Alliance for IoT and Edge Computing Innovation

White Paper
IoT/Edge Computing and Health Data and Data Spaces

Release 1.0

AIOTI WG Health

March 2024

Executive Summary

The objective of this paper is to provide an overview of EU health data spaces in terms of regulation and existing practices, as well as to provide examples and make some recommendations, in particular from the point of view of the computing continuum (cloud-Edge-IoT-AI).

The paper list current state of play of health data spaces in the EU, but also in the US and China. Building on that, it provides insights in ongoing activities based on which recommendations are proposed.

Table of Content

1. Introduction

The EU has always had a role in public health, but COVID-19 has created substantial additional political momentum for an EU Health Union. The need to be better prepared for future health crises, the benefits of information sharing and research at EU level during pandemics, and the success of cooperation in developing digital tools like the EU digital COVID certificate have paved the way for more integration at EU level in the field of health.

The European Health Data Space proposal is one of the initiatives that the Commission has put forward as part of the Health Union package adopted in November 2020. It is the outcome of the convergence of two major policy streams of the last decade: the data economy and eHealth. It can be read as a lex specialis and one of the first sectoral applications of the Data Governance Act (2022) that sets a data governance framework for data intermediaries that facilitate data exchanges and sharing between several parties.

There are several objectives the EHDS aims at pursuing, but the main one are the following: i) Empower individuals through better digital access to their personal health data; support free movement by ensuring that health data follow people; ii) Unleash the data economy by fostering a genuine single market for digital health services and products; and iii) Set up strict rules for the use of individual's non-identifiable health data for research, innovation, policy-making and regulatory activities. As such, the EHDS aims to improve and support healthcare delivery within Europe by allowing public health data to be accessible throughout Europe. The EHDS also aims to promote better access and exchange of different types of health data for research and policy purposes. The aim is to have the EHDS up and running in 2025.

The EHDS is expected to bring great benefit, but it also brings challenges related to technology, governance and privacy as such EU approaches to health data have struggled due to several key limitations:

1. Uncertain demand on the part of patients for cross-border delivery of eHealth services;

2. Impediments posed by the simultaneous need to maintain the privacy and confidentiality of sensitive health data;

3. Insufficient incentives for Member States and institutions to participate in data-pooling arrangements;

4. Lack of a strong mandate to proceed at EU level (subsidiarity); and

5. The risk of problematic interactions with other EU and national legal instruments.

These limitations manifest differently for primary use versus secondary use, and they have different implications for the degree to which the proposed EHDS Regulation can be expected to be effective, efficient, coherent, and adding European value.

This paper aims at shedding the light on some key elements of the EHDS Regulation, its relationship and comparison with international big players such as the USA and China as well as on the vision, expectations and use cases and best practices provided by the AIOTI WG Health's members.

2. The European Health Data Space: the reference EU regulation

Within the European Health Data Space, all processing of health data must have a lawful basis, as dictated by the GDPR. Explicit consent from data subjects is fundamental, especially considering the sensitive nature of health data. Moreover, individuals can exercise the right to access, rectify, erase, and restrict the processing of their health data.

In addition, the EU regulation defined strategies for implementing the data governance framework, by establishing a European Committee for Data Innovation. The Committee aims to coordinate national practices and policies related to the regulation and support cross-sectoral data usage, adhering to the principles of the European Interoperability Framework and utilizing standards and specifications (such as the Building Blocks of the Connecting Europe Facility and Core Vocabularies).

With the initiative "A European Strategy for Data", proposed by the European Commission, the main goal is to address various aspects of data management, utilization, and governance within the European Union. The strategy aims to unleash the full potential of data-driven innovation, ensure the EU's global competitiveness, and promote data sovereignty, by upholding privacy and ethical considerations.

At the end, the EU regulation sheds light on the security of network and information systems across the European Union, with the Directive (EU) 2016/1148, also known as the NIS Directive (Network and Information Security Directive). It aims to improve the EU's cybersecurity resilience and response capabilities, promoting a safer and more secure digital environment for businesses and citizens.

The European Commission officially launched the EHDS effort in May 2022[1], outlining the main areas of intervention, as follows:

- Develop regulatory, process and technical framework for enabling patients across the Union to share health data with medical professionals based on health data interoperability and providing patients with full control over access and usage to their data – the so called MyHealth@EU[2] initiative for cross-border medical services and information exchange.

- Enact a Common European Format for laboratory results, e-Prescriptions, image reports, etc, to which all Member states should comply;

- Mandate the Member states to set up digital health authorities who shall facilitate safeguarding citizen rights and dispute resolutions.

According to the EC's estimates[3], researchers and industries are also expected to benefit from the regulation and the EHDS setup in terms of secondary usage of health data to an estimated 5.4 billion euro saved over shared data for research purposes and 20-30% growth on the digital health market across the Union.

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711
[2] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en
[3] https://ec.europa.eu/commission/presscorner/api/files/attachment/872447/Factsheet%20-%20EHDS.pdf.pdf

The Commission further published a **proposal for the EHDS regulation** based on impact assessments, a public consultation held in 2021 and a couple of studies directed at validating the impact assessment, assessing national level regulations and assessing benefits across the healthcare sector in terms of digital services and other uses of health data.

The proposal specifies in its scope four categories of interested parties: (1) manufacturers and suppliers of EHR systems ("electronic health record" systems); (2) processors and controllers of medical data in the EU; (3) processors and controllers of such data in third countries; (4) data users. It establishes definitions for a lot of terminology related to the field of digital health, including EHR, wellness applications, etc; while also specifying the scope of personal and non-personal health record data; primary and secondary usage of health data (i.e. for healthcare purposes or otherwise) and others. The concepts of MyHealth@EU (services platform) and HealthData@EU (data infrastructure) are introduced.

The proposed regulation furthermore narrows down the provisions of the Data Governance Act and hence the operational and infrastructural requirements in the health data domain, in order to specify the framework for the EHDS.

The EHDS Regulation Proposal is thus published in the context of other relevant legislation.

First and foremost, this is the **Data Governance Act**, in force since September 2023, which postulates general requirements for data sharing and data intermediation, data altruism, data sovereignty, dispute resolution and relevant certification and dispute resolution authorities. It facilitates re-use of public data (that is not open data under the ODD 1024/2019 provisions) among different economic actors and sets rules for trust.

The **Medical Devices Regulation** and the proposed **AI Act** both have implications on devices generating medical data and hence possible data suppliers to EHR systems and other storages of health data. Those devices and the data they generate are also subject of the Data Act proposal that introduces rules for allowing natural persons access and shareability to their IoT generated data (in particular medical data) and moving it between different service providers. The Data Act also mandates "force majeure" access to such data for cases of public emergency. Some of the provisions of the Data Act remain controversial for the industry and there have been iterations on the subject.

The **NIS directive**, as well as **NIS-2 directive**, cited above, pose requirements to the security of data storage and data sharing.

The **Regulation (EU) 2018/1725, also known as GDPR**, posits the fundamental requirements for access, sharing and storage of personal data, including health data. As mentioned above, usage of raw health data with personal details included for research purposes, remains controversial in terms of consent and audit logging.

The **European Digital Identity Regulation** is key element of the health cross-border services at MyHealth@EU, as well as the EHDS and the HealthData@EU infrastructure. It would require relevant access to medical data, as well as referential integrity to conform to the EDI infrastructure. Finally, the EHDS Regulation Proposal builds upon the provisions of the CBHC directive which posits some (voluntary) requirements on cross-border exchange of health data.

3. Health Data Management: state of play in the EU, USA and China

3.1 EU

Member States Rules on health data

The Assessment of the EU Member States' rules on health data in the light of GDPR can be found here for each EU Member State.

Electronic cross-border health services

The following 2 electronic cross-border health services are currently being introduced in all EU countries:

- **ePrescription and eDispensation** (eHealth Network guidelines on ePrescription, Release notes) allows EU citizens to obtain their medication in a pharmacy located in another EU country, thanks to the online transfer of their electronic prescription from their country of residence where they are affiliated, to their country of travel.

- **Patient Summaries** (eHealth Network guidelines on Patient Summary, Release notes) provide information on important health related aspects such as allergies, current medication, previous illness, surgeries, etc. It is part of a larger collection of health data called an electronic Health Record. The digital Patient Summary is meant to provide doctors with essential information in their own language concerning the patient, when the patient comes from another EU country and there may be a linguistic barrier. In the long term, **medical images, lab results and hospital discharge reports** will also be available across the EU, with the full health record to follow later on. The exchange of ePrescriptions and Patient Summaries is open to all the EU countries.

Many EU/EEA countries are implementing these services. More information can be found here.

3.2 China

According to available data, online medical users increased from 214.8 million in 2020 to 233.3 million in 2021, generating an additional $44.7 in revenue per user. Statista is also very positive, predicting that China's digital health industry will gross $46 billion in 2022 and $84.7 billion in 2027, indicating a growth rate of 12.98% year over year.

While this growth is exciting and induces the temptation to jump into China's digital medical space. Healthcare companies will need to get acquainted with personal data protection laws to have a smooth business operation. Below, we will reveal all necessary China medical device regulations businesses must comply with while sharing data outside the country.

Who should be aware of medical data regulations in China

According to Article 28 of China PIPL, personal health information is considered sensitive data and must be protected from unlawful collection, transfers, and processing. Not complying with the rules governing PHI data residency regulation could mean opening the portal that leaves your business at the mercy of fines and other penalties.

Here are businesses that need to be aware of medical data regulations in China.

- Telemedicine/Virtual care providers
- Mobile medical Apps
- Providers of medical robots
- Manufacturers/providers of medical wearables include hearing aids, wearable ECG monitors, biosensors, smart health watches, wearable blood pressure monitors, etc.
- Software as a medical device (SaMD) providers
- Clinical decision support software providers
- Providers Of AL/ML-powered digital medical solutions
- Digital therapeutics
- Medical 3D printings/bioprinting
- Internet of things and connected devices

Key Chinese data protection laws for healthcare industry

With a population of over 1.45 billion people and a digital health market projected to hit $46 billion in 2022 and $84.7 billion by 2022, China is one market that can cause colossal upside spikes in your company's revenue if successfully tapped into. However, in tapping into this huge market, your business or products can suffer significant setbacks if they fail to comply with any of China's medical device regulations or data privacy laws.

DIDI, one of China's largest ride-hailing companies, was fined $1.2 billion, while top-tier executives were fined $148,000 in personal liability. If your company hopes to have hassle-free operations, below is a list of China's medical regulations that your business or company's products must comply with:

- Laws of the PRC on Protection of consumer rights and interest.
- Data security law of PRC.
- Personal information protection law
- Cybersecurity laws of the PRC
- Civil Code of PRC
- Guiding opinions on the internet plus medical services
- Guiding opinions of the national healthcare security administration on improving the internet plus medical service.
- Administrative measures for the internet-based diagnosis.
- Administrative measures for internet hospitals.
- Administrative regulations for telemedicine service.
- Laws of the PRC on the promotion of Basic Medical and Healthcare.

- Administrative regulations on applications of electronic medical records.
- Administrative measures on standards security and services of national Healthcare big data.
- Guiding Principles for AI medical software products.
- Information security technology- personal information security specification (GB/T 35273-2020).
- Measures for Cybersecurity Law.
- Administrative regulation on Human Genetic Resources of PRC.
- Measures for the administration of scientific data.
- Measures for the administration of population health information.
- Certification Specification for Cross-Border Processing of Personal Information.
- The standard contract for the cross-border transfer of personal information.

Chinese data cross-border rules

The PIPL in Article 28 defines health data as sensitive data and, as such, mandates companies and businesses that collect, process, store, and transmit these data in their normal course of business to set up security management systems to ensure the secured management of data during its lifecycle. The PIPL obligates these companies to store personal data information of Chinese citizens within China. However, business operations often warrant that citizens' data be transferred outside the originating country, and in such scenarios, Chapter 3 of PIPL comes into force.

The PIPL in Chapter 3 provides the rules that business owners that utilize personal information must follow to avoid breaches when sharing China health data across borders. These rules are provided below:

Article 38: General requirement

Medical company owners must satisfy the following requirements before sharing personal information with any party outside China.

(i). Must satisfy the security assessment requirements organized by the State cyberspace administration in line with Article 40. In essence, your company must be subjected to a security assessment by specialized government institutions before sharing the medical data of users or customers with an overseas partner in the following circumstances per Article 40:

- If your company processes the personal data of more than 1 million users or if your company is certified as a critical information infrastructure operator.
- If your company has processed over 1 million personal data since January of the previous year.
- Or have processed sensitive information (medical data of over 10,000 persons.

(ii). The company must have been certified by a specialized body (Certification Specification for Cross-Border Processing of Personal Information) to protect the personal information of users or consumers in line with the provisions of the state cyberspace administration.

(iii). Companies must have a contract with the overseas recipient that specifies the rights and obligations of both parties in line with the standard contract formulated by the state cyberspace administration.

(iv). Companies (data processors) must have met other conditions stipulated by other relevant laws and regulations of the People's Republic of China.

Article 39: Guidelines for cross-border data sharing

The PIPL in Article 39 mandates medical health service providers who wish to disclose personal information of their users to a party outside of China to do the following:

- Firstly, they must inform their users or consumers of the names of the overseas recipient of their health data.
- Provides the users with the contact information of the overseas recipient.
- Furnish the users or consumers with information regarding the purpose of collection, method of processing, and the type of health data to be transmitted.
- In this regard, medical companies (data controllers) are also mandated to inform their users or customers of the way and procedure to exercise the rights prescribed herein against the overseas recipient.
- Also, medical companies are mandated to obtain the separate consent of their users before sharing personal data with a third party across China's borders.

Article 42: Guidelines for Special Purpose

As a digital health service provider, your company can work with the permission of Competent authorities of the People's republic of China and, concerning relevant laws and international treaties, honour requests from foreign judicial or law enforcement bodies to transfer personal information of Chinese citizens stored in China. But granting this request is subject to express approval from a competent authority of the People's Republic of China.

The penalty for breach of data privacy laws

Violating the provisions of the Chinese personal data protection laws may expose your business to crippling penalties. Your company may be fined up to 5% of its previous year's turnover, or its operating license may be revoked. Also, your company's executives may face personal liabilities.

Now you know the numerous laws guiding sharing data in China and overseas, the question that readily comes to mind is how your institution can run successful business operations in China while remaining compliant with China's medical device regulations. Let's find out in the next section.

China recently finalized the Measures for Security Assessment for Cross-Border Data Transfers, unveiling the last piece of the puzzle for cross-border data transfer. This LawFlash highlights the key requirements in the data protection regime and the implications for business operators in the highly regulated, data-intensive field of healthcare.

Data privacy has been a hot topic in China since the Chinese government actively released data privacy laws and regulations in recent years. Three milestone laws in the privacy regime have been published and come into effect, including the Cybersecurity Law (CSL) (2017), the Data Security Law (DSL) (2021) and the Personal Information Protection Law (PIPL) (2021).

Under the umbrella of these fundamental laws, the Chinese government has recently been focusing on rolling out rules and regulations for implementing its cybersecurity, data security, and personal information protection laws.

For example, on June 24, 2022, China published the final version of the Certification Specification for Cross-Border Processing of Personal Information, which provides guidance for companies to have their cross-border data transfer certified as one of the legal routes for business operators to transfer the personal information outside China. On June 30, China further published the draft version of the standard contract for the cross-border transfer of personal information, considered China's standard contractual clauses (similar to SCC under the EU General Data Protection Regulation), which also provides additional obligations for filing of the standard contract with the government authorities, before the cross-border data transfer can take place.

Finally, on July 7, the Measures for Security Assessment for Cross-Border Data Transfers were finalized, which clarify under what circumstances a company must undergo a security assessment approved by the competent Chinese government authority before exporting data out of China.

Highlights of data protection laws

The data protection laws require companies as data handlers (a concept under the PIPL, similar to data controllers under the General Data Protection Regulation) to obtain informed and separate consents from the data subjects for the collection, processing, and cross-border transfer of personal information (limited exceptions apply).

The law has an extra-territorial effect, which applies both to personal information processing activities within China and those that take place outside China if their purpose is to provide products or services to individuals located in China, or to analyse or assess the behaviours of individuals located in China. Overseas companies caught by the exterritorial jurisdiction of the PIPL should establish a dedicated entity or appoint a representative in China to handle matters in relation to the protection of personal information they collect, and to file the information of the entity or the representative with competent government authorities. Foreign organizations or individuals may be put on a "blacklist" that would restrict or prohibit them from receiving personal information from China if they infringe the personal information rights and interests of Chinese citizens or harm the national security or public interest of China.

Additionally, the law grants statutory rights to data subjects, such as the right to withdraw and modify consents, the right to data portability, and the right to refuse automated decision-making. The law also imposes a number of new administrative requirements on the data handlers, including, but not limited to, designating a data protection officer, signing data processing agreements with data processors, preparing data breach notices, conducting a personal information protection impact assessment (PIPIA), or in some cases obtaining regulatory approval for certain data processing transfer activities.

Employers also qualify as data handlers, so every company will need to ensure that they understand the new requirements that cover the collection and processing of their employees' personal information, in addition to other types of personal information, as part of their routine employee management functions.

A company must undergo a security assessment approved by the competent government authority before exporting data under any of the following scenarios:

- transferring "important data" out of China;
- the company is certified as a critical information infrastructure operator (CIIO), or transferring personal information out of China if it processes personal information of over one million individuals;
- having transferred personal information out of China reaching the following thresholds since January 1 of the previous year:
    - other personal information of more than 100,000 individuals, or
    - the sensitive personal information of more than 10,000 individuals; or
- under other circumstances specified by the government authority.

Companies in violation of the data protection laws may be subject to severe penalties, including a fine of up to 5% of the last year's turnover of the company, revocation of the company's license to do business in China, and personal liabilities for company executives.

Implications for the healthcare industry

Healthcare data (such as medical, genetic, and biometric data) is sensitive personal information, which is subject to a higher level of protection. Processing sensitive personal information requires the data handlers to ensure:

- data subjects have given their explicit and separate consent;
- data subjects have been well informed as to the purposes, scope, necessity and methods of the processing, retention period, and impact on an individual's rights and interests of the processing, among other things;
- measures (such as encryption, anonymization, etc.) are implemented;
- an internal risk assessment (i.e., the personal information protection impact assessment) is conducted; and
- before transferring the personal information outside China, depending on the nature of the exporter and the nature and volume of the data to be transferred, one of the following mechanisms should be completed:
    - undergo a security assessment approved by the government authority (for the CIIOs and entities that transfer important data and a large volume of personal information as analysed above);
    - obtain certification from "qualified institutions" in accordance with the rules of the government authority (e.g., the Certification Specification for Cross-Border Processing of Personal Information that is newly published);
    - enter into a data transfer agreement with the overseas recipient based on a "standard contract" published by the government authority; or
    - other transfer mechanisms permitted under laws and regulations.

A patient's access to their personal information

When a patient requests access to their medical records, a medical institution shall provide the appropriate service after checking the patient's valid identification.

When a patient accesses their medical records through the online system, the medical institution is also required to take steps to verify the true identity of the patient. For example, a patient is required to log into the system via a real-name mobile phone number and a verification code. The Information Security Technology - Guide for Health Data Security (GB/T 39725-2020) recommends that medial institutions display user instructions via system pages when patients perform the appropriate actions, such as informing patients that they are responsible for protecting the security of their medical records after downloading. At the same time, medical institutions shall consider using verification or encryption technology to ensure the confidentiality and integrity of personal healthcare data during transmission.

A third party's access to a patient's medical records

According to the 2013 Regulations on the Management of Medical Records in Medical Institutions (the 2013 Regulations), except for medical personnel providing medical services to patients, as well as departments or personnel in charge of case management and medical management authorized by the National Health and Family Planning Commission, the administration of traditional Chinese medicine, or medical institutions, no other institution or individual shall have unauthorized access to patients' medical records. If other medical institutions and medical personnel need to access or borrow medical records for scientific research or teaching purposes, they shall apply to the medical institution where the patient is treated, and only after the institution has agreed and gone through the appropriate procedures can they access or borrow the records. Medical records shall be returned immediately after access, and borrowed medical records shall be returned within three working days. Accessed medical records shall not be taken away from the institution. The Guide for Health Data Security provides a reference for medical institutions to establish systems for managing access to patient records by medical personnel in terms of data classification, role definition, data labelling, authority allocation, identity identification, and data access.

In addition, a patient's agent, a legal heir, or an agent of the deceased patient, insurance agencies, and relevant law enforcement agencies can apply for access to the patient's medical records. The 2013 Regulations require medical institutions to designate a department or full-time (part-time) staff to receive applications for copying or accessing medical records. When accepting an application, medical institutions shall require the applicant to provide relevant supporting materials and review the application materials.

If a medical institution provides medical records to others in violation of the law, it may face administrative penalties. For example, in December 2022, the Health Commission imposed an administrative penalty and fine of RMB 20,000 (approx. $2,810) on a hospital for disclosing a patient's privacy by providing a patient's medical records to a third party other than the patient themself in violation of the provisions of the 2013 Regulations.

Online processing context

As the digital transformation of the health industry progresses, the People's Republic of China (PRC) is gradually entering a state of development where hospital-led online hospitals are in the majority.

In order to provide online diagnosis and treatment services to patients, medical institutions will process personal information, including patients' identity information and medical history data. In order to protect the security of personal information in the process of online diagnosis and treatment, the PRC has put forward personal information protection requirements for online hospitals through legal documents, such as the Measures for the Administration of Online Diagnosis and Treatment (trial implementation), the Measures for the Administration of Online Hospitals (trial implementation), the Norms for the Administration of Telemedicine Services (trial implementation), and the Norms for the Application of Electronic Medical Records (trial implementation), including that:

- an online hospital shall strictly implement the relevant laws and regulations on cybersecurity and confidentiality of medical data, properly store patient information, and not illegally trade or disclose patient information;

- an online hospital shall establish a data access control information system to ensure system stability and service traceability throughout the online diagnosis and treatment, and realize data exchange and sharing with the Hospital Information System (HIS), Picture Archiving and Communications System (PACS), Radiology Information and System (RIS), and Laboratory Information System (LIS) of a brick-and-mortar medical institution;

- an online hospital shall establish and improve relevant management systems and service processes to ensure that the entire process of online diagnosis and treatment is traceable, and open data interfaces to the regulatory authorities;

- an online hospital shall have at least two sets of servers for its operation and divide a database server from an application system server, whereby the room where the servers are housed shall have dual power supply or emergency power generation facilities;

- servers used by an online hospital to store medical data shall not be stored outside the territory of the PRC;

- the information system of an online hospital shall implement the third level of cybersecurity-graded protection;

- an online hospital shall designate personnel responsible for the management of medical quality, medical safety, and electronic medical records, provide technical services, such as maintenance of the online hospital information system, and ensure the stable operation of the online hospital system; and

- in the event of leakage of patient information and medical data, an online hospital shall promptly report to the competent health administration department and immediately take effective response measures.

Pharmaceutical clinical trial context

In a pharmaceutical clinical trial context, sponsors, and investigators (i.e., personal information processors) are also required to comply with legal documents, such as the Personal Information Protection Law (PIPL) and the Code of Practice for the Quality Management of Pharmaceutical Clinical Trials, which require the protection of the subjects' personal information. In addition, in March 2023, the Guangdong Pharmaceutical Association released the Pharmaceutical Clinical Trial, Information Security, Guangdong Consensus, which provides detailed requirements on personal information protection in pharmaceutical clinical trials, which can be used as an important reference for personal information processors.

Inform and obtain consent in advance

In a pharmaceutical clinical trial context, personal information processors will process the subjects' personal information by collecting, using, and storing it, among others, and shall therefore inform the subjects and obtain the subject's consent or other legal bases in advance. Personal information processors could add content related to the processing of personal information to original informed consent forms and allow the subjects to choose whether to consent after reading.

In this context, personal information processors may process sensitive personal information or provide personal information to other personal information processors. In this case, personal information processors shall obtain the separate consent of the subjects. If personal information processors obtain the subjects' general consent to all personal information processing activities only through one informed consent form, that consent may be found to be invalid. To reduce this risk, personal information processors could consider the following approaches:

- issuing a separate informed consent form for a specific context, such as sensitive personal information processing or external provision of personal information; and

- adding checkboxes to the original informed consent form for sensitive personal information processing or provision of personal information; if a subject agrees to the specific personal information processing, they could manually check the checkbox to indicate separate consent.

In addition, personal information processors shall establish and disclose response mechanisms for the subjects' personal information rights and interests and promptly process the subjects' requests for exercising their rights. Where a subject's request is rejected, the personal information processor shall give reasons as to why.

Personal information categorization and classification management

Personal information processors shall categorize and classify subjects according to their personal identification information, health information, contact information, and other categorization dimensions, as well as data sensitivity levels, and be equipped with appropriate security protection measures. If an industry authority or other regulatory authorities stipulate that certain categories of personal information are important data, personal information processors shall give it the highest level of security protection.

Internal management system and authority setting

Personal information processors shall establish internal management systems and operational procedures of personal information protection to limit the processing of the subjects' personal information within the scope of the subject's consent. Further, personal information processors shall clarify the processing authority of test participants to avoid unauthorized personal information processing activities. For instance, in trials where subjects are assigned codes in lieu of names, only the investigator and research team members could access the subjects' information corresponding to the codes to the extent necessary in accordance with their work authorization. Subject to the principles of confidentiality and relevant regulations and to the extent necessary for their work, supervisors, inspectors, ethics committees, and drug regulatory authority inspectors could access the original medical records of relevant subjects to verify the process and data of the clinical trial. Before any person is allowed to access the subjects' personal information, the person in charge shall verify their valid identity to ensure the confidentiality of the trial information.

Marketing context

Medical institutions and pharmaceutical companies may also be involved in using personal information for marketing purposes in order to raise awareness of medical institutions and pharmaceutical companies or to sell medicines. In these contexts, medical institutions and pharmaceutical companies shall still inform the subjects and obtain the appropriate legal bases of the processing of personal information, otherwise, they may face penalties.

In addition, medical institutions and pharmaceutical companies shall safeguard the subjects' rights of refusal. When a subject refuses to have their personal information processed by medical institutions and pharmaceutical companies in order to send them marketing information, the medical institutions and pharmaceutical companies shall promptly cease to continue sending such information. If medical institutions and pharmaceutical companies use automated decision-making to push information and commercial marketing to subjects, they shall also provide the option of not targeting the subjects' personal characteristics or provide them with convenient ways to refuse.

Provision of personal information outside the territory of the PRC

Data which shall in principle be stored in the territory of the PRC.

The PRC currently has requirements for specific categories of personal information that are, in principle, not allowed to be provided outside the territory of the PRC, as reflected in the health and pharmaceutical industries as follows:

Category	Requirement	Related legal document
Population health information	Entities in charge shall not store population health information in any server outside the PRC and shall not host or lease any server outside the PRC.	Measures for the Administration of Population Health Information (trial implementation)
Medical data	The server storing medical data must not be stored outside the PRC.	Basic Standards for Internet Hospitals (trial implementation)
Healthcare and medical big data	Healthcare and medical big data shall be stored in the territory of the PRC on secure and trusted servers. A personal information processor that, due to business needs, provides information outside the territory of the PRC, shall be in accordance with relevant laws and regulations and relevant requirements for a security assessment and review.	National Management Approach for Healthcare and Medical Big Data Standards, Security and Services (trial implementation)
Human genetic resources	Human genetic resources cannot be cross-border transferred in principle. Personal information processors are required to meet specific conditions in specific contexts, such as international collaborative scientific research, before they can provide human genetic resources outside the territory of the PRC.	Regulation on Human Genetic Resources Administration

Main approaches to provide personal information outside the territory of the PRC

A medical institution or pharmaceutical company that truly needs to provide personal information for a party outside the territory of the PRC for business' sake or other reasons, shall meet one of the following requirements:

- passing the security assessment for cross-border data transfers organized by the Cyberspace Administration of China (CAC);
- obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the CAC; and
- concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the CAC.

Security assessment for cross-border data transfers

When a medical institution or pharmaceutical company really needs to provide personal information outside the PRC for business or other reasons, and one of the following circumstances exists, it shall apply a security assessment for cross-border data transfers to the CAC through the provincial cyberspace administration where it is located:

- the personal information provided by a medical institution or pharmaceutical company outside the PRC is deemed to be important data;
- a medical institution or pharmaceutical company identified as a critical information infrastructure operator provides personal information abroad;
- a medical institution or pharmaceutical company that processes personal information of more than one million subjects provides personal information outside the PRC;
- a medical institution or pharmaceutical company that has provided personal information of 100,000 subjects or sensitive personal information of 10,000 subjects in total abroad since January 1 of the previous year; and
- other circumstances prescribed by the CAC for which the application of a security assessment for cross-border data transfers is required.

Before applying a security assessment, a medical institution or pharmaceutical company shall conduct a Personal Information Protection Impact Assessment (PIPIA) and a risk self-assessment for cross-border transfers in accordance with the PIPL and the Measures on Security Assessment of Cross-border Data Transfer, and clarify with the overseas recipient their responsibilities for data security protection.

The results of an approved security assessment are valid for two years from the issue date of the assessment result. If there is a need to continue data export activities, the medical institution or pharmaceutical company shall re-apply the assessment 60 working days before the expiry of the validity period. In the event of the circumstances stipulated in Article 15 of the Measures on Security Assessment of Cross-border Data Transfer, the validity period shall expire and the corresponding medical institution or pharmaceutical company shall re-apply the assessment.

Based on the sensitivity and volume of the personal information processed by medical institutions or pharmaceutical companies, applying security assessments for cross-border data transfers may be the major way for them to provide personal information outside the territory of the PRC.

In January 2023, the Cyberspace Administration of Beijing disclosed that the CAC approved and passed a research project between Beijing Friendship Hospital and Amsterdam University Medical Centres, becoming the first case in the PRC to pass a security assessment for cross-border data transfers. This case provides practical guidelines for strengthening the secure management of healthcare and medical data out of the PRC and promoting international medical research collaboration.

Standard contract and personal information protection certification

A medical institution or pharmaceutical company could choose to conduct personal information export activities by signing a standard contract with an overseas recipient or obtaining personal information protection certification from the relevant specialized institution when it meets all four of the following conditions:

- it is not a critical information infrastructure operator;
- it processes the personal information of less than 1 million subjects;
- it has cumulatively transferred abroad the personal information of less than 100,000 subjects since January 1 of the previous year; and
- it has cumulatively transferred abroad the sensitive personal information of less than 10,000 subjects since January 1 of the previous year.

When a medical institution or pharmaceutical company chooses to provide personal information abroad by signing a standard contract, it will be required to sign a Standard Contract of Personal Information Cross-Border Transfer with the overseas recipient, which is annexed to the Measures for the Standard Contract for Personal Information Cross-Border Transfer (which took effect on June 1, 2023). It is also required to conduct a PIPIA. The PRC has not yet issued official guidelines or reporting templates for PIPIA. There are overlaps in the content of the key assessment elements of the PIPIA required by the Measures for the Standard Contract for Personal Information Cross-Border Transfer and the cross-border data transfer risk self-assessment report template provided in the first version of the Guidelines for the Application of Security Assessment of Cross-border Data Transfer. The risk self-assessment report template can be used as a reference for preparing a PIPIA report. In addition, it shall file the standard contract with the provincial cyberspace administration where it is located within 10 working days from the date of the standard contract entry into force. The following materials shall be submitted for filing:

- the standard contract; and
- the PIPIA report.

Regarding the personal information protection certification, the PRC has currently issued the Personal Information Protection Certification Implementation Rules, the Cybersecurity Standard Practice Guideline - Safety Certification Specification for Personal Information Cross-border Processing Activities V2.0, and the draft Information Security Technology - Certification Requirements for Cross-border Transmission of Personal Information. Currently, a personal information processor can apply to the China Cybersecurity Review Technology and Certification Center for a personal information protection certification. However, there are still many gaps in the designation of specialized institutions and the implementation of certifications in the PRC, and further improvements are needed.

Special personal information: providing human genetic resources outside the PRC

There have been several cases in the PRC where the Ministry of Science and Technology (MOST) has penalized the unauthorized provision of human genetic resources information outside the PRC. The violations included:

- the unauthorized export of human genetic resources (human serum) as dog plasma, with the following penalties:
    - warning;
    - confiscation and destruction of the human genetic resources materials in the research project; and
    - suspension from accepting applications for international cooperation and export activities involving human genetic resources from the PRC by the company, to be reinstated after rectification is accepted by the MOST;
- the unauthorized transfer of part of the human genetic resources information from the internet outside the PRC, with the following penalties:
    - requirement to cease the relevant research project;
    - requirement to destroy all genetic resource materials not exported, as well as all related research data from the research project; and
    - requirement to stop the company's international cooperation involving Chinese human genetic resources and restart it again after the rectification is accepted by the MOST.

According to the Regulation on Human Genetic Resources Administration, foreign organizations, individuals, and the institutions established or actually controlled thereby shall not collect or preserve Chinese human genetic resources within the territory of the PRC, nor shall they provide Chinese human genetic resources out of the country. Where Chinese scientific research institutions, institutions of higher learning, medical institutions, or enterprises use Chinese human genetic resources to carry out international cooperative scientific research, or it is truly necessary to transport, mail, or carry out Chinese human genetic resources materials due to other special circumstances, they shall meet the following conditions and shall obtain export certificates for human genetic resource materials issued by the MOST:

- there is no harm to the public health, state security, and public interest of the PRC;
- the entities have legal person status;
- the entities have clear overseas cooperation partners and reasonable purposes of use for the transfer;
- the human genetic resource materials are collected in a legal manner or obtained from legal preservation institutions; and
- the entities have passed the ethical review.

When carrying out international cooperation in scientific research by utilization of Chinese human genetic resources, if it is necessary to transport, mail, or carry Chinese human genetic resources out of the PRC, a separate application may be filed, or the application may be filed simultaneously by listing the export plan in the application for international cooperation in scientific research, which shall be examined and approved in a consolidated manner by the MOST. If the Chinese human genetic resource materials are transported, mailed, or carried out of the PRC, the customs formalities shall be processed on the basis of the export certificates for human genetic resource materials.

In addition to the administrative penalties that may be imposed for illegally providing Chinese human genetic resources outside the PRC, a personal information processor may also commit the crime of smuggling human genetic material under the Criminal Law and will be subject to criminal liability for:

- whoever illegally transports, mails, or carries Chinese human genetic resources materials out of the PRC, endangering public health or social public interests, and the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, or public surveillance, and shall also be sentenced to a fine or a single fine; and

- if the circumstances are particularly serious, the personal information processor shall be sentenced to fixed-term imprisonment of not less than three years and not more than seven years, and shall be liable to a fine.

3.2 US

Health Data Standards Principles

Principles

The HHS health data standards efforts are based on the following principles:

- Health data should be more consistent across programs, payers, and other data holders; users should not be comparing "apples to oranges" when using data from different sources.

- Public and private sector health data should be of value to multiple users. As we move to more shared data standards, data collected once can be used for multiple purposes, dramatically reducing administrative burdens.

- Improvements in the collection and use of health data must be accompanied by assurances of privacy and security appropriate to an electronic environment.

- All interested parties -- private sector, states, consumers, federal agencies -- should collaborate in the evolution toward more shared data standards.

- Data standards are voluntary. Data standards efforts must move as a public- private partnership, with HHS facilitating evolution toward common data standards.

- The federal government can and should play three important roles in this voluntary process:

    - create a national forum allowing interested parties to collaborate;

    - participate fully with private standards development organizations and other interested groups in the voluntary effort to develop uniform health data standards; and

- to the greatest extent possible given its business needs, choose health data standards for its own health information systems that are compatible with state and private sector business needs and standards.

HHS efforts are wholly compatible with, but also move beyond, the principles set forth in "A Process for Government Selection of Standards for Its National Information Infrastructure (NII) Activities," June 29, 1995 draft (hereafter, the NII Report). The NII Report addresses standards selection internal to the federal government. While a portion of our efforts are aimed at improving the policy coherence of internal federal standards, in the health arena the line between internal and external data is porous, at best. In deciding how best to organize internal federal health data standards efforts, the need for coordination with our external data partners must always be kept in mind. Thus, the issues of interoperability and consensus development addressed here are broader than those addressed in the NII Report. We build on those principles and extend the effort to external interoperability issues.

This effort relies heavily on interdepartmental working groups, both as a matter of principle and as a practicality. As noted in the NII Report, selection of federal data standards should proceed through such inter-departmental working groups (called "affinity groups" in the NII Report), which "require representation from experts familiar with the technology and the extant standards...". Part of our effort involves reorganizing and consolidating multiple existing groups across agencies, and creation of an organizational framework that provides policy coherence across the groups and Departments.

- The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

- A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

- This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in the end notes. Visit our Privacy Rule section to view the entire Rule, and for other additional helpful information about how the Rule applies. In the event of a conflict between this summary and the Rule, the Rule governs.

Statutory and Regulatory Background

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

- HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2]

In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments.The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E.

Who is Covered by the Privacy Rule

The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use CMS's decision tool.

Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. If an insurance entity has separable lines of business, one of which is a health plan, the HIPAA regulations apply to the entity with respect to the health plan line of business.

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.

Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.[7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

Business Associates

Business Associate Defined. In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.

Business Associate Contract. When a covered entity uses a contractor or other non-workforce member to perform "*business associate*" services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that had an existing written contract or agreement with business associates prior to October 15, 2002, which was not renewed or modified prior to April 14, 2003, were permitted to continue to operate under that contract until they renewed the contract or April 14, 2004, whichever was first.[11] See additional guidance on Business Associates and sample business associate contract language.

What Information is Protected

Protected Health Information. The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]

General Principle for Uses and Disclosures

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16]

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See additional guidance on Government Access.

Permitted Uses and Disclosures

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See additional guidance on Treatment, Payment, & Health Care Operations.

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23] Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.[25] The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

For Notification and Other Purposes. A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care.[26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27] See additional guidance on Incidental Uses and Disclosures.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as required by law (including by statute, regulation, or court orders).[29]

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30] See additional guidance on Public Health Activities and CDC's web pages on Public Health and HIPAA Guidance.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32]

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.[33]

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39] See additional guidance on Research and NIH's publication of "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule." - PDF

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrolment in certain government benefit programs.[41]

Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] See additional guidance on Workers' Compensation.

(6) Limited Data Set. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.43 A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Authorized Uses and Disclosures

Authorization. A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrolment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45]

An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.[46]

Psychotherapy Notes.[47] A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:[48]

- The covered entity who originated the notes may use them for treatment.
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.

Marketing. Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;
- Communications for treatment of the individual; and
- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See additional guidance on Marketing.

Limiting Uses and Disclosures to the Minimum Necessary

Minimum Necessary. A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. See additional guidance on Minimum Necessary.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Access and Uses. For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

Disclosures and Requests for Disclosures. Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures*, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

Reasonable Reliance. If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.

Notice and Other Individual Rights

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See additional guidance on Notice.

- **Notice Distribution.** A covered health care provider with a *direct treatment* relationship with individuals must have delivered a privacy practices notice to patients starting April 14, 2003 as follows:
    - Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);
    - By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and
    - In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether direct treatment providers or indirect treatment providers (such as laboratories) or health plans must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an organized health care arrangement may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrolees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrolee at enrolment, and send a reminder to every enrolee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

Acknowledgement of Notice Receipt. A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrolment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. [58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

Disclosure Accounting. Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

Restriction Request. Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62]

Confidential Communications Requirements. Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyse their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64]

Privacy Personnel. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65]

Workforce Training and Management. Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68]

Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69]

Data Safeguards. A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See additional guidance on Incidental Uses and Disclosures.

Complaints. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72]

Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

Retaliation and Waiver. A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrolment or benefits eligibility.[74]

Documentation and Record Retention. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75]

Fully-Insured Group Health Plan Exception. The only administrative obligations with which a fully-insured group health plan that has no more than enrolment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]

Organizational Options

The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections.

Hybrid Entity. The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule.

Affiliated Covered Entity. Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.

Organized Health Care Arrangement. The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81]

Covered Entities With Multiple Covered Functions. A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan:[83]

- Enrolment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan.

- If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information).

- Protected health information of the group health plan's enrolees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.

Other Provisions: Personal Representatives and Minors

Personal Representatives. The Privacy Rule requires a covered entity to treat a "*personal representative*" the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

Special Case: Minors. In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See additional guidance on Personal Representatives.

State Law

Pre-emption. In general, State laws that are contrary to the Privacy Rule are pre-empted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal pre-emption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits.

Exception Determination. In addition, pre-emption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law:

- Is necessary to prevent fraud and abuse related to the provision of or payment for health care,
- Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
- Is necessary for State reporting on health care delivery or costs,
- Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
- Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

Enforcement and Penalties for Noncompliance

Compliance. The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes a set of national standards for the use and disclosure of an individual's health information – called protected health information – by covered entities, as well as standards for providing individuals with privacy rights to understand and control how their health information is used. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews.

Consistent with the principles for achieving compliance provided in the Privacy Rule, OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Privacy Rule. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution. These penalty provisions are explained below.

Civil Money Penalties. OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

Adjustments to CMP amounts for 2022 For violations on or after November 3, 2015	
Penalty Amount Per Violation	$127 - $63,973* per violation
Calendar Year Cap for Violation of Identical Requirement or Prohibition	$25,000 - $1,919,173**
***The Department of Health and Human Services *may* make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. The annual inflation amounts are found at 45 CFR § 102.3. **Pursuant to HHS's Notification of Enforcement Discretion, https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties	

A penalty will not be imposed for violations in certain circumstances, such as if:

- the failure to comply was not due to wilful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or

- the Department of Justice has imposed a criminal penalty for the failure to comply (see below).

In addition, OCR may choose to reduce a penalty if the failure to comply was due to reasonable cause and the penalty would be excessive given the nature and extent of the noncompliance.

Before OCR imposes a penalty, it will notify the covered entity and provide the covered entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be submitted to OCR within 30 days of receipt of the notice. In addition, if OCR states that it intends to impose a penalty, a covered entity has the right to request an administrative hearing to appeal the proposed penalty.

Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretences, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Priv

Compliance Dates

Compliance Schedule. All covered entities, except "small health plans," must have been compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, had until April 14, 2004 to comply.

Small Health Plans. A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.

4. Examples and Use cases

4.1 Azienda ospedaliero-universitaria Senese

Stating the concept of a Europe without borders, where all citizens can freely move for work or tourism, it is crucial that clinical data can also follow patients. As a consequence, clinicians will have access to patient's relevant data in order to provide clinical decisions that are consistent with the patient's medical history. The availability of shared data would allow the doctor, who knows the patient, and the specialist, to get to shared decisions (second-opinion) wherever they are. As an example, the following use case is briefly introduced.

A patient from Germany who is visiting Italy requires medical attention. With the cross-border health data exchange system, the Italian hospital can access the patient's medical history and treatment records from their home hospital in Germany. It will allow Italian healthcare physicians to provide informed and coordinated care, knowing about the patient's allergies, previous treatments, and medical conditions.

Using the same approach in the field of applied research would allow us to use the health data not only for clinical purposes, but also in sharing datasets for research purposes. A realistic use case is presented In the following paragraph.

Researchers, from different hospitals in Europe, collaborate on a study to understand the effectiveness of a new cancer treatment. They access anonymized and aggregated patient data from multiple hospitals, pooling their resources and expertise. This collaborative approach accelerates research progress and leads to potential breakthroughs in cancer treatment.

4.2 HealthData@EU pilot - European Health Data Space (EHDS2) EU project

French Health Data Hub coordinates and sets up a pilot project called EHDS2 (2022 -> 2024) with sixteen partners from ten European countries for the European Health Data Space to feed the legislative discussions about the draft regulation proposed by the European Commission on May 3rd on the EHDS. The project addresses the challenges of accessing health data throughout the EU. Five use cases have been selected: 1) infectious disease surveillance, Antimicrobial Resistance (AMR), 2) Thrombosis in COVID-19 patients, 3) COVID-19 testing, vaccination and hospitalization, 4) cardiometabolic diseases, and 5) colorectal cancer. Health Data Hub also highlights the need to compare health standards, nomenclatures, data formats, etc. such as SNOMED, HL7 FHIR, OMOP, DICOM. The ambition is to implement a first end-to-end European user pathway including data discovery (European metadata catalogue) and data access requests (development of a single data access application form).

4.3 BEIA

SHIFT-HUB proposes a technical platform pilot including a Health Data Hub, a Smart Health Apps Repository and an on-line Marketplace to support the experimental development based on a secure and interoperable access to data and showcase a portfolio of solutions developed by the community members. SHIFT-HUB aims to establish a pan-European Smart Health Innovation Hub bringing together a rich network of multidisciplinary stakeholders across the dimensions of the quadruple helix, with the mission to facilitate the development, ensure the promotion and foster the uptake of Smart Health technologies and services. SHIFT-HUB will develop and test with the community a complete service offer, integrating networking and matchmaking, identification of partners and support for procurement, guidance for access to funding, research infrastructures and scientific expertise.

4.4 CCG

Health data may come from many sources. Often sources are the annotations resulting from medical appointments, periodic records created by health professionals that track long-term patients, different health exams prescribed by doctors, and, more recently, data automatically generated by new technological devices like smartwatches.

A significant effort is being made to create standards and implement interoperable systems, seeking an ideal scenario with a unique record for each person, regardless of the data source. This praiseworthy effort would create a data lake. It would benefit patients, who would have permanent access to their unified data, and practitioners, who would have more information that eventually helps make medical decisions.

Falls are the worldwide leading cause of injury-related deaths and non-fatal injuries in people 65 years and older. Falls represent the second leading cause of unintentional injury death. When falls are not fatal, they leave serious injuries and levels of morbidity with a major risk of long-care needs.

Alertfalls research project[4] aimed to identify the prevalence and risk factors of falling in older people living alone. The research team made an analytic cohort study, including 186 participants aged 65+ living alone or in community-dwelling.

The questionaries included sociodemographic information, social and health resources, physical conditions, functionality, technical devices used, difficulties related to daily life, medication, risk behaviours and physical environmental conditions related to the house. It included data that can't be found in any regular health database.

Although some constraints may arise from the small sample of participants, the project data allowed us to achieve some valid results:

- It enabled the identification of various fall risk profiles. This awareness should be considered by those who get in touch with older persons living alone in a community context.
- A predictive model was developed, revealing a satisfactory discriminatory performance of the model to identify the risk of falling among older people living alone in a community context.
- Some falling factors currently are subject to no records on health databases. Expanding information about older people would enable calculating a falling risk and, consequently, working to mitigate it.

Based on the Alertfall findings, it is possible to facilitate more proactive interventions across multiple stakeholders in the social and health sectors.

[4] Lage, I.; Braga, F.; Almendra, M.; Meneses, F.; Teixeira, L.; Araújo, O. Older People Living Alone: A Predictive Model of Fall Risk. *Int. J. Environ. Res. Public Health* 2023,*20*,6284. https://doi.org/10.3390/ijerph20136284

4.5 IDERHA project

The aim of **IDERHA project** is to facilitate access and reuse of heterogenous health data and it will be demonstrated in use cases selected throughout the lung-cancer patient journey. The IDERHA network infrastructure will connect (WP1) existing data resources at data providers' sites and allow users to access the data, share them and perform their integrative analysis (WP2) through the application of common data standards (WP4) and in conformance with GDPR and regulatory requirements (WP5). Existing (retrospective) datasets will be used by the project partners for the development of analysis algorithms (WP2), as well as to evaluate and demonstrate the value and utility of the IDERHA platform to patients, researchers, regulators, and other stakeholders (WP3). In addition, remote patient monitoring and data access consent management will be enabled with dedicated mobile applications (WP1).

The expected types of research data that will be addressed within IDERHA include several categories of low and high dimensional data: clinical and molecular data (such as genomics, transcriptomics, proteomics, metabolomics), image data and patient generated data types, including wearables measurements, PROMs and PREMs, and questionnaires. In addition to interconnecting data providers, IDERHA aims to also offer solutions for individual data providers to enable them to share their own resources, so-called citizen-controlled data, with other users for specific purposes. With the citizen-controlled data sharing application, citizen users (whether patients or not) can decide what personal health data (PHD) pertaining to themselves is shared with other parties, and for what purposes.

4.6 Astea

High availability of anonymized medical imaging data is crucial for the technology development and readiness improvement of a number of projects pursued by Astea Solutions, all related to combining research with addressing physician needs especially in places with high ration of patients to physicians. Astea is working on a number of such projects in the fields of ophtalmology, oncology and others with relevant medical and research partners. These projects involve training state-of-the-art prediction models and so require high volumes of data that require all dataspace prerequisites, as provided by the reference model: automated conversion workflows, anonymisation, data rooming, among others. Medical facilities are willing to participate but usually on a single basis, i.e. it is difficult to provide enough trust in the flow to incentivize more providers of medical imaging data. The projects further involve reusable medical workflows components, addressing the needs of physicians for AI-assisted tele-based quick diagnostics and patient journey discovery. Such projects necessarily need to be interoperable with national and European standards and government systems and this is where a common European dataspace for medical data is a crucial asset for the success and scaling up uf the innovative component of the projects.

5. Conclusion and Recommendations

Within the European Health Data Space (EHDS), prioritizing data sustainability, synchronization, interoperability, and minimizing the workload for healthcare professionals can lead to significant advancements in healthcare. By fostering seamless data exchange and integration across different healthcare systems, the EHDS can enhance the coordination of patient care and minimize potential errors. Access to comprehensive medical histories and anamnesis data allows healthcare providers to make well-informed decisions, resulting in improved patient care pathways.

Additionally, the availability of a larger and more diverse database within the EHDS can lead to the development of more advanced and personalized healthcare applications. These applications can leverage insights from extensive datasets to offer tailored healthcare solutions, optimizing treatment plans based on individual patient needs. Such data-driven approaches hold the potential to improve healthcare outcomes and enhance the overall quality of healthcare services across the European Union.

In conclusion, prioritizing data sustainability, synchronization, interoperability, and reducing the workload for healthcare professionals within the EHDS can pave the way for more efficient, patient-centred, and data-informed healthcare practices, ultimately benefiting the health and well-being of EU citizens.

The EHDS is expected to bring great benefit, but it also brings challenges related to technology, governance and privacy as such EU approaches to health data have struggled due to several key limitations that we believe need to be addressed to make the full potential of the EHDS:

1. Uncertain demand on the part of patients for cross-border delivery of eHealth services;
2. Impediments posed by the simultaneous need to maintain the privacy and confidentiality of sensitive health data;
3. Insufficient incentives for Member States and institutions to participate in data-pooling arrangements;
4. Lack of a strong mandate to proceed at EU level (subsidiarity); and
5. The risk of problematic interactions with other EU and national legal instruments.
6. Guidelines from the Commission on how various actors have at their disposal and how to implement/use data spaces.

When dealing with healthcare projects based on Big Data, another issue to be considered is standardization.

Usually, Clinical Data Repositories lay at the basis of such projects, aiming to organize the corporate information assets according to an open and stable standard model. The goal is to achieve data integration into the health information system (i.e. to Laboratory Medicine), fetching info from different applications with no need to modify existing applications. As a matter of fact, data coming from different diagnostic sources may be not comparable since they're not harmonized, because of:

- coming from analytical methodologies with evident biases between them
- reported with different units of measurement
- presenting different levels of analytical quality.

It should also be noted that laboratory information is not only made of structured data but interpretative comments are often used as well (i.e. haematology or urine tests). In such cases the data, being not structured, should first be processed with AI software in charge of structuring the information.

The reuse of laboratory results contained in repositories, in order to ensure unique provenance and standardization, requires additional data items (material, analyte, value, unit and reference interval) in order to support interpretation and comparability (e.g., method, test vendor, equipment, and consumable lot numbers).

For the univocal identification of the performance on a particular biological matrix, the adoption of unique national or international coding such as LOINC (Logical Observation Identifier Names and Codes) or more generally SNOMED (Systematic Nomenclature of Medicine, Clinical Term) becomes essential.

Another challenge is represented by POCTs (e.g. blood glucose meters, blood gases).

In fact, laboratory diagnostics are currently provided by multiple operators (laboratory technicians or nurses for POCT), multiple laboratories or even by the patients themselves when they use self-test devices or wearable devices to acquire physiological measurements. POCTs represent in all respects instruments for in vitro diagnostics but are used by departments and in any case by non-laboratory structures. The legislation and the Guidelines however speak of a control by the Laboratory but where these POCTs are not interfaced with the LIS, the data are not monitored in a standard way. As a consequence, the data flow is weak and often is not even adequate for the administrative purposes.

Contributors

Editor:

Pietro Dionisio, Medea

Reviewer:

Damir Filipovic, AIOTI Secretary General

Contributors:

Pietro Dionisio, Medea

Damir Filipovic, AIOTI Secretary General

Alberto Marini, Azienda ospedaliero-universitaria Senese

Gianluca Daino, Azienda ospedaliero-universitaria Senese

Roberto Guerranti, Azienda ospedaliero-universitaria Senese

Gianpaolo Ghisalberti, Azienda ospedaliero-universitaria Senese

Amelie Gyrard, Trialog

George Suciu, BEIA

Luminita Marcu, BEIA

Filipe Meneses, CCG

Odete Araújo, CCG

Fátima Braga, CCG

Philip Gribbon, Fraunhofer

Joro Penchev, Astea Solutions

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.