報告

Date: 2023.2.21
https://jilis.org/report/2023/jilisreport-vol5no4.pdf

EHDSと日本の医療データ保護法制への示唆

情報法制研究所理事
弁護士・ひかり総合法律事務所
板倉 陽一郎

私からは、EHDSとは何なのかという概要と解説、それから日本の医療データ保護法制への示唆が得られそうなところに絞りまして、その中身の解説をします。そして、個人情報保護法[1]の2020年[2]、2021年[3]の改正と、次世代医療基盤法[4]の5年見直し[5]についての示唆を述べていきたいと思います。

EHDS：欧州健康データスペースとは

まず、EHDSというのは、正式名称the European Health Data Spaceというもので、もともとは欧州連合の取り組みです。欧州連合の政府機関である、欧州委員会が提案したEuropean strategy for dataというのがあって、これは、データに関する色々な取り組みが入っているわけですが、その中で、欧州共通データスペースというのが提案されております。これはデータ保護の話というよりは、共通で使えるデータのうち、安全に共通に使えるデータの範囲をいろいろな分野で広げていこうというものです。どういう分野があるかということは後でお示しします。

その中で、最初にthe European Health Data Space、EHDSが規則の提案という形で出てきております。図にあるように、2022年5月3日に出たわけですが、Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Spaceとなっておりまして、この「規則」というのは、GDPRの"R"の「規則」と

欧州健康データスペース（the European Health Data Space: EHDS）とは

- European strategy for data（2020年）：欧州共通データスペースの提案
- 欧州健康データスペース（the European Health Data Space: EHDS）は欧州共通データスペースの最初の提案
  - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space(COM/2022/197 final)[**2022.5.3**]
- CBHC指令（14条）ではeHealth networkが提唱されているが，任意の取組みであり広がらず。
  - Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare

1） 個人情報の保護に関する法律（平成15年法律第57号）。
2） 令和2年法律第44号によるもの。
3） 令和3年法律第37号によるもの。
4） 医療分野の研究開発に資するための匿名加工医療情報に関する法律（平成29年法律第28号）。
5） 次世代医療基盤法附則5条。

一緒です。

個人データに関しては、元々1995年の欧州データ保護指令があって、2018年からGDPR、一般データ保護規則に切り替わっているわけです。ここで基本的な情報を提供しておきますと、指令というのは、各国がそれを法令等にして、みんなで守るというEUの法律の形です。一方、規則というのは、各国が議会を通さなくても、そのまま法律として適用されるというものです。ですので、GDPRは各国で同じGDPRをデータ保護機関が執行しているということになります。このEHDSについても、規則という形で提案されておりますので、これでできた法律をそのまま各国で適用しましょうという提案だということになります。

ヨーロッパって実はあまり広くないのですね。メルカトル図法で見ると、日本よりはるかに広そうに見えますが、実際に同じ縮尺で重ねてみると、そんなに広くないです。そうするとどうなるかというと、越境で出勤したり、越境でビジネスをしたりといったことが当然あるわけであります。ヨーロッパに行かれて電車で移動した方もおられると思います。例えばパリからブリュッセルまで、飛行機がなくても、電車で数時間で行けてしまうわけであります[6]。ですので、ヨーロッパでビジネスを展開する際に、30ヵ国のうち、いくつかの国で展開しようというのは自然な流れでありまして、それは健康データに関するビジネスであるとか医療についても、当然だということになってくるわけです。

なので、早いうちから、eHealth networkという形で医療の越境的な展開を可能にしようという取り組みがあったのですが、これは全くボランタリーというか、参加できる国は参加しましょうという形だったので、あまり広がらなかったと、EHDSの説明書で説明されています[7]。GDPRでいうデータ保護指令に相当するご先祖様にあたるのが、このCBHC指令の14条、eHealth networkだと考えられているようです。

EDPB-EDPSとは

今日の分析の対象になっているのは、図の左側のEHDSの規則と、もう1つ、しばしば私が「EDPB-EDPSの意見です」と引用しているものがあります。これは2022月の7月12日に出たEHDSに対するEDPBとEDPSのジョイントの意見です[8]。

EDPBだEDPSだと、略語ばっかりでなんだという方もおられるかもしれないので、若干説明します。EDPBもEDPSも、欧州連合の機関のひとつであります。EDPBは、ヨーロッパのデータ保護機関の集


EUROPEAN COMMISSION

Strasbourg, 3.5.2022
COM(2022) 197 final

2022/0140 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Health Data Space

(Text with EEA relevance)

{SEC(2022) 196 final} - {SWD(2022) 130 final} - {SWD(2022) 131 final} - {SWD(2022) 132 final}

EN EN

6) 例えば，パリ北駅を30分ごとに発車しているTHALYSで1時間20分ほどである。

7) 「電子健康データの二次利用に関しては、eHealth networkの活動は非常に限定的であり、あまり効果的ではなかった。ビッグデータに関するいくつかの非拘束的な文書は、さらなる具体的な行動によってフォローアップされず、その実践は非常に限定的なままである。」とされている（EHDSのEXPLANATORY MEMORANDUM，以下，「EM」3.）。

8) EDPB-EDPS Joint Opinion03/2022 on the Proposal for a Regulation on theEuropean Health Data Space, Adopted on 12 July 2022(以下,「EDPB-EDPS意見」)。

まりです。GDPRを執行しているのが、各国のデータ保護機関で、著名なのはフランスのCNILとか、ドイツの連邦データ保護監察官と呼ばれている、これは独任制の機関になるわけですが、データ保護のトップであるとか、イギリスだとICO、Information Commissioner's Officeというのがあります。こうした機関や事務局がデータ保護法を執行しているわけです。彼らの集まりがEDPBというもので、GDPR上もさまざまな権限を与えられています。昔は29条作業部会と呼ばれていたものですが、GDPRが施行されて、EDPBは正式に欧州連合の機関のひとつになりました。

一方、EDPSは、European Data Protection Supervisorという人でありまして、これは、欧州連合の各機関にとってのデータ保護機関、つまり、フランスにとってのCNILに相当するような欧州連合の欧州委員会等の機関のデータ保護を監督するデータ保護機関ということになります。欧州連合所属の民間事業者というのは、基本いませんから、欧州連合所属の公的部門を監督している人ということになるわけです。また、単にそれのみにとどまらず、データ保護界の上がりポストのひとつみたいな感じで、欧州の各国のデータ保護機関の中でも、代表的な人が最終的にEDPSになっているということが多いです。

EDPBも、EDPBの議長というのは、やはり欧州のデータ保護機関の中でも評価が高い方がなります。データ保護のカンファレンスにEDPBの議長やEDPSの方が出てくると、バシッと締まるというようなところがあります。

このEDPB-EDPSがデータ保護の観点から、EHDSについて、2022年7月時点でのコメントをしているというのが、この図の文書であります。EHDSは100ページ程度、右側の意見は30ページぐらいのボリュームです。

COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces(SWD(2022) 45 final)

Annex 1: Common European Data Spaces – Timeline

The blue **colour** represents legislative and political initiatives. The green **colour** represents funding initiatives of the Commission. The brown **colour** describes other actions.

こちらの図が、先ほどの the European Health Data Space です。どんな分野があって、今、どんなタイムラインを考えているのかという欧州員会の事務局資料です。

どのようなスペースが考えられているかというと、製造業、環境、交通、それから今回のヘルス、そのほか、金融、エネルギー、農業、公共公益といった分野が並んでおります。それぞれの分野で、こんなことをやったらどうかというような計画が出ているわけです。例えば、Mobility（交通）のところには、輸送データについてのパイロットプログラムを2021年から2022年ぐらいかけてやりましょうといったことが書いてあったりします。

Health のところを見ていただくと、自分の健康データ、患者の健康データのアクセスの実験である、MyHealth@EU というパイロットについて書かれています。この MyHealth@EU というのが後の説明には全然出てこないのですけど、これは何なのかというと、EU の各加盟国間で健康データを連結して、アクセスするための枠組みであります。

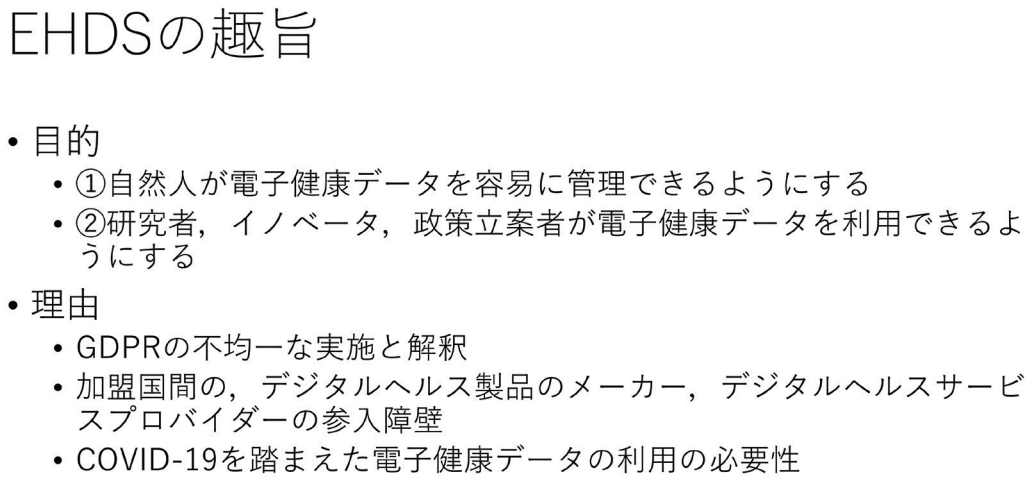
さらに2022年の計画としては、健康データの二次利用の基盤についてのパイロットが入っていたりします。

この元になる法令、規則が今、最初に提案されているというところであります。さまざまな分野の中で、Health が最初に来たということです。GDPR では、健康データは特別カテゴリデータに入っていて[9]、全然使えないわけです。GDPR だと、もうほとんど不可能なぐらい、厳しい要件が課せられているわけであります。だからこそ、加盟国を通じた特別法として、こちらが必要になったのでしょう。だから、難易度が高そうではあるが、Health から始まったのだということができるかなというところであります。

EHDS の趣旨

1つは、自然人が電子健康データを容易に管理できるようにするということです。もう1つは研究者やイノベーター、政策立案者が、電子健康データを利用できるようにする。この2つを両立しないといけないというところから EHDS が始まっています。

その理由は、あまり整理されていなくて、バラバラと書いてあります。1つは、なかなか面白いのですが、欧州連合は GDPR を制定しました。データ保護指令に基づいて、各国がデータ保護法を作ってというような体制では、デジタルシングルマーケットと言っていますが、欧州の統一市場との関係で、不便です。先ほども申し上げましたが、ヨーロッパでは国境を越えて出勤するといったことがコロナ前は当然でしたし、企業がある程度のボリュームを持って展開しようと思ったら、何ヵ国かに展開するのは当然であるという中で、データを使ったビジネスをやるというような際には、各国バラバラなのは、非常にビジネスにも問題があるし、人権保障という意味でも、レベルが違うというのは不適切だというのがあって、GDPR にしたわけです。したわけですが、データ保護機関の執行は、EDPB があったり、いろいろな集まりがあったりして、それなりに横のつながりはありますが、全部一緒ではないわけですね。そもそもデータ保護機関というのは、その国の行政機関から独立し



9) GDPR9条（特別な種類の個人データの取扱い）は，1項で，「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される。」（個人情報保護員会仮訳。以下GDPRの条文につき同じ。）と定めている。

て権限を行使しているので、他のデータ保護機関からもEDPBなどの枠組みで、法理的に義務付けられていない限りは、こういう風に執行しろと義務付けられることもなく、独立性が保たれているわけです。

それからもう1つ、GDPRのかなりの箇所で、―データ保護指令はすべて国内法化しなければならなかったわけですが―、各国に委ねられている部分というのがあるわけです。欧州委員会がそもそも権限を持ってないような部分、例えば罰則が最も典型的ですが、罰則は各国でしか科せられないので、GDPRに罰則についてのガイダンス的な条文はありますが[10]、それに基づいて、各国がデータ保護法に基づいた各国のデータ保護法で定めていたりするわけです。健康データのあたりは、実施がバラバラで、解釈もバラバラです。

各国でEHDSが言っているセカンダリーユース、二次利用をどうやって許しているのかといったようなものを調べた調査などもあるのですが[11]、ある形態の利用について許されるのか許されないのかというのは統一されていません。逆説的ではありますが、GDPRが不均一に実施され、解釈されていることから、結局2段階目のEHDSが必要になったのだという内容が説明書きのところで述べられています[12]。このような状態になると何が起きるのかというと、加盟国、ヨーロッパのどこかの国でビジネスをやろうと立ち上げたデジタルヘルス製品のメーカーであるとか、デジタルヘルスサービスのプロバイダーが、他の国に参入しようとすると、参入障壁になるというのがあります。もう1つは、Covidの対応など、公衆衛生というのは、基本的に警察と一緒で、欧州委員会は権限を持っていなくて、各国の権限ですが、国境を越えて、コロナの対策のためのデータを共有したり、患者さんがヨーロッパの他の国の出先で、コロナにかかって、現地の出身国の方のカルテがいるのだといったような事態が、通常の時に比べれば非常に多く発生したわけです。この時にはやはり電子的に健康データが整備されていて、必要があればアクセスできるということが必要だということが認識されました[13]。こういうモチベーションからEHDSが提案されてきている、そういう状況にあります。

他の法令との関係はどうなっているのか

EHDSの説明書の中からデータに関係するところを引っ張ってきたのがこちらの図です。

EUDPR[14] は、EUの行政機関、欧州委員会等の行政機関に限らず、EUの機関のデータ保護を定めた規則です。GDPRは皆さんご存じの通りで、ePrivacy

他の法令との関係（データ関連）

- GDPR，ePrivacy指令，EUDPR
  - GDPR及びEUDPRに「完全に準拠」
  - 健康情報がGDPR上の「特別な種類のデータ」であることを前提に，「権利の実施を支援」するとされる。特にポータビリティ権は強化されている。
    - EDPB-EDPSはePrivacy指令に言及がないことを指摘（26項）。
- データガバナンス法，データ法（案）
  - データガバナンス法
    - 公共部門のデータの二次利用のための一般的な条件を定める
  - データ法
    - ポータビリティを強化する
  - これらを保管し，医療のより具体的なルールを提供
- NIS指令，サイバーレジリエンス法提案

10）GDPR83条9項等。

11）“Report on secondary use of health data through European case studies”, 28 February 2022, https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf

12）「加盟国によるGDPRの不均一な実施と解釈は、かなりの法的不確実性を生み出し、電子健康データの二次利用を妨げる結果になっている。したがって、研究者、革新者、規制当局、政策立案者が必要な電子医療データにアクセスすることを妨げる障壁のために、自然人が革新的な治療の恩恵を受けられず、政策立案者が健康危機に効果的に対応できない状況が生まれる。」（EM 1.）。

13）「COVID-19の大流行により、国家レベルでの既存の技術的専門知識を基にした相互運用性と調和の緊急の必要性と高い可能性が明らかになった。」（EM 1.）。

14）Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), PE/31/2018/REV/1

指令[15]は、電気通信分野のデータ保護についての指令です。ePrivacy規則案[16]がなかなか通らないというのも、広くデータ保護を勉強されている方はよくご存じだと思います。EHDSの説明書きで、GDPR及びEUDPRには完全に準拠していると書かれています[17]。何が準拠なのか、よくわからないところもありますが、健康情報はGDPR上の特別カテゴリデータ、特別な種類のデータであるということを前提に、GDPR上の権利の実施を支援するという法律であるとされています[18]。特にデータポータビリティ権が強化されているというのは、EHDSの権利コーナーを見るとわかります。GDPRの権利コーナーは12条から23条にあり、GDPRの条文の中でも多くを占めていますが、EHDSでは3条に権利の話が書いてありまして，GDPRのポータビリティ権よりも、さまざまな面で強化された多数のポータビリティ権が定められています。健康データに関して、オンラインサービスであるとか、アプリを使ったサービスがありますので、ePrivacy指令との整合性も必要なのではないかということを、EDPB-EDPSからは指摘されています[19]。今のところ、EHDSの説明のところには確かにePrivacy指令との整合性が含まれていません。

それからもう1つ、関係してくるデータガバナンス法[20]とかデータ法案[21]、こちらとの関係でも、具体的なルールであると整理されています。データガバナンス法は、2次利用の一般条件が定められています。一方、データ法案には、個人データに限らないポータビリティの話が入っていたりします。確かにこれらとの関係では、医療でより具体的なルールを提供しているという側面が存在します。

それから、NIS指令[22]とか、サイバーレンジエンス法案[23]といった、サイバーセキュリティの関係の法律または提案との関係でも、特別な部分があるのだと説明書に書いてあるわけであります。

GDPRとの関係

GDPRとの関係をもう細かく見ていきましょう。

GDPRとの関係①

- 第9 条 特別な種類の個人データの取扱い
  - 1. 人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される。
  - 2. 第1 項は、以下のいずれかの場合には適用されない。
  - (a)-(f)　略
  - **(g) 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、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定めるEU 法又は加盟国の国内法に基づき、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) 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、かつ、第3 項に定める条件及び保護措置に従い、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) データ主体の権利及び自由、特に、職務上の秘密を保護するための適切かつ個別の措置に関して定める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) 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、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める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。**
  - 3.-4.（略）

15）Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

16）Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017, COM(2017) 10 final, 2017/0003 (COD)

17）「EHDSでアクセスされる相当量の電子データがEU内の自然人に関する個人健康データであることを考慮し、本提案はGDPRだけでなく、規則（EU）2018/1725（EUデータ保護規則）にも完全に準拠して設計されている。」（EM 1.）。

18）「EHDSは、電子医療データに適用されるGDPRに明記された権利の実施を支援する。」（EM 1.）。

19）EDPS-EDPB意見5.

20）Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), PE/85/2021/REV/1

21）Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final

22）Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), PE/32/2022/REV/2

23）Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Text with EEA relevance) Brussels, 15.9.2022, COM(2022) 454 final, 2022/0272 (COD)

GDPRとの関係②

- 第6 条 取扱いの適法性
  - 1. 取扱いは、以下の少なくとも一つが適用される場合においてのみ、その範囲内で、適法である：
  - (a)-(b)略
  - **(c) 管理者が服する法的義務を遵守するために取扱いが必要となる場合。**
  - (d)　略
  - **(e) 公共の利益において、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に取扱いが必要となる場合。**
  - **(f) 管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く。**
  - 2.-3.（略）

第9条が、EHDSとの関係では重要です。

「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い」を挙げた上で、そのあと「並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータ」と、こういったものが、特別カテゴリデータに入り、これに関するデータの取り扱いは禁止です、となっています。禁止ですと言っても、そもそもGDPRは個人データの取り扱いも原則禁止なので、そんなに驚かなくてもいいかなというところがあります。ここには書かれていないですが、原則明示的な同意じゃないとダメだという風になっているわけですね。

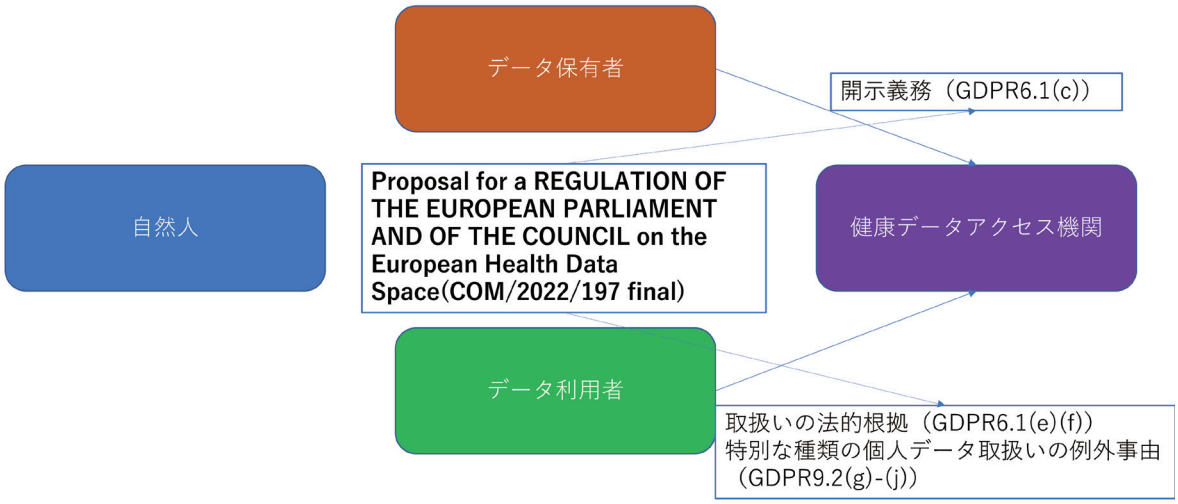
EHDSの前提として、明示的な同意だけでは健康関連のデータの取扱いは色々回らない。特に二次利用については回らないという認識があるわけで、9条2項の適法化事由がaからjまであるわけですが、EHDSに従った取扱いは、健康関連データの取扱いとの関係で、これらの除外事由にあたるという整理がされています。例えば、gは重要な公共の利益のためにEU法があれば、その範囲で使えるとなっています。それからhは、予防医学や産業医学、それから医療診断、社会福祉、治療の提供といったもののためのEU法に従って使う分には使えますとなっています。iは、公衆衛生に関係するような医療や医薬品の開発等となっています。jは、研究ですね。「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使う場合」といったような除外があるわけです。この除外のセットとしてのEU法として、EHDSはできているのだという整理がされています。

一方、第6条で、普通の個人データの取り扱いについて根拠がいるわけです。通常、GDPRについて議論しているときには、Webサービスを念頭に置いていることが多く、大体、aとbとfぐらいしか使わないですね。aは同意、bは契約に従う場合、fが正当な利益です。大体同意が取れないので、正当な利益でなんとかなりませんかみたいな相談になって、ええ～となっているのが多いのですが、今回は全然話が違います。

例えば、「管理者が服する法的義務を遵守するために取扱い」。これは、この法律の監督をする、医療データアクセスのための公的部門ですね。こちらがやることというのは、もう公的機関の法的義務として与えられているので根拠になるといわれていたり、それから、データ利用者という名前で出てきますが、2次利用をそのアクセス機関に申し込む。使いたい人たちはe（公共の利益）かf（正当な利益）が根拠になる、と考えられていますので、eなのか、fなのかを自分で定めて申し込んだりする、ということになっています。

健康データアクセス機関とその役割

アクセス機関への申し込みというのをもう少し詳しく説明しますと、データ利用者は、病院などのデータ保有者に対して、データを使いたいのだとお願いをします。これを「健康データアクセス機関」を通じてやることになっています。健康データアクセス機関はデータ利用者の申し込みに対して審査をします。審査が通ったらデータ保有者の方に、このようなデータを出してあげてください、と連絡します。これがEHDSの二次利用ですが、データ利用者が健康データアクセス機関を通じてデータを使うというようなところが、先ほどの6条でいうと、e、fにあたります。



それから、特別な種類の個人データは同意で使うにしても、明示の同意を取らないといけないから、ほとんど使えなかったわけですけど、このgからjの仕組み自体が、例外のEU法にあたるからクリアするというようなカラクリで使えるようにしているわけであります。健康データアクセス機関がデータ保有者にデータ出してくださいというのは、公的部門に与えられた義務だということで、データ保有者はこれに対して出さなきゃいけないということになります。これでさまざまな禁止がクリアされるのだと説明されています。

EHDS の概要

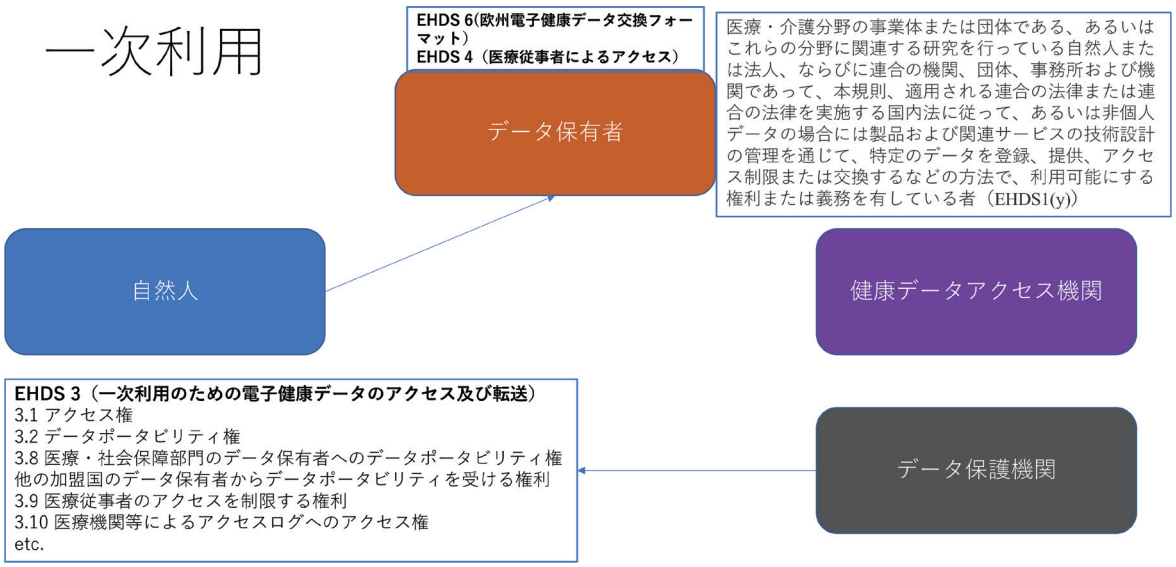
第1章が一般条項で、定義がずらっと並んでいます。GDPRもかなり定義が並んでいましたが、Yとか、アルファベットが終わるくらいまで並んでおり、そのうちの一部は、データ法を参照、データガバナンス法を参照、GDPR参照などとなっています。第2章は一次利用。これは、普通の医療などの提供のための利用で、EHR、Electric Health Recordを標準化して、同じフォーマットでやりましょうというのがメインです。第3章は、EHRシステム、ウェルネスアプリケーションなどについてのさまざまな定めです。第4章が二次利用で、これは先ほど説明したように、研究などの際に利用申し込みとその情報が提供されるというような仕組みです。2章と4章を主として、この後、若干細かく見ていきます。

それから、5章、6章、7章、8章と、割と手続き的、行政組織的な規定が色々入っていて、最後に最終規程という形になっています。まだ提案なので、どれぐらい細かく見るかというのはありますが、ただこの提案の大まかな仕組みが参考になりますので、見ていきたいと思います。

まず個人の権利が非常に強化されているというよ

EHDSの概要

- 第1章　一般条項
- 第2章　電子健康データの一次利用
- 第3章　EHRシステム，ウェルネスアプリケーション
- 第4章　電子健康データの二次利用
- 第5章　追加的措置
- 第6章　ガバナンスと協力
- 第7章　委任立法とコミッティ
- 第8章　雑則
- 第9章　経過措置と最終規定



うなことを述べましたが、それがEHDSの3条です。3条の1項が強化されたアクセス権です。3条の2項が強化されたデータポータビリティです。さらに、データポータビリティ権の特別な場合が、3条の8項～9項に色々入っていて、例えば、医療社会保障部門のデータ保有者へのデータポータビリティ権というのがあります。これは要するに公的部門や病院などがデータを保有しているときに、これを他の病院に行くからといった理由でそこにデータを送ってくれという権利です。他の加盟国のデータ保有者から受け入れるという権利ですね。例えば外国で医療にかかりました。このデータを使ってくださいと言って今かかろうとしている医療機関にデータを渡させる権利であります。3条9項が面白いのですが、一種のオプトアウトなんですね。医療従事者のアクセスは―この医療従事者の定義は後で問題になりますけど―、医療従事者のアクセスは、ここで出てくるEHRについてはできるというのが原則になっているのですが、医療従事者のアクセスも嫌だというような場合には、この権利を行使して除外するようです。それからアクセスログですね。これは、医療機関であるとか、医療従事者が、その人のフォーマットが統一されて、アクセスログが全部管理されているはずのEHRにアクセスした時のログを見たいということができるようにしましょうとなっています。

この3条等の個人データに関する権利の部分は、データ保護機関が監督をするという定めになっています。それ以外は健康データアクセス機関、これはどこかの公的部門が担当することになり、その健康データアクセス機関が本人の権利以外の部分の監督執行を担当しますということになっています。

それ以外に「データ保有者」という概念が出てきます。このデータ保有者というのはGDPRで言うとデータコントローラーにあたるのですが、微妙に違います。データコントローラーと言ってしまうと、GDPR上の用語なので、違う名前を使っているのではないかと思いますが、ここだけ重要な概念なので、条文を引っ張ってきています。図の右上のEHDS1(y)という箇所です。ここで「医療・介護分野の事業体または団体である、あるいはこれらの分野に関連する研究を行っている自然人または法人、ならびに連合の機関、団体、事務所および機関であって、本規則、適用される連合の法律または連合の法律を実施する国内法に従って、あるいは非個人データの場合には製品および関連サービスの技術設計の管理を通じて、特定のデータを登録、提供、アクセス制限または交換するなどの方法で、利用可能にする権利または義務を有している者」と、こういう定義になっています。「権利または義務」というのは要するに、責任を有しているということです。

その中で、欧州電子健康データ交換フォーマットで標準化しようとしていたり、医療従事者によるアクセスは基本的には確保されるとされています。医療従事者にはさまざまな方がいますので、その範囲については各国法で定めて、原則、必要なアクセスは確保されるような定め方になっている。これが一次利用です。

一次利用の対象となるデータ

どんな項目が一次利用の対象になっているのかというと、患者の概要ということで、年齢とか住所とか基本的なデータ。それから処方箋と処方箋に応じてなされた調剤。医用画像、画像の報告書、検査結

一次利用される電子健康データの項目（EHDS 5.1）

- (a)　患者の概要
- (b)　電子処方箋
- (c)　電子調剤
- (d)　医用画像，画像報告書
- (e)　検査結果
- (f)　退院報告書

果、退院報告書。これが基本的に一次利用として医療従事者は共有する、使えるようになる電子健康データの項目とされています。

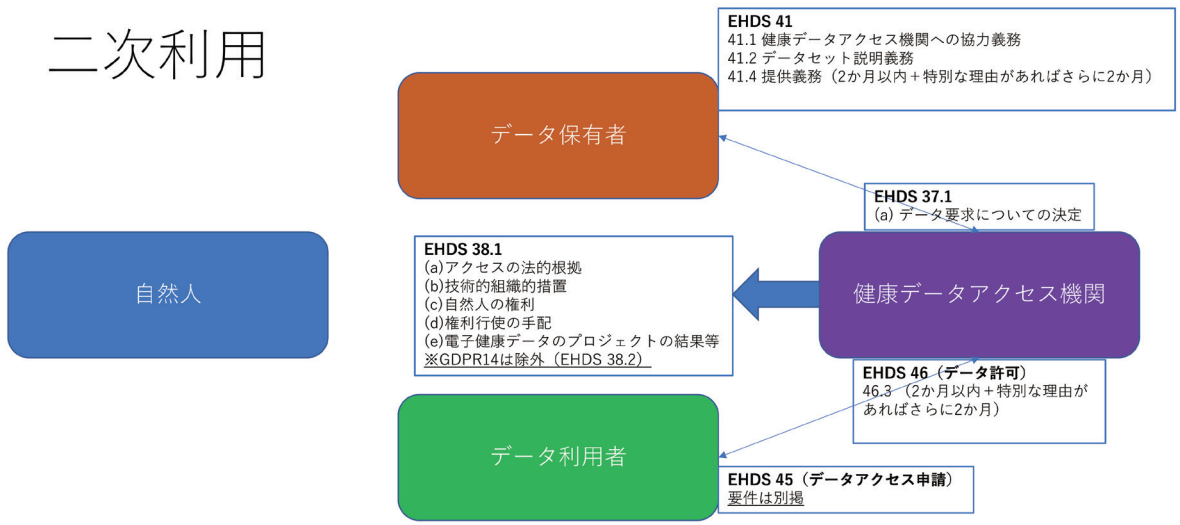
ここに同意とかは全然出てこないです。基本、医療従事者は見られるという前提でやっています。同意ではなくて、オプトアウトという言い方はしていないけど、医療従事者の拒否の権利という中で、おそらく調整するのでしょう。例えば外科のお医者さんには見られたくないとか、そういう設定ができるのかなと思いました。

二次利用の対象となるデータ

二次利用のほうがややこしいです。どのような仕組みになっているのかと言うと、「データ利用者」と「データ保有者」が出てきます。

データ保有者は医療機関や、医療に関する研究を行っている機関、健康保険とかを取り扱っている役所などです。データ保有者が保有しているデータを使いたい者をデータ利用者と呼んでいます。データ利用者は、データを使うための目的その他の事項を記載した申請書を作成し、健康データアクセス機関に申請をします。これをデータアクセス申請と呼びますが、これに対する対応は、許可するか、許可しないかですね。

これに対して健康データアクセス機関が2ヵ月以内に応答する。情報公開請求っぽいですよね。特別な理由があると、さらに2ヵ月以内は応答を延長できますが、4ヵ月以内には絶対返事するということですね。健康データアクセス機関が、申請を受け入れるとなると、データ保有者を名指してくるわけですね。例えば、日本だったら東京大学病院の何やらのデータを使いたい、みたいな申請を―日本にはないのですが―、健康データアクセス機関にお願いするわけですね。そして、この申請は通した方がいいとなると、健康データアクセス機関がデータ保有者に対して出してくださいと言うわけですので、ここは法的義務になっています。



たぶん、これからもいろいろ揉めると思いますけど、EHDSの41条で出しなさいってことになっている、提供義務があると。データ保有者の応答のための期間が2ヵ月、特別な理由があるとさらに2ヵ月なので、マックス4ヶ月です。だから申請が受け入れられるとしても最大8ヵ月かかってしまうのですが、データ保有者からデータが出てくるということになります。このデータ保有者のほうに諸々の義務がかかっています。例えばデータセットの説明の義務。これは日本で言うと個人情報ファイルを公表する義務みたいな感じです。どんなデータセットがあって、ラベルがどんなもので……というのを公表しないといけません。

それから、一般的な義務として、この健康データアクセス機関には協力してねというのが入っていたりします。これを通じてデータ利用者は適切な目的だということになると、データが得られます。これをどういう形式で行うのかというは、この後ご説明しますが、ここまでで、本人の出てくる余地はほとんどありません。

GDPRは、13条や14条で透明性確保義務があります。日本で言うと利用目的の通知公表や保有個人データについての開示事項などに対応します。日本法は、令和2年改正で安全管理措置も増えましたね。そういったものをインフォームしないといけませんということで、今、みなさんプライバシーポリシーとか書いていただいているかと思います。

データ保有者の方で公表しないといけないのかと言うと、不要です。健康データアクセス機関のほうで法定の公表事項があるだけということになっていまして、それがこの38条1項ですね。

どんなアクセスの法的根拠でデータが出ていくのか、技術的、組織的な安全管理装置をどんな風にとっているのか、自然人の権利としてはどんなのがあるかとか、権利行使するのだったら繋ぎますよとか、それからこの電子健康データで何らかの研究とかをやったプロジェクトとかがあったら、その結果を公表する。このような形で、集団的に透明性を確保するようなやり方になっています。

では、自然人は権利行使が全然できないのかというと、38条1項のcに自然人の権利というのがありますから、行使はできますが、データ利用者に提供されるデータというのは、原則、匿名化データ、ここで言う匿名化データというのは、日本の匿名加工情報とは違って、個人データじゃないという意味なので、統計に近いような、特定の個人との紐付けなくなっているデータです。例外的に仮名でないと目的が達成できないとなると、仮名化データになりますが、仮名化データも、これは日本の仮名加工情報の元ネタなので似ていますけど、権利行使が制限されることが想定されています。また自然人の権利としては、データ保有者のほうに、権利行使するんだったらする、おそらくそういう仕組みなのだろうと思います。これも具体的に中身を見ていきます。

二次利用されるデータのカテゴリ

どんなカテゴリについて出さないといけないか、これは非常に広いですよね。EHRそのもの、EHRの中身には、処方箋などが入っていましたけど、あれ全部ということでしょうね。それから健康に影響を与えるデータ、社会的、環境的な健康の行動決定要因を含むといったデータ。それから、ヒトの健康に影響を与える、関連する病原体ゲノムデータ。請求データ及び診療報酬データを含む、健康に関連する行政

二次利用される電子健康データの最小限のカテゴリ（EHDS 33.1）

- (a) EHR
- (b) 健康に影響を与えるデータ、社会的、環境的な健康の行動決定要因を含む。
- (c) ヒトの健康に影響を与える、関連する病原体ゲノムデータ。
- (d) 請求データ及び診療報酬データを含む、健康に関連する行政データ。
- (e) ヒトの遺伝子、ゲノム及びプロテオミクスデータ。
- (f) 医療機器、ウェルネスアプリケーション又はその他のデジタルヘルスアプリケーションを含む、人が生成した電子健康データ。
- (g) 自然人の治療に関与する医療専門家に関連する識別データ。
- (h) 集団全体の健康データレジストリ（公衆衛生レジストリ）。
- (i) 特定の疾患に関する医療登録からの電子的健康データ。
- (j) 臨床試験からの電子健康データ。
- (k) 医療機器からの電子健康データ、医薬品及び医療機器に関する登録からの電子健康データ。
- (l) 健康に関連する研究コホート、質問票及び調査。
- (m) バイオバンク及び専用データベースからの電子健康データ。
- (n) 健康に関連する保険状況、職業状況、教育、ライフスタイル、健康状態及び行動データに関する電子データ。
- (o) データ許可証に基づく処理後にデータ保有者が受け取った、修正、注釈、リッチ化などの様々な改良を加えた電子的な健康データ。

データ、レセプトですよね。ヒトの遺伝子、ゲノム及びプロテオミクスデータ、タンパク質ですね。医療機器、ウェルネスアプリケーション又はその他のデジタルヘルスアプリケーションを含む、人が生成した電子健康データ、FitBit などのデータですね。

それから、自然人の治療に関与する医療専門家に関連する識別データというのは、お医者さんに番号が振られていたらそれが該当します。それから集団全体の健康データレジストリ（公衆衛生レジストリ）は、全体の公衆衛生としての登録です。特定の疾患に関する医療登録からの電子的健康データの登録ですね。臨床試験からの電子健康データ。それから医療機器からの電子健康データ、医薬品及び医療機器に関する登録からの電子健康データ。健康に関連する研究コホート、質問票及び調査。バイオバンク及び専用データベースからの電子健康データ。健康に関連する保険状況、職業状況、教育、ライフスタイル、健康状態及び行動データに関する電子データ。データ許可証に基づく処理後にデータ保有者が受け取った、修正、注釈、リッチ化などの様々な改良を加えた電子的な健康データとなっています。

データアクセスを申請する際の項目

これは、利用者がデータアクセスを申請する際に書く項目です。どの目的で使いたいかということです。それから、どの範囲で求めているか。データソースも可能な場合は記載することとなっています。それから、匿名化されたフォーマットでいいかどうか。c と d はセットっぽいのですが、d は原則、匿名化されたデータです。個人データではなくなるところまで加工します。

どうしても仮名でなくてはいけない場合は、仮名でなきゃいけない理由というのが d です。e は、目的外利用を防ぐための措置、どんなことやっていますかということです。これは例えば、関係する従業員と守秘義務の契約を結んでいます、組織的な措置を取っていますといった、そういうことを書きます。同じように自然人の権利利益を保護するための保護措置。それから、g は、どれぐらいの期間使いますかということ。h は、コンピューティングリソースが準備されていて、安全に取り扱いますという説明です。a の目的のところ、何が許されるかは、日本でも二次利用を設計する時にどれを入れてどれを入れないのか、一番揉めるとこだと思います。

二次利用の処理目的

今のところ、EHDS が 34 条 1 項で、a から h まで定めているのは、例えば、a は「国境を越えた健康への深刻な脅威に対する保護、公衆衛生監視、ヘルスケア及び医薬品又は医療機器の高い品質と安全性の確保など、公衆衛生及び労働衛生の分野における公共の利益のための活動」と、割と国側でやらなければならないものですね。b は、日本でいう厚労省みたいな公共部門が法的にやらなきゃいけないことを遂行しなくてはいけないという話です。c は統計の作成。この a から c は、他に法律で権限がないといけないことになっていますので、私がやりたいのですというだけではダメということですね。公的部門の権限として、各国が定めていることが必要になります。d 以下には、民間事業者も出てくるわけですけど、保健医療部門における教育指導活動、大学で授業に使いたいとかですね。最長で 8 か月かかるのにどうかって

データアクセス申請のための項目（EHDS 45.2）

- (a) 第 34 条第 1 項で言及されているどの目的のためにアクセスが求められているかを含む、電子医療データの意図された使用についての詳細な説明。
- (b) 複数の加盟国からデータが要求されている場合、地理的範囲を含む、要求された電子健康データの説明、そのフォーマット及びデータソース（可能な場合）。
- (c) 匿名化されたフォーマットで電子医療データを利用可能にすべきかどうかの表示。
- (d) 適用可能な場合、仮名化された形式での電子健康データへのアクセスを求める理由の説明。
- (e) 電子健康データの他の利用を防止するために計画されたセーフガードの説明。
- (f) データ保有者及び関係する自然人の権利及び利益を保護するために計画された保護措置の説明。
- (g) 電子的健康データが処理のために必要とされる期間の見積もり。
- (h) 安全な環境に必要なツール及びコンピューティングリソースの説明。

二次利用の処理目的（EHDS 34.1）

- (a) 国境を越えた健康への深刻な脅威に対する保護、公衆衛生監視、ヘルスケア及び医薬品又は医療機器の高い品質と安全性の確保など、公衆衛生及び労働衛生の分野における公共の利益のための活動。
- (b) 保健又は医療分野の公共部門機関又は連合機関、規制当局を含む機関及び団体が、その任務において定められた任務を遂行することを支援すること。
- (c) 医療又は介護分野に関する国内、多国間及び連合レベルの公的統計の作成。
- (d) 保健又は医療部門における教育又は指導活動。
- (e) 医療又は介護分野に関する科学的研究。
- (f) 公衆衛生若しくは社会保障に寄与する製品若しくはサービス又はヘルスケア、医薬品若しくは医療機器の高い品質及び安全性を確保するための開発及び技術革新活動。
- (g) 医療機器・AIシステム及びデジタルヘルスアプリケーションを含む、公衆衛生若しくは社会保障に寄与する、又はヘルスケア・医薬品若しくは医療機器の高い品質及び安全性を確保するためのアルゴリズムの訓練・試験及び評価。
- (h) 他の自然人の健康データに基づき、自然人の健康状態を評価、維持又は回復することからなる個人向けヘルスケアを提供すること。

- (a)-(c)は権限の範囲内で認められる（EHDS 34.2）

いうのはありますけど、しかしながら、ここで出してもらったデータで、例えば、何ヵ月間のトレーニングコースを行うといった場合、十分これは考えられるでしょう。それから、医療介護の科学的研究、メインのところですね。fは、サービスやヘルスケアの開発、イノベーションですが、制限がかかっていまして、「公衆衛生若しくは社会保障に寄与する」となっています。みんな、「うちは公衆衛生に寄与する」って言うでしょうけど、ラインを引くのは結構難しいのかなと思います。次のgもそうですよね。「医療機器・AIシステム及びデジタルヘルスアプリケーションを含む、公衆衛生若しくは社会保障に寄与する、又はヘルスケア・医薬品若しくは医療機器の高い品質及び安全性を確保するためのアルゴリズムの訓練・試験及び評価」ですから、学習データで使いたい、テストデータで使いたいといったことになるのでしょうが、「公衆衛生若しくは社会保障に寄与する」とあるので、なんでもかんでもいいっていうわけではないということになっています。hは、自己健康管理アプリみたいなものですか。他の自然人の健康データに基づいて、自分の健康状態を評価して、「もうちょっと運動したらどう？」みたいなアプリケーションですね。

二次利用が禁止されるケース

こういうのはやってはダメというのが定められています。これが、なかなか面白いのですが、aは、GDPRのプロファイリングや自動的決定の条文と似ていますが、「自然人に不利益な決定を行うこと」というところです。これは高木先生が整理していますが、選別っていうのに、割と発想としては近いでしょう。このEHDSも、若干そこは制限をかけていて、法的効果が生じるか、自然人に重大な影響を与えないといけないとなっているので、単純に個別に効果を与えるというだけではなくて、1つ上乗せをしていますが、不利益な決定。これは、やはりヨーロッパは、データ保護指令の頃から自動的な決定というものに対し

二次利用の禁止される目的（EHDS 35）

- (a) 自然人の電子健康データに基づいて、その自然人に不利益な決定を行うこと。「決定」と認められるためには、法的効果を生じさせるか、または同様にその自然人に重大な影響を与えなければならない。
- (b) 自然人又は自然人の集団に関連して、保険契約の利益から彼らを除外すること、又は彼らの保険料及び負担金を変更することを決定すること。
- (c) 医療専門家、医療機関または自然人に対する広告またはマーケティング活動。
- (d) データ許可証に記載されていない第三者に対して、電子健康データへのアクセスを提供すること、またはその他の方法で利用可能にすること。
- (e) 違法薬物、アルコール飲料、タバコ製品、公序良俗に反するような方法で設計又は変更された商品又はサービスなど、個人及び社会全体に害を与える可能性のある商品又はサービスを開発すること。

て非常に警戒をしているというのがあります。その流れで、ここでもaに入っているわけです。bは、グループプライバシーみたいな感じで、自然人に関連しては当然ダメですが、自然人の集団に関連して保険契約との関係で、例えば、保険会社がいろいろなデータを取ってきて、この人たちはリスクが高そうだから保険金を上げようというのはダメだということです。集団的なプライバシーを暴くっていうのに近いと思いますし、個別にやるのは当然ダメですけど、集団に対しても、保険などでこういうのを使ったらダメとなっています。それから、このデータを取ってきて、お医者さんに営業かけるのもダメですよというのが、cです。それから、dは、転売です。データ許可書を申請した人以外に渡すつもりで取ってくるのというのはダメです。eは、ヨーロッパらしいですけど、「違法薬物、アルコール飲料、タバコ製品、公序良俗に反するような方法で設計又は変更された商品又はサービスなど、個人及び社会全体に害を与える可能性のある商品又はサービスを開発する」ことには使えないとあります。これを日本で書いたらね、アルコールとタバコは公序良俗に反するのかって怒る人がいると思いますが、私が書いたのではないので、怒らないでください。今のところ禁止されているのは、このaからeということになります。

データの提供形式

どんな形でデータが出てくるのかというのを皆さん興味あると思います。これは、データ・ミニマイゼーション（データ最小化）、パーパス・リミテーション（目的制限）というタイトルの第44条というのがありまして、原則、匿名化されたフォーマットです。繰り返しになりますけど、個人データじゃないということですから、ほぼ統計に近いような形でデータをくださいということです。どうしても仮名化じゃないといけない場合は、その理由を説明してくださいというのが44条3項になります。

日本法との関係

まずは位置付けとして、EHDSについては、EDPB-EDPSなどは、GDPRの権利との関係が不明確だとかいろいろ文句をつけてはいるのですけど、しかしながら、他の法令との関係コーナーというのが、説明書（EM）に割と詳細に載っていて、これはいいと思うんです。日本の医療データ保護構成って、データ保護法の中でも最悪にぐちゃぐちゃで、これを見ましょうか。

これは、最新の「個人情報保護法の基本」です。個人情報保護法が一応統一されたので、左から右まで個人情報法となりました。4段目のところで、左側に民間事業者があって、右側が行政機関等の義務です。令和3年改正で、病院、大学及び研究機関は民間法になりましたので、ごく一部を除いて医療機関は民間法の義務が適用され、そこに民間部門のガイドラインがあって、Q＆Aがあって、ここには載ってないですけど、研究の場合は倫理審査のための研究倫理指針という謎の文書があって―これがなぜ謎の文書なのかは後で説明しますが―、それを全部守ってやらないといけないということになっています。でも、個人情報保護法まわりのことしか書いていないのですよね。実際、次世代医療基盤法のことも書いてな

データ利用者への提供形式（データ最小化，目的制限　EHDS 44）

- 2.　健康データアクセス機関は、データ利用者によって提供された情報を考慮し て、データ利用者による処理の目的がそのようなデータによって達成できる場合には、**匿名化されたフォーマット**で電子健康データを提供しなければならない。
- 3.　データ利用者から提供された情報を考慮し、**匿名化されたデータではデータ利用者の処理目的を達成できない場合、健康データアクセス機関は電子健康データへのアクセスを仮名化された形式で提供しなければならない**。仮名化の取り消しに必要な情報は、健康データアクセス機関にのみ提供されるものとする。データ利用者は、偽名化された形式で提供された電子健康データを再識別してはならない。データ利用者が、健康データアクセス機関による偽名使用のための措置を尊重しない場合、適切な罰則の対象となる。

示唆①　位置付け

- EHDSは，GDPRその他の法令との位置付けを明らかにしようとしている（EDPB-EDPSからの意見はあるものの）

- 日本の医療データ保護法制は，
  - 個人情報保護法及び医療介護ガイダンスが存在し，医療介護ガイダンスは個人情報保護委員会と厚生労働省の連名であるにも拘わらず，厚生労働大臣は事業所管大臣にはなっていない
  - 医療関係法令に医療データ関係の規律がないわけでもない（医療法，医師法等）
  - 倫理指針の位置付けが転換されたはずだが（研究例外が精緻化されたため）未整理

いし、医療法とか医師法の守秘義務の話なども書いてない。医療介護ガイダンス[24]というのが医療分野のガイドラインなのですが、まず、平成27年改正の時に、「ガイドライン」から「ガイダンス」に名前が変わりました。しかし、なぜガイドラインからガイダンスになったのか、厚労省から説明はあるのですけど、よくわからないのです。説明を読んでも納得いかないっていうか、よくわからないです。ガイダンスなので、その解釈を示すものではなくて、いろいろな事例を示します、とか言っているのですが、どう見ても解釈が書いてあるので、何だこれと思っています。

もう1つ2つ不可思議なところがあります。総務省のガイドラインって、総務省は、結構な分野について、電気通信とか郵政とか、事業所管大臣になっているのですね[25]。電気通信分野や郵政分野のガイドラインで、総務省の単独名義だったのですが、2022年夏のガイドラインの改正で、個人情報保護委員会との連名になったのです。それで、不思議なところはなくなったわけです。

他方で、医療介護ガイダンスは、もともと個人情報保護委員会と厚労省の連名なのです。連名なのですが、厚生労働大臣は医療に関して事業所管大臣になっ

24）個人情報保護委員会・厚生労働省「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（平成29年4月14日（令和4年4月一部改正））。

25）個人情報保護委員会「権限の委任を受ける事業所管大臣、委任しようとする事務の範囲、委任の期間及び報告の期間」（令和４年４月１日時点），https://www.ppc.go.jp/files/pdf/kengeninin_R4.pdf

てないから、執行には一切携わらないのです。ここがよくわからないのですよ。もともと、特に医療法って都道府県に権限が降りているので、全然執行されてなかったのですよね、旧法の時ですよ。平成15年法の時に執行されてなかった。その反省で、個人情報はややこしいから、全部個人情報保護委員会に任せるってことになったのかと思うのですけど、ガイダンスは連名だけど、事業所管大臣になっていないっていうのが、よくわからないところではあります。

それから医療関係の法令に医療データ関係がないわけでもないのですが、この関係というのも問題です。個人情報保護法制は基本法人単位なのです。他方で、医療法は病院単位で文書管理など書いてあるので（医療法21条，同規則20条）、そこがズレていて、そこを直すという気が、あまりないですよね。

今回の改正で倫理指針の位置付けが大転換しているのです。なぜかと言うと、研究例外が見直されたのですよ。

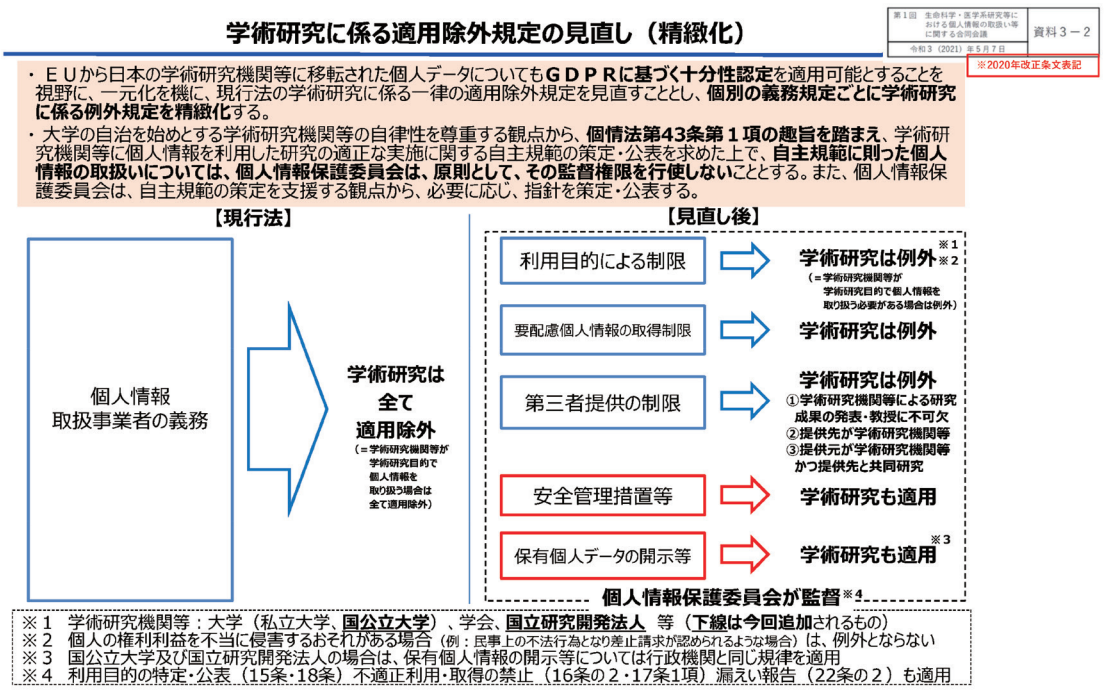
精緻化した学術研究の適用除外

これは、条文は2020年改正のもので、勝手には直していないのですが、2021年改正の資料です。元々学術研究は学術研究機関が個人情報を取扱う場合は全部適用除外だったのが、今回精緻化したのですね。精緻化したというのは、すごい大転換で、実は研究機関の研究だろうが、原則法律は適用されるのですよ。この3項目、要配慮個人情報の取得と利用目的制限と第三者提供だけ、除外にしたのですね。ということは、原則研究であっても、個人情報保護委員会の権限は及ぶのですよ。倫理指針って、今まで法令の監督が及ばないから倫理指針でやっていると、何となく皆さん思っていたと思うのですが、2021年改正以降は法令も及ぶのだけど倫理指針もかかりますみたいになってしまったのですよね。位置付けがよくわからないのですよ。

医療介護ガイダンスと研究倫理指針の関係性の矛盾

『法律のひろば』にガイドラインの解説を書きました[26]。倫理指針とはそもそも何なのかということを探っていくと、厚労省が言うには、厚労科研の補助金の取り扱い規定に、この倫理指針守って研究してねって書いてあるから、その範囲では規範性があると言われているんですね。一方、個人情報保護法との関係ではどうかっていうと、これ、私がバカなのかなと思うのですが、何を言っているのかわからない。「（行政指導指針）であり、個人情報保護法（個情法）の規定が上位規制となります。そのため、個人情報関連の用語の定義は、個情法を踏襲することとなります」となっているのですね。

この文章のすべてがわからないですけど、行政指導指針っていうのはわかるのですが、個人情報保護



26）板倉陽一郎「医療関連分野ガイダンス等及び研究倫理指針の改正と実務への影響」法律のひろば75巻5号（2022年）45頁。

医療介護ガイダンスと研究倫理指針

図1　医療介護ガイダンスと研究倫理指針の適用関係（簡略版）

	学術研究目的以外の目的（診療目的等）	学術研究目的だが例外規定は適用されない場合	学術研究目的の例外規定が適用される場合
医療介護ガイダンス	適用	適用	内容に留意
研究倫理指針	適用されない	適用	適用

なお、研究倫理指針は、厚生労働科学研究費補助金等取扱規程（平成10年4月9日厚生省告示第130号）12条で「研究者等は、研究事業及び推進事業の遂行に当たり、遺伝子治療等臨床研究に関する指針（平成31年厚生労働省告示第48号）、人を対象とする生命科学・医学系研究に関する倫理指針（令和3年文部科学省・厚生労働省・経済産業省告示第1号）等の研究に関係する指針等を遵守しなければならないこと。」としていわゆる厚労科研費の交付の要件を構成しており、規範性を有するが、個人情報保護法との関係では、「指針は法に甚づかない命令等（行政指導指針）であり、個人情報保護法（個情法）の規定が上位規制となります。そのため、個人情報関連の用語の定義は、個情法を踏襲することとなります。」とされており（注3）、行政手続法2条8号二の行政指導指針であって、個人情報保護法の処分等の基準（行政手続法2条8号ハの処分基準）ではないという整理が明らかにされている。

そうすると、「個人情報保護法の規定が上位規制」という意味が判然としないことになるが、法令と命令等の一般的な上下関係を踏まえて「上位規制」としているということになろうか。研究倫理指針は個人情報保護委員会名義の文書でもなく、後述するように、研究目的例外の精緻化に伴い、個人情報保護法と同時に適用される場面は今後増加するものの、個人情報保護法違反の基準ではなく、あくまで、各倫理指針の名義人である省庁において、行政指導の基準となるに過ぎない、ということになると思われるが、このような整理は個人情報保護委員会及び倫理指針の名義人たる省庁において、明確になされるべきであろう（板倉・法律のひろば2022年5月号45頁以下）。

法の処分の基準ではないんですよね。だから、個人情報保護法を守ると書いてあっても、倫理指針違反は個人情報保護法違反ではないわけです。個人情報保護法の規定が上位規制というのもよくわからないのですが、法律と、行政指導のための法に基づかない命令等だとすると、法律の方が上位だからこう言っているのかなというぐらいの話なのです。でも、倫理指針って、ほとんど個人情報の話じゃないですか。こんなぐちゃぐちゃなまま、放っておくのはダメなんじゃないかなと思っています。

医療介護ガイダンスと研究倫理指針の適用関係を簡略に整理しました。学術研究目的の例外規定が適用されない部分では、医療介護ガイダンスと研究倫理指針が両方適用される。学術研究以外の目的、診療などの一時利用の場合は、医療介護ガイダンスだけが適用されます。他方で、例外規定が適用される場合も、医療介護ガイダンスには「内容に留意」と書いてあって、では結局、両方守るの？という話になるんですよ。めちゃくちゃなので､何とかしないと、わかんないですよね。何とかしないといけないのではと思っています。

監督機関

EHDSでは健康データアクセス機関というのを、新しく作るか、誰かに割り当てることになっているのですが、ここは何をやるかっていうと、制度の監督と，情報提供ネットワークシステム的な機関ですよね。情報提供ネットワークシステムというのは、マイナンバーをやり取りするためのシステムですけど、それを手動でやっているみたいな感じで、ここはデータを持ったりしないです。次世代医療基盤法の認定事業者は、大きいデータベースを作りますよね。この健康データアクセス機関は、ここに出してくれとか言うだけで、処理は手伝うって書いてあるので加工とかは手伝ってあげるのかもしれないですけどデータは持たないのですよね。処理の範囲でと書いてある。EDPB-EDPSの意見を見ても、それが前提のようなの

示唆②　監督機関

- EHDSでは，「健康データアクセス機関」が，監督機関　兼　情報提供ネットワークシステム的な機関として求められる（公的機関）。
- 自然人（データ主体）の権利についてはデータ保護機関が担当。

- 次世代医療基盤法では認定事業者と主務大臣
- 個人情報保護法では個人情報保護委員会（厚生労働省は事業所管大臣になっていない）

で、そういう機関なのですよね。自然人の権利、データ保護的なところは、データ保護機関が見るよとなっています。日本は次世代医療基盤法だと認定事業者なんです。これは事業者だから公的な権限もないし、医療機関等に強制的に出してくれとは言えないわけですね。吉原先生(吉原博幸.一般社団法人ライフデータイニシアティブ（LDI）代表理事）が、まさに個別にお願いしてデータ出してもらっているみたいな。吉原先生がいろいろな会議で、「政府がきちんと集めるべきである」とおっしゃっていますけど、そこはEHDSでは公的な権限で出せという形になっているわけですね。

次世代医療基盤法は、認定事業者を主務大臣4つが監督するっていうことになっていて、個人情報の関係では個人情報委員会がいて、厚労省はこっちでは事業所管大臣になってないという形なので、もう少しシンプルにしてもいいのかなとは思います。

本人の権利

本人の権利です。一次利用は権利が強化されていて、ポータビリティが非常に強く認められるようになっている。二次利用のデータ利用者に対しては、仮名化か匿名化されるので、権利行使は限定的だという風に見られます。日本法はまず、一次利用がちゃんとできていないのです。一次利用がちゃんと使えるようにどこにも定められてないので、一次利用のために、例えば医師の皆さんが、このケースは判断に迷うから、友達の外科の方に聞こうかって言って、法人を越えると第三者提供になっちゃうから、なぜか院内掲示で黙示の同意という、昔からガイダンスにある謎のやり方でやっているのです。これはやはり変なので、法律に書いたらと思うのですよね。

次世代医療基盤法における「丁寧なオプトアウト」は、認定機関が病院等からもらってくる時の話ですけど、これが丁寧すぎてワークしないということが、実際、次世代医療基盤法の見直しでもしっかり言われています。何らか緩和する方向ではあるようですが、匿名加工情報や仮名加工情報については、別のルールになっていますし、仮名加工情報の共同利用が、20年改正でできるようにはなっているのですけど、倫理指針の方では、前から作っていた匿名加工情報や仮名加工情報でない限り倫理審査は逃れられないというさらにややこしいルールになっています。EHDSを見ながら整理を試みてもいいかなという気はします。

アクセス範囲

最後にアクセス範囲です。一次利用の医療従事者の範囲が、やはり曖昧だとなっていて、これから個別に議論されていくのかなと思います。二次利用はアプリケーションを出したデータ利用者なので、わかりやすいですね。日本では個人情報保護法は法人単位で、医療法は病院単位です。患者さんからすると、割と医師個人だったりするので、混乱が見られるので、整理したほうがいいのではと思います。次世代医療基盤法は誰でも、お金を払えば一応取れるようにはなっていますが、匿名加工医療情報だから、生データが全然残ってない、仮名ですらないものしか提供されないということになっています。ここも次世代医療基盤法の見直しで、生データの段階で使えないかといった検討はされています。EHDSでアプリケーション出して使うと最大8ヵ月かかりますけど、

示唆③　本人の権利

- EHDSでは,
  - 一次利用は権利強化（ただしGDPRの権利との関係整理必要（EDPB-EDPS）
  - 二次利用は仮名化・匿名化されるので権利行使は限定的，処理根拠は同意ではない
- 日本法では,
  - 一次利用における院内掲示（従前からのガイダンスの記載）
  - 次世代医療基盤法における「丁寧なオプトアウト」
  - 匿名加工情報，仮名加工情報（共同利用を含む）
    - さらに倫理指針の定め

示唆④　アクセス範囲

- EHDSでは，
  - 一次利用は「医療従事者」（ただしEDPB-EDPSにより曖昧さが指摘）
  - 二次利用は，データ利用者

- 日本法では，
  - 一次利用は法人単位のはずだが混乱
  - 次世代医療基盤法では対象は問わない（ただし匿名加工医療情報のみ）

そういう仕組み参考にして、検討してみてもいいのではというところが示唆かなという風に思います。

全体的に知識が非常にいるものだったので、十分伝えきれなかったかもしれませんが、私からは以上です。

（本稿は、第6回情報法制シンポジウム「個人情報保護法と医療データ特別法～仮名加工医療データを中心に」（2022年7月22日、オンライン開催）での報告を元に作成しました。）

情報法制研究所理事
ひかり総合法律事務所 パートナー 弁護士
板倉 陽一郎（いたくら・よういちろう）

2002年慶應義塾大学総合政策学部卒、2004年京都大学大学院情報学研究科社会情報学専攻修士課程修了、2007年慶應義塾大学法務研究科（法科大学院）修了。2008年弁護士（ひかり総合法律事務所）。2016年4月よりパートナー弁護士。2017年4月より理化学研究所AIP客員主管研究員、2018年5月より国立情報学研究所客員教授、2020年5月より大阪大学ELSIセンター招へい教授。JILIS参与を経て2021年4月より理事。