがる日本における医療情報利活用時の課題

前提
・治療目的、学術研究目的での活用においては、ルールの複雑さなどを指摘する意見もあるが、現場での課題感は薄い
・「民間企業」による「研究目的」活用時に課題が多く、以下は主にこのケースで発生する

「法律」、「運用」、「インフラ」領域にまたがる日本の課題

01 データ収集
・学術研究目的外では、基本的に「同意取得」か「匿名化」の2択しかなく、同意の取得が困難な場合、データ収集に行き詰る
・同意取得の手間やトラブル時のリスクが医療機関に集中するにも関わらず、十分なインセンティブもなく提供に消極的になる
・データの標準化ができておらず、複数医療機関からデータを収集してもスムーズに結合できない

02 匿名化
・個々の医療機関が、匿名加工基準が不明瞭なまま作業を行うため、加工データの分散が大きい（復元して検証できない）
・匿名加工を行った時点でデータの精度が低下する（特異値が欠損する可能性が高い）
・匿名加工データを収集しても名寄せができない

03 判断・判定
・個人情報保護委員会には、コンサルテーション機能が十分でなく、相談相手がいない
・倫理審査委員会、個人情報保護審査会のメンバーに専門家がいないケースが多く、基準も曖昧で判断の分散が大きい
・既存の医療DBも主体や利用目的の制限があり、利用できない組織が存在する

学術研究目的を外れると、データ収集に手間がかかり、得た情報の結合は不可能な上、組織によって判断の分散が大きいことが日本の課題である

②課題の海外比較：研究分野での利活用に積極的な米国、英国は日本が抱える各々の課題に対して複合的なアプローチで対応している

日本の課題に対する米国、英国の対応策

	日本	米国	英国
01 データ収集		✓ 政府自身が積極的で1億人を越える公的医療DBを保有 ✓ データの標準化にも積極的でインセンティブも導入 ✓ 官民の医療DBの使い勝手が良く、日本の法律面、運用面での課題がカバーされている	✓ 政府が医療情報の標準化、電子化に積極的 ✓ 近年公的医療DBの構築に積極的で活用が増えている ✓ 公的医療DB（CPRD）は診療所データが中心だが近年病院データとの結合も進めている（※CPRDへはオプトアウトでデータ収集）
02 匿名化		✓ 非識別化基準に関しては、リスクをゼロにするのではなく、個人特定と利活用のメリットのバランスを取る方針 ✓ 加工基準は明確（18個の識別子削除） ✓ 非識別化水準は長年水準向上の議論を経たが、利活用促進のため変更は行わなかった	✓ 匿名化水準は高く、日本同様復元や名寄せは不可能。加工基準は日本と同様曖昧との見解もあるが、ガイドラインで具体例を提示 ✓ 同意取得に頼らない利用も行う（公益性や正当性の適用） ✓ 一方で、欧州域内でのGDPR等に対する解釈が異なるという独特な課題がある
03 判断・判定		✓ 医療DBが発展しており、同意取得の必要性も薄く、提供判断は医療DBが行うケースが多い ✓ IRB（組織内判定主体）には専門家が配置されるケースが多く、OCR（政府監督機関）がコンサルテーションも行う ✓ ただし、罰則規定が厳しく、個人の権利（撤回権など）が重視される	✓ ガイドラインで具体例を提示 ✓ DPO（組織内判定主体）の責任が大きいため、専門家が就き、ICO（政府監督機関）がコンサルテーションも行う ✓ ただし、罰則規定が厳しく、個人の権利（同意撤回権など）が重視される
その他		✓ 政府が利活用に積極的な姿勢を発信 ✓ 政府が新技術等に対応して4年毎に戦略を発表 ✓ 医学部に医療情報取扱い専門医制度を導入済み	✓ 政府が2011年からICT戦略を発表し電子化を進める ✓ 政府が利活用に積極的な姿勢を発信 ✓ 政府（NHS）の提供する医療が無料であることもあり、国民の理解は得られやすい土壌がある

特定の分野のみでの解決は本質的な解決にならず、各国とも複合的なアプローチを取っている

③海外比較の上での日本の課題の提示：「次世代医療基盤法」によって解決の道筋は示されている個所が多いが、現時点では活用可能なデータ量が少ないという課題が残る

日本の課題に対する次世代医療基盤法による解決策

「法」、「運用」、「インフラ」領域にまたがる日本の課題（再掲）

次世代医療基盤法による解決

01 データ収集
・学術研究目的外では、基本的に「同意取得」か「匿名化」の2択しかなく、同意の取得が困難な場合、データ収集に行き詰る
・同意取得の手間やトラブル時のリスクが医療機関に集中するにも関わらず、十分なインセンティブもなく提供に消極的になる
・データの標準化ができておらず、複数医療機関からデータを収集してもスムーズに結合できない

解決方針：オプトアウトでの認定事業者に医療情報を提供可能
・「丁寧な」オプトアウトが推奨されているため、収集コストが嵩む課題は残る
・活用時には匿名化されているため、本人・利活用者ともにリスクは少ない
・認定事業者はEHRによってスムーズなデータ収集・結合が可能

02 匿名化
・個々の医療機関が、匿名加工基準が不明瞭なまま作業を行うため、加工データの分散が大きい（復元して検証できない）
・匿名加工を行った時点でデータの精度が低下する（特異値が欠損する可能性が高い）
・匿名加工データを収集しても名寄せができない

解決方針：認定事業者内で名寄せし、匿名化を行う
・匿名加工は認定事業者が行うため分散は少ない
・認定事業者内には医療機関から収集した元データが存在するうえ、目的に応じて匿名化を行うため、精度の低下を防ぐことができる
・認定事業者間で名寄せしたデータを匿名化するため、名寄せの課題はない

03 判断・判定
・個人情報保護委員会には、コンサルテーション機能が十分でなく、相談相手がいない
・倫理審査委員会、個人情報保護審査会のメンバーに専門家がいないケースが多く、基準も曖昧で判断の分散が大きい
・既存の医療DBも主体や利用目的の制限があり、利用できない組織が存在する

解決方針：目的や主体によらず利用が可能
・認定事業者が支援サービスを行う
・倫理審査委員会等の審査が不要であり、判断の分散は少ない
・医療分野の研究開発の為であれば、ビジネス目的であろうと利用制限はない

概ね解決可能なのだが、最大の課題は「保有データ量の少なさ」
研究内容によるが、現状では利用が困難との意見がある　※2021年2月時点では1万件程度と言われている

↓何故データ量が少ないのか？

医療機関：「丁寧な」オプトアウトにかかる手間を上回るメリットがない
国民：データ利活用の仕組み及びデータ提供に対するメリットを理解しておらず、データ提供のモチベーションがない

※仮にデータを（強制的に）集める他の方法を検討するにしても、国民の合意形成が困難

データ量を増やすには、提供者である国民がメリットを感じる事が重要であり、そのためにも理解を得られやすくなる「仕掛け」が必要である

④日本の課題の解決策：データ量を増やすには国民の理解が必要で、各国とも利活用によって得られるメリットと安心を得られるような対策を講じ理解を得ようとしている

各国政府の国民への理解の求め方概念図

参考）英国が医療DB化を進めた際の広報物（2011年）

大規模医療DB（HIE）の構築

情報保護
- 匿名化利用
- 利用者への罰則
- 利用者の監視

成果の還元（メリットの発信）
- PHR活用による健康増進
- 医療の効率化による医療費の削減
- 研究による医療の発展

個人の権利
- 同意撤回権等の制定
- 利活用実態の公開
- 相談、通報窓口設定

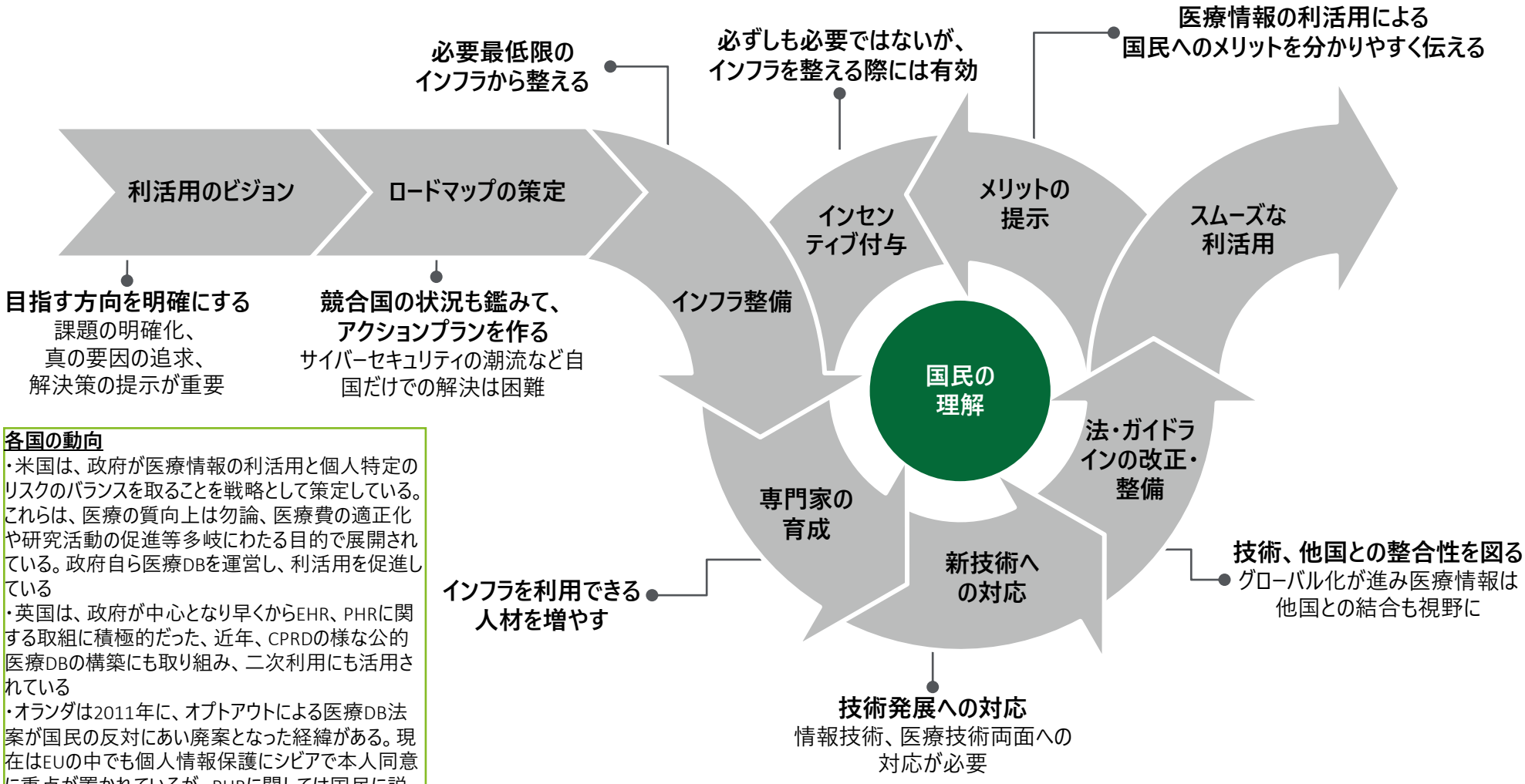
国民の理解を得るための総合的な取組み

ルールの明確化	データの電子化・標準化	インフラへのインセンティブ	罰則強化	権利拡充	情報公開
非識別化水準の明確化（US） 具体的なガイドライン（US・UK等） 相談窓口の拡充（ US・UK等）	電子化の推進（共通） データ標準の策定（共通）	EHR導入インセンティブ（US） EHR推奨（UK）	罰則公開（共通） 監視体制強化（共通） アクセスログ公開（NL・EE）	同意撤回権制定（共通） データポータビリティ（共通）	利活用実態の公開（共通） 通報窓口の設定（共通）

各国、目的や方策に違いはあるものの、医療情報利活用のメリットの説明と安心感につながるような対策を講じる事で、国民の理解を求めている

⑤今後の目指すべき方向：技術発展が著しく、ビッグデータ化が求められる現在、医療情報の利活用促進には国民の理解を中心にした総合的な整備・対策が必要と考えられる

医療情報利活用促進プロセス概念図



各国の動向

・米国は、政府が医療情報の利活用と個人特定のリスクのバランスを取ることを戦略として策定している。これらは、医療の質向上は勿論、医療費の適正化や研究活動の促進等多岐にわたる目的で展開されている。政府自ら医療DBを運営し、利活用を促進している

・英国は、政府が中心となり早くからEHR、PHRに関する取組に積極的だった、近年、CPRDの様な公的医療DBの構築にも取り組み、二次利用にも活用されている

・オランダは2011年に、オプトアウトによる医療DB法案が国民の反対にあい廃案となった経緯がある。現在はEUの中でも個人情報保護にシビアで本人同意に重点が置かれているが、PHRに関しては国民に説明を重ねながら半官半民での取組みを進めている

【参考】法律の確認：医療情報を利活用するには、個人情報保護法等の法律に従う必要があるが、学術研究機関以外の組織や学術研究目的以外の活用時に課題がある

日本における医療情報の第三者提供時のルールと課題

個人情報保護法が認める第三者提供可能要件

- 本人の同意
- 法令に基づく場合
- 生命や財産の保護に必要で同意取得が困難な場合
- 公衆衛生の向上のために必要で同意取得

個人情報保護法の適用除外：報道・著述・宗教・政治と並びに学術研究に関する適用除外の定めがある

行政および独立行政個人情報保護法が認める第三者提供可能要件

- 本人の同意
- 他の行政・独法に提供する場合で法令事務・業務に提供する場合
- 統計・学術研究の目的で提供する場合
- 第三者提供が明らかに本人の利益になる場合
- その他特別の理由がある場合

治療利用目的での第三者提供

・行個法、独個法では目的内利用で第三者提供が可能
・個人情報保護法では同意が必要→黙示の同意※1が認められている

研究利用目的での第三者提供

・本人の同意が必要
・ただし学術研究の際にはオプトアウトが可能※2
・個人情報保護法適用除外対象の学術研究機関と共同研究を行う機関も全て適用除外となると解釈されている

個人情報保護法の適用除外対象にならない組織（民間研究機関や一般医療機関など）は「同意」を取るか、個人情報保護法適用外の「匿名化」に頼るしかない

※1厚生労働省・個人情報保護委員会「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」
※2「人を対象とする医学的研究に関する倫理指針」（平成26年12月22日）

【参考】海外実態の確認①：5つの対象国いずれもPHRを目的としたHIEや医療DBの構築に積極的であり、特に米国と英国は医療DBを研究に活用できるよう法整備を行ってきた

調査対象国の医療情報利活用実態サマリー

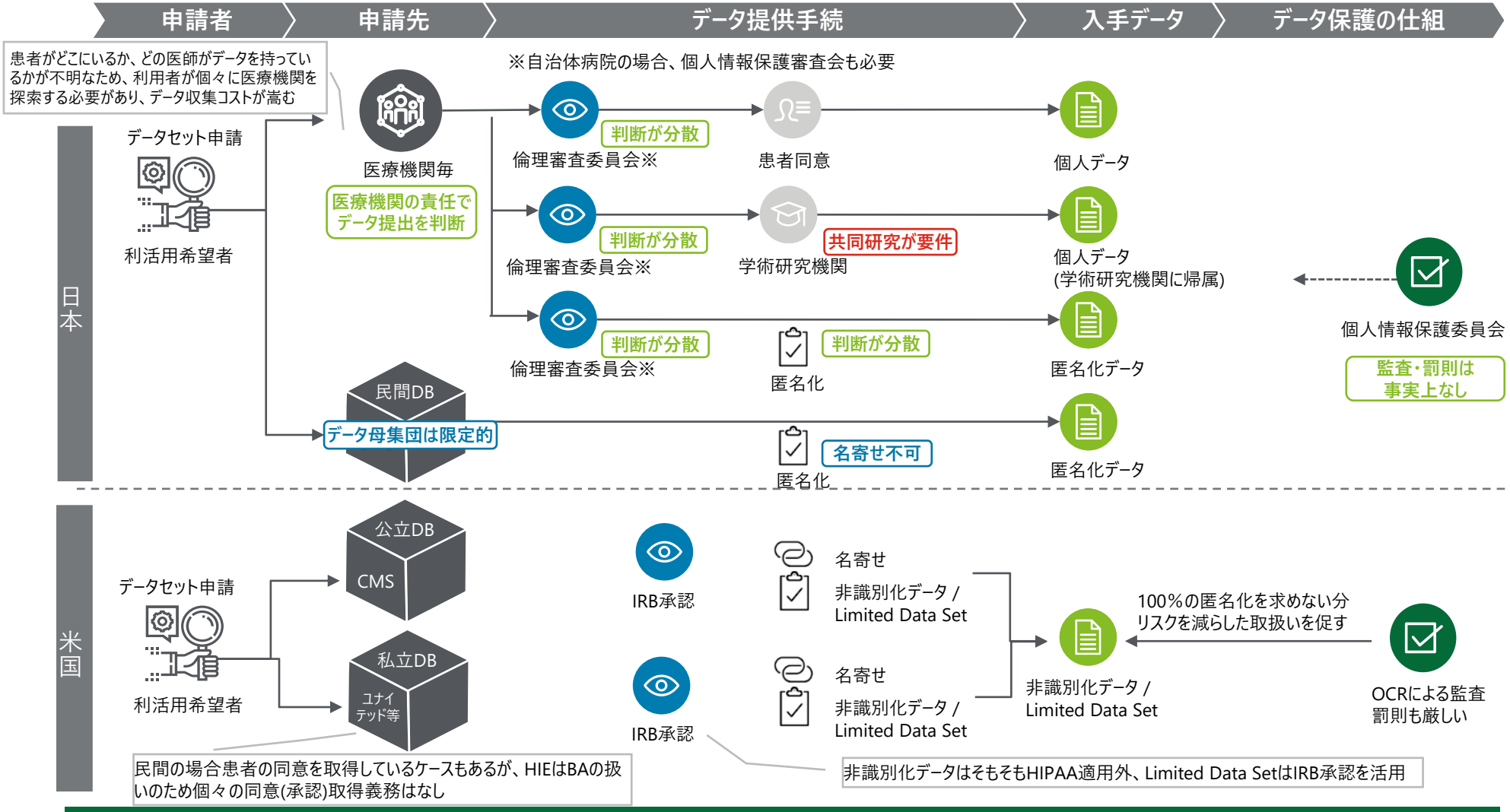
調査対象国	概要（研究目的での第三者提供時）
米国 （327,906）	大規模医療DBが官民で発達しており、医療DBが目的に応じて名寄せ、非識別化加工を行うため、研究目的利用時に個人情報が必要なケースがそもそも少ない。政府が医療情報の利活用と保護のバランスを取ると明言しており、セーフハーバー方式の非識別化など「分かりやすい」ルールを定めているうえ、医療情報の標準化にも積極的で、基準を満たしたEHRの導入にはインセンティブも提供している（現在は基準を満たさないと公的保険利用時の報酬を下げるディスインセンティブ方式）
英国 （67,172）	匿名化ルールなど日本同様に基準が曖昧なケースが多いが、罰則が厳しいため取扱い事業者の意識は高い。元々同意取得もしくは公益目的等による活用が中心であったが、近年政府がデジタル化を進めており、オプトアウト（ナショナル・データ・オプトアウト）で医療DB（CPRD、GPデータ中心）を構築し、利活用を進めている。この動きの中で医療情報の標準化にも積極的で、GP用のEHRは基準を満たしたサプライヤーをNHS Digitalが4社指定している
オランダ （17,060）	過去に政府がオプトアウトで医療DB整備しようとするも民意の反対で挫折。この影響が現在でも根強く残っており、治療目的時も含め、全体的に本人同意を重視する実態がある。政府としてもPHRは進めたいので官民で新たなHIE（LSP)を整備しているが、このHIEもオプトインで情報を収集している。これとは別に政府統計局であるCBSが医療情報を集約しており、非識別化データでの二次利用を可能としているが不十分との評価が多い
エストニア （1,323）	PHRや電子処方箋等、国民の健康増進と医療費の適正化のためにほぼ完全な電子化を進めてきた。公的医療DBへの情報提供を義務化している個別法などが存在するが、利活用周辺のルールが緩いわけではなく、むしろ医療DBのアクセスログが全て解析されるため不正閲覧に対する罰則などが厳しく整備されている。医療情報に関して特に治療目的では国外での利用も可能にすべく周辺国との連携も進めている
シンガポール （5,758）	他の4か国ほど、法整備が進んでいない（ガイドラインでの規定が多い）。国民の健康増進と医療費の適正化を目的としたPHRのための公的医療DB（NEHR）の構築には積極的に取り組んでおり、NEHRへの情報提供の義務化も予定されている。これまではさほど二次利用に積極的ではなかったが、DBの量の増大に伴い、他のデータとの統合を図ることで積極的に二次利用できないか検討している

（カッコ内）は2018年時点の人口。単位は千人。

国の規模や目的、過去の経緯によって状況は異なるが、研究目的での利活用に積極的な国は医療DBの構築に注力している

【参考】海外実態の確認②：特に医療DBの構築に積極的な米国と日本とでは、情報利活用プロセスが大きく異なるため、単純比較は困難である

研究目的での利活用希望者の医療情報利活用プロセスの違い



米国の利活用プロセスは「大規模DB」×「非識別化」が前提となっており、データ収集プロセスが日本とは大きく異なる