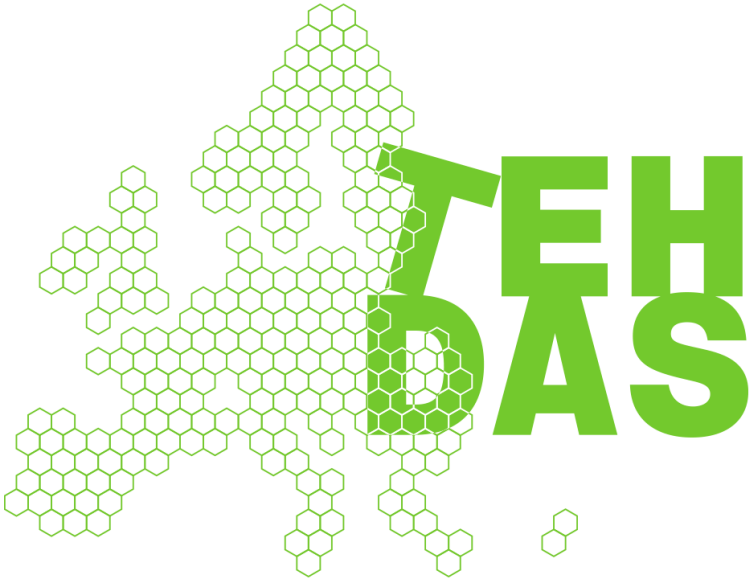


Towards European Health Data Space

Summary of Milestone 5.1 & 5.2

Annex A | Case studies: different governance and health data systems in Europe

Authors: Linda Abboud, Shona Cosgrove, Irini Kesisoglou, Rosie Richards, Flavio Soares.

28 September 2021

This project has been co-funded by the European Union's 3rd Health Programme (2014-2020) under Grant Agreement no 101035467.

Accepted in Project Steering Group on 28 September 2021.

Disclaimer
The content of this deliverable represents the views of the author(s) only and is his/her/their sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use of its contents.

Copyright Notice
Copyright © 2021 TEHDAS Consortium Partners. All rights reserved. For more information on the project, please see www.tehdas.eu.

Contents

1 Austria

1.1 Overview

The Austrian ministry of health is responsible for oversight and aggregated data for policy makers and health authorities, while maintaining and developing federal data systems for special purposes, such as the epidemic reporting system, or drug addiction treatments. Databases developed by the ministry further allow for processing and analysis based on aggregated data, with the Ministry acting as data controller. Data originates from a range of healthcare providers.

Other bodies, such as ELGA - a legal entity owned jointly by the federal administration, federal states, and the social insurance developing the Austrian electronic health record system - is tasked with handling, exchanging, and making accessible Electronic Health Records. These records are legally not available for research, and there is no cross-border exchange.

In addition, several other entities and organisations hold personal data relating to citizens' health. The Austrian social insurance processes data related to health insurance cases. The Institute for Public Health and Food Safety (AGES), collects, maintains, and processes data related to food and medicine safety. The National Institute for Health Research (GÖG) provides pandemic data to verified medical universities after a standardized application process.

1.2 Accessing health data in Austria

Access to health data must have a legal basis. If such basis is provided, standardised processes allow access to such data to research institutes and universities. The health data which are shared are typically pseudonymised. There are a variety of access mechanisms and monitoring processes, dependent on each organisation's own governance processes. For example, requests to access pandemic data held by GÖG overseen by a committee with delegated authority.

2 Belgium

In Belgium there are a number of actors within the health data system. Key organisations include:

- **Intermutualistic Agency**: health care prescription data
- **Statbel:** mortality and cause of death data
- **Belgian Cancer Registry**: cancer diagnosis
- **FPS Health**: hospital discharge data
- **Intego (KU Leuven)**: primary care (GP)
- **Sciensano**: health surveys, surveillance, and rare disease registries

The federal health data system is eHealth, a platform that includes the following organisations:

eHealth Platform Organisations	
National Institute for Sickness and Invalidity Insurance (INAMI)	Federal Public Service Public Health, Food Chain Safety and Environment
EHealth platform	Scientific Institute of Public Health
Brussels Health Network - Abrumet asbl	Federal Agency for Medicines and Health Products
Medex	Data protection authority
Agentschap Zorg & Gezondheid	Federal Center of Expertise for Health Care (KCE)
Walloon Health Network (RSW)	Agency for a Quality Life
Zorgplatform collaborator	Vlaams Ziekenhuisnetwerk KU Leuven
National Intermutualist College (CIN)	Mutual funds
The League of Users of Health Services (LUSS)	ZNA - care portal
Wallonia	

These organisations can act as controller, processor or neither depending on the specifics of the data processing. There is no "fixed" definition of who can act as data processor or controller because this depends on specific applications. Data comes from citizens (directly or indirectly e.g., from registers, surveillances, other databases). Organisations can have

different types of data and most have several types including health records, survey data, biological material, and samples.

2.1 Accessing health data in Belgium

Access to health data is granted through collaboration agreements between the data holder and the organisation requesting access. In some circumstances it is necessary to submit an application to the information security committee.

3 Denmark

3.1 Overview

The two main national bodies that host health data are Statistics Denmark, which stores data about the wider Danish population, and the Danish Health Data Authority (Sundhedsdatastyrelsen), which hosts disease registers and data bases with health-related information. Statistics Denmark is a public independent agency and holds copies of register data and can extract health data and combine it with social conditions when the researcher requests it.

All data is exchanged via the platform Sundheddatanettet. Data is not stored there but it is a secure space where you need authentication and approval to be linked up through VPN-access so that you can exchange data. MedCom is responsible for developing and setting standards for data exchange and testing supplier products before they are released to ensure data compatibility. Sundhed.dk's two-year strategy intends to open up safe spaces for storage of citizen generated data, which can potentially be marked as available for research too, but this is not operating yet.

3.2 Accessing health data in Denmark

Researchers can apply for access to data locally with data custodians, or for the whole country through the Researcher Service (Forskerservice) at Serum Institute (when it is health data only) and through Statistics Denmark, if the researcher wants to combine health data with other data types. The Danish Health Data Authority holds all health registers and provides research support service (Forskerservice) for researchers who wish to access health data. It is also responsible for national coordination of data exchange systems and infrastructures for the provision of healthcare. The Danish Clinical Quality Program (RKKP) is the cross-regional network organisation of the five Danish regions that constitutes the infrastructure of clinical quality registries and coordinates access to the data for researchers.

Decisions regarding access are made by the steering group of the individual database. There is a fee for accessing data for research that must be paid to Statistics Denmark, the Serum Institute, or DAK-E. The fee covers the hours spent on setting up the specific data set, and for DAK-E it also covers the commercial vendor fee. It does not cover the cost of the infrastructure. Registry data is available for research with no informed consent ("solidarity by law").

In Denmark there is a differentiation between clinical access points and research access points. Sundhed.dk is the access point to European health records for patients and for health professionals for clinical purposes. A researcher needing data for research has several access points and can go to the Danish Clinical Quality Program (RKKP) for quality databases, the Serum Institute for health data, and to Statistics Denmark for registry data combined across sectors.

Primary care data must be accessed through the municipalities (for homecare and nursing homes) and DAK-E/KIAP from the Danish Quality Unit for General Practice for GP-data. Sundhed.dk is an independent agency governed by the Regions and the Government and contains the national European health records. At the sundhed.dk platform patients can access personal health information from European health records, laboratories, personal choices (e.g., organ donor), and the national patient registry. The patients can access their record, but they cannot report data or control the data. Health professionals also have access to the European health records.

The National Biobank, hosted by the Staten Serum Institute, and the Regional Biobank Program provide access to tissue samples. The National Genome Centre provides access to genomic data. The Health Act specifies that all genomic data from comprehensive genetic analyses is stored in a national genomic database and that patients have the right to opt-out of further use of the data.

Statistics Denmark has been involved in several working groups to facilitate data exchange between different countries. Data from Statistics Denmark is as a main rule only available for Danish researchers, but foreign researchers can get access to micro data through an affiliation to a Danish authorised environment. The Danish Health Data Authority applies the same rules.

There is a fee for accessing data for research that one must pay to Statistics Denmark, the Danish Health Data Authority, the Serum Institute, or DAK-E (for GP data) but that only covers the hours spent on setting up the specific data set, and for DAK-E also the commercial vendor fee. It is not the cost of the infrastructure.

The capital and Zealand region of Denmark use the EPIC systems. The health data is structured in an SQL database where data is stored in both EPIC defined keys and locally defined keys. External access to health data requires an approved research project.

4 Estonia

4.1 Overview

In Estonia, the Health Information System (HIS) database contains records relating to health care, including contracts for the provision of health services, health statistics and for the management of health care. The database was established by the Health Services Organisation Act. HIS enables the exchange of information between doctors by connecting IT systems for health services. The HIS gives doctors access to a selection of a patient's health information and provides timely, critical information to ambulance services. The data controller of the Health Information System is the Ministry of Social Affairs.

Health care providers are required to submit the following data:

- Waiting lists
- Medical images
- Health services provided to patients
- Management of health care, including for maintaining registers concerning the state of health established based on law.

The composition of the data, such as documents, conditions, and procedure for the preservation of the documents to be forwarded to the HIS, are established by the Ministry of Health and Labour.

4.2 Accessing health data in Estonia

Patients can access their personal data held on HIS. In order to protect a patient's life or health, a health care provider may delay forwarding data to the HIS to allow patients an opportunity to examine their personal data with a health care professional.

Health care providers and third parties involved in the provision of health services have access to the personal data in HIS for entry into and performance of a contract for the provision of a health service.

The basis for collecting data is context dependent:

- Within the health system patients opt-in. Patients' data is collected by default for all healthcare services and there is an assumption that a person agrees to the processing of their health data when using the services.
- Outside the health system individuals must opt-out. This means data subjects' consent is necessary for the processing.

Patients have the right to prohibit the access of a health care provider to their personal data in the HIS. The health service provider must be registered in the National Registry of activity licenses for provision of health services and the National registry of health care professionals.

When researchers wish to access data for scientific research, they must apply for access to the personal data held on HIS to the controller of the HIS. The ethics committee of the HIS assesses whether the release of personal data from the HIS for the purposes of scientific research or statistics is justified. The assessment of the ethics committee is not legally binding for the controller, and the controller grants authorisation.

5 Finland

5.1 Overview

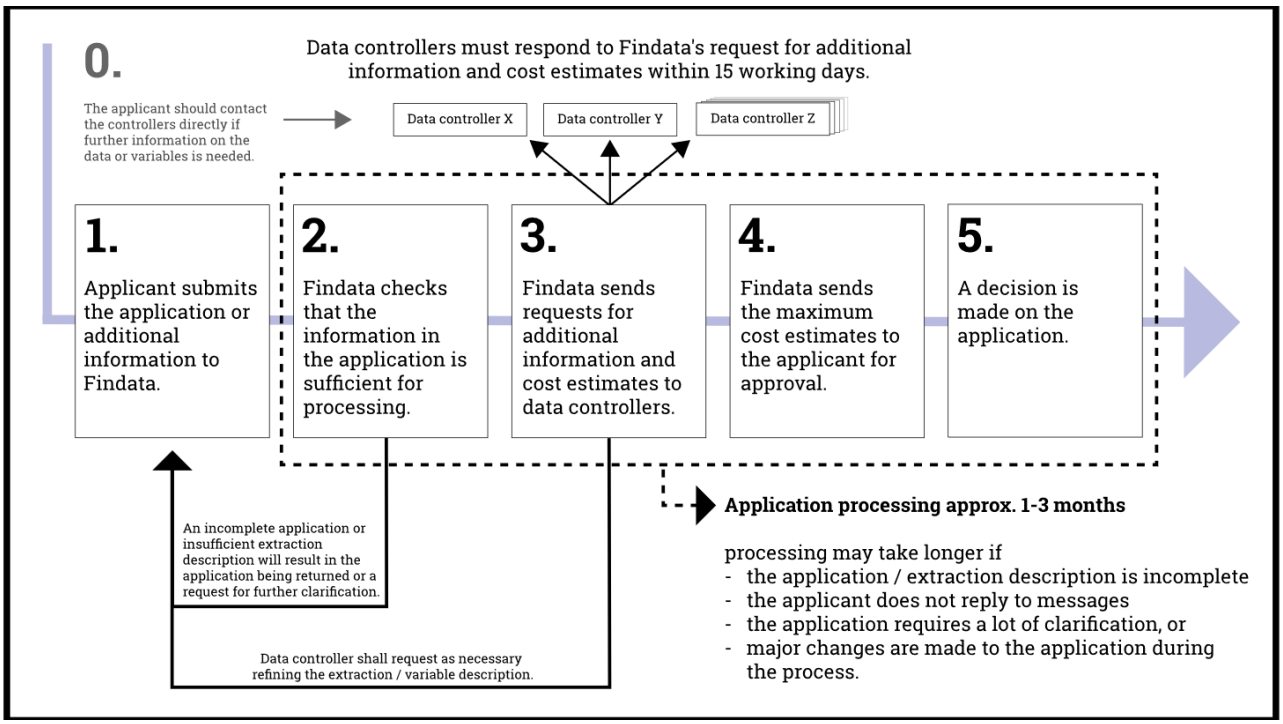
The data comes from local and regional health service providers, they are registered owners or data controllers (mainly municipalities responsible for primary health care or hospital districts, university hospitals responsible for special health care or from national registers/data controllers) like the Finnish Institute for Health and Welfare, Social Insurance Fund, Finnish Centre for Pension, Statistics Finland. Data comes digitally from European health records (EHR) and electronic patient records (EPR) systems to national systems and registries. The National Electronic Health Records archive system is available for secondary use of health and social data.

Data from 11 Finnish Biobanks is available, alongside socio-economic data from income registries, family and household data from a population registry. The organisation has social and health data: client and patient data EPR's, EHR's, prescriptions, referrals, medication data, patient flows, social care client data and social insurance data, income data, household data, family structure data, and other economic data and statistical information.

5.2 Accessing health data in Finland

If you need health data from only one data controller or register keeper, you need to ask for permission from that data controller or registry. If you need data from several and different sources and data controller on the national, regional, or local level, you need to ask for permission from FinData, a national social and health care data permit authority. FinData both gives the permit and collects, combines the data from the different data controllers and transfers the combined needed dataset into safe and secure ICT environment to customer who can have access to anonymous or pseudonymous data. Aggregated data can be delivered to user's own ICT environment.

Figure 1: The monitoring and data access process in Finland



6 Greece

6.1 Overview

EOPYY, the National Organisation for the Provision of Health Services, holds electronic health record data for patients through the e-prescription IT platform. Since 2011, Greece holds an e-prescription Information Platform for medicines, medical tests and materials needed to be prescribed. The e-prescription procedures are obligatory for health providers (doctors, health organisations, pharmacies) either in the public or private Health Sector, under public insurance laws. These health data do not include diagnosis and test results but only the prescribed medicines, tests, and materials.

- **EOPYY** also holds data for all health providers with which they have legally binding contracts. Health Providers of the public sector must belong to EOPYY. Health Providers of the Private Sector cooperate with EPOYY through legally binding contracts.
- **HDIKA AE:** is the public organisation which is the owner of the e-prescription IT Platform.
- **Hospital Information System**: each hospital (either public or private) has its own information system, so each hospital produces, holds, and controls data of all types. These Health Organisations share regulated data with EOPYY (National Organisation for the Provision of Health Services) through e-prescription and other IT platforms. The data does not include diagnosis or test results. These organisations may

exchange data under the GDPR and national laws grid for health data with other organisations, mainly for research and/or governance purposes.

- **Primary Health Care Units** (either in Public or in the Private sector): Produce and hold health data. They share regulated data with EOPYY through the e-prescription IT platform.

6.2 Accessing health data in Greece

For a citizen, in order to obtain health data from a health organisation (e.g., a hospital) a citizen should lawfully apply for a copy of its health file. This procedure refers only for a person's own health data and does not include electronic data. The e-prescription IT platform is not yet open to citizens but only to health providers.

The health organisation which produces and holds the data is the only responsible for the data. Only under the strict national law grid for data protection and the GDPR rules and after an application of interest and purpose can someone (person, organisation, etc) gain access to data.

7 Ireland

7.1 Overview

The Health Information and Quality Authority (HIQA) has a statutory remit to develop standards, evaluate information and make recommendations about deficiencies in health information under the Health Act 2007. The HIQA oversees the following data collections:

- National Screening Service - BreastCheck
- Hospital Pricing Office (HPO) - Hospital In-patient Enquiry (HIPE) scheme
- Health Service Executive (HSE) - Primary Care Reimbursement Service (PCRS)
- Health Protection Surveillance Centre (HPSC) - Computerised Infectious Disease Reporting (CIDR)
- HSE – National Incident Management System (NIMS)

HPSC disseminates information and data from CIDR through a wide variety of methods to ensure that infectious disease data and information is accessible to a wide range of stakeholders. For example, weekly, monthly, quarterly, and annual reports are published online on HPSC website. Other outputs include frequent social media posts, presentations, and scientific paper publications. HPSC have a number of national KPIs in relation to the dissemination of CIDR data which ensures the timely publication of key infectious disease data on a weekly basis. At a local level, CIDR data is used to manage infectious diseases. Within hospitals, medical staff and management can use surveillance data for audit and research purposes.

At a national level, the data is used to trend incidence and burden of infectious disease regionally and nationally, as well for planning services. In addition, CIDR data is used to enable Ireland to meet its obligations in reporting notifiable infectious disease data to international agencies such as the European Centre for Disease Control (ECDC), the European Food Safety Authority (EFSA) and the World Health Organisation (WHO). For example, the data is submitted to ECDC through the European Surveillance System (TESSy) and is used to analyse and disseminate surveillance data on infectious diseases in Europe.

7.2 Accessing health data in Ireland

On the HPSC website, the publications page is dedicated to disseminating a variety of reports which provide website visitors with access to summary statistical data on the range of disease topic areas monitored on CIDR. The use of information is monitored by an Information Officer and the use of data is reported in a monthly and annual report on the impact assessment of outputs. There is a process in place for assessing and processing external data requests at a national level. The protection and disclosure of CIDR data is subject to the legal remit of the Health Act 2007 and data protection legislation. The CIDR National Peer Review Group reviews requests for data from CIDR and the purpose for which it is requested. This purpose needs to be in line with the reason that the information was originally collected, that is, the surveillance, management, prevention and control of the notifiable infectious diseases and their causative organisms. To ensure that this information is protected and only disclosed appropriately, application to the CIDR National Peer Review Group is required for CIDR data requests from third parties and from CIDR partners seeking access to CIDR data beyond their current access level. The CIDR National Peer Review Group provides a clear procedure regarding the application and assessment process for accessing and using CIDR data. However, information relating to this group, or the formal data request procedure is not available online on the HPSC website.

8 Moldova

8.1 Overview

The National Bureau of Statistics (NBS) is the central administrative authority which manages and coordinates the activity in the field of statistics from the country. The NBS works independently or in collaboration with other central administrative bodies to approve the methodologies of statistical and calculation surveys of statistical indicators. The NBS ensures these methodologies are in accordance with international standards, especially those of the European Union, and with the advanced practice of other countries, as well as considering the peculiarities of the socio-economic conditions of the Republic of Moldova. In addition, the NBS, organizes programmes of statistical works, annually approved by the Government, statistical surveys regarding the situation and economic, social, demographic development of the country and collects, processes, stores and disseminates statistical data.

A component part of NBS is the General Division for Social and Demography Statistics with Social Services Statistics Division, which produces statistical indicators and provides statistical data and information on various social issues, such as health, justice, public utilities, social protection and assistance, gender statistics, etc. The Social Services Statistics

Division processes and controls data coming from the regional institutions working in the field of social services statistics. Statbank “Health protection” has health records, collected in electronic format through the ""e-Reporting"" portal.

The Ministry of Health, Labour and Social Protection provides data to NBS and has an Internal Audit Service, which conducts audit activities in subordinated institutions. The National Agency for Public Health (NAPH) is an administrative authority subordinated to the Ministry of Health, Labour and Social Protection, and is responsible for maintaining and managing the national database of health statistics. Its basic functions include the collection, standardisation, and analysis of statistical information on public health received from territorial subdivisions including public health centres, and the creation of automated systems for the collection of operational information on the population’s health.

Many other separate information flows reflecting activities within different national health programmes, and in state surveillance of public health, are managed by the NAPH: Transplant, Tuberculosis, AIDS, etc.

The Family Doctor's Centre coordinates the activity of the primary medical assistance in the territory, performs the centralization of the statistical medical data and submits reports of their activity directly to the public health centre. The National Health Insurance Company (NHIC) is a state non-profit-making body with financial autonomy and manages a separate information system for monitoring of individuals covered under medical health insurance, oversight of contributions and economic aspects of health service provision. The NHIC covers the whole territory of the Republic of Moldova through territorial agencies, coordinating and supervising their activity within the existing legal framework.

8.2 Accessing health data in Moldova

Moldovan citizens have free access to the health data within the Statbank “Health protection” on the web page (www.statistica.gov.md). The access to data in our health data system within the National Bureau of Statistics is free (www.statistica.gov.md). The web page www.statistica.gov.md permits to download free “statistical yearbooks of the health system”.

9 Sweden

9.1 Overview

The National Board of Health and Welfare is the data controller for health data registers in the field of health care and social services and the cause of death register. The registers form the basis for the official statistics in the field of health and diseases, health care, social services and causes of death.

Swedish National Quality Registries is the data controller and data processor for registries containing individualized data about medical interventions, procedures, and outcomes. They are integrated into clinical workflows and have the capacity to generate data in real time. Each registry is supported by an organisation of health care professionals and patient representatives. They are jointly responsible for developing the registry.

Swedish eHealth Agency is the data controller and data processor for several registries and databases that link healthcare, pharmacies, and patients. The eHealth Agency facilitates the work of healthcare and create the conditions for better health.

Sweden's healthcare system consists of 21 regional healthcare authorities and different healthcare providers and the use of different journal systems with no or very few interconnections in between. The journals act as data controller. Data is supplied by health care practitioners and consists of health records for in-patient care, diagnoses, and pharmaceuticals.

Registerforskning.se acts as a data controller and is operated by the Swedish Research Council to provide researchers with information on existing registers, as well as support during the process of register-based research. Information on each part of the process of identifying, requesting, and using register data. A metadata tool called RUT (Register Utiliser Tool) enables efficient searching and matching of metadata in registers is also available.

9.2 Accessing health data in Sweden

Data access is primarily governed by the Patient Data Act, the General Data Protection Regulation (GDPR) and the Public Access to Information and Confidentiality Act which lay out how personal data may be used, and medical records are to be handled. The healthcare provider must have its own procedures that complement how and when the data may be used.

The National Board of Health and Welfare is the data controller for health data registers in the field of health care and social services and the cause of death register. The registers form the basis for the official statistics in the field of health and diseases, health care, social services and causes of death.

The data in the National Board of Health and Welfare's health data register and registers in the field of social services are covered by absolute confidentiality. From the registers, personal data can only be disclosed for research and statistical purposes and data that cannot be directly attributed to the individual. In these cases, the information may be disclosed if it can be disclosed without injury or harm to the person concerned or to any related party.

The registers are protected by confidentiality, but data may be disclosed after special examination which includes an application to the Swedish Ethical Review Authority. Each disclosure requires a formal written decision based on a special confidentiality review in which the National Board of Health and Welfare investigates whether there is legal support for breaching confidentiality under the Public Access to Information and Confidentiality Act (24:8). This applies to new cases as well as when ordering updates to ongoing projects where the National Board of Health and Welfare has previously disclosed data.

In Sweden access depends on the purpose. For clinical use, medical staff have access to the information in the NPÖ, provided the individual gives his or her consent. All research where individuals are directly or indirectly involved or affected requires the approval of an agency (Etikprövningsmyndigheten) tasked with reviewing the ethics of the proposed research.

Health care, as well as health data, is managed separately by 21 different regions and to some extent, mostly home care for the elderly, by 290 municipalities. Some of the health care for which the regions are responsible for is outsourced to private operators who, in some cases, use the same Electronic medical records (EMR) and other systems as the region-operated health facilities. In other cases, they use their own systems. In all these cases, they are controllers.

The National Patient Overview (NPÖ) which allows clinicians to access (=viewing) limited, predefined sets of information in the EMR-systems in other regions. Separate from the EMR-systems and all other care and care management systems in the regions, there are some 100 freestanding, mostly diagnosis-related national "quality registries" in which interventions and outcomes in the different medical domains are manually recorded. The latter are used for monitoring and research within, but because of stovepipe nature not across, medical domains. The National Board of Health and Welfare (Socialstyrelsen) keeps six national registries, on cancer; patients treated in hospitals and specialised care facilities; births (incl. medical data); drugs sold over the counter; dental care; and care carried out at county level.

10 United Kingdom

10.1 Overview

The structure of UK health data systems is complex with multiple organisations collecting, holding, and sharing data. Individual NHS hospital trusts, and GPs (primary care) act as data controllers for the patients they treat. There is also a small number of private and voluntary sector providers of healthcare, sometimes commissioned or funded to provide NHS services. Local authorities and private providers of social care also hold data on recipients of social care in residential homes or domiciliary settings. Academic institutions and pharmaceutical companies running clinical trials and cohort studies also hold bespoke data about participants in their research. Health is a devolved matter in the UK, so each of the home nations has slightly different arrangements for managing health and care information, particularly in relation to secondary purposes but in England:

A number of the Department for Health and Social Care's Arms Lengths Bodies also hold health data. In particular:

- NHS Digital is the national information and technology partner to the health and care system. NHS Digital has responsibility for standardising, collecting, and publishing data and information from across the health and social care system in England.
- NHS England also holds a range of health data - to support a range of secondary health care purposes such as service planning and population health management; it also established a Covid-19 Datastore to support the pandemic response.
- Public Health England has powers to collect patient data in relation to communicable disease surveillance and other risks to public health (e.g., to support the administration of immunisation programmes). It is also responsible for the National Cancer Register.

Furthermore, UK Biobank, is a large-scale biomedical database and research resource, containing in-depth genetic and health information from half a million UK participants collected with their explicit consent.

Genomics England (GE) was set up to deliver the 100,000 Genomes Project and clinical, laboratory and health data flows from a number of NHS, Social Care, and research organisations to GE.

Clinical Practice Research Datalink (CPRD) is a real-world research service supporting retrospective and prospective public health and clinical studies. CPRD collects anonymised patient data from a network of GP practices across the UK. Primary care data is linked to a range of other health related data to provide a longitudinal, representative UK population health dataset.

Health Data Research UK, the national institute for health data science, runs the Health Data Innovation Gateway. This portal provides a common entry point to discover and request access to UK health datasets.

The data collection and sharing landscape varies between devolved administrations, with some organisations (e.g., UK Biobank) operating across the four nations, whereas others (e.g., NHS Digital) are England only.

Processes for accessing health data vary according to organisation. However, all operate within the UK legal framework. All use of personal data in the UK is subject to the following data protection legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)

The UK GDPR establishes the basis for sharing personal data (that is data which directly or indirectly identifies a living person). The DPA puts those safeguards into UK Law. The legislation provides several key protections and safeguards for the use of an individual's data as set out below.

10.2 Principles for sharing data

Sharing of personal data in the UK has to follow strict rules and must follow the seven key data protection principles set out in the UK GDPR. These provide that personal data must be:

- used fairly, lawfully, and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant, and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage.
- used responsibly ensuring compliance with the principles of the UK GDPR.

10.3 Lawful basis

The UK GDPR and the DPA set out the ways in which personal data can be lawfully processed. All processing of personal data must be on the basis of at least one of the following:

- **consent:** the individual has given clear consent for you to process their personal data for a specific purpose
- **contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations),
- **vital interests**: the processing is necessary to protect someone's life
- **public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- **legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Under the UK GDPR, health data is defined as special category data (that is data that requires additional protections due to its sensitivity). For this type of data to be processed a further condition must be met in addition to one of the lawful bases set out above. These conditions could be:

- explicit consent
- employment, social security, and social protection (if authorised by law)
- vital interests
- not-for-profit bodies
- made public by the data subject
- legal claims or judicial acts
- reasons of substantial public interest (with a basis in law)
- health or social care (with a basis in law)
- public health (with a basis in law)

- archiving, research, and statistics (with a basis in law)

10.4 Common Law

Alongside data protection legislation, the common law duty of confidentiality also applies to the use of confidential patient information.

The general position is that if information is given in circumstances where a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

The three circumstances where disclosure of confidential patient information is permitted are:

- where the individual to whom the information relates has consented
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest
- where there is a statutory basis for disclosing the information or a legal duty (such as a court order) to do so

10.5 Monitoring

In the UK, the Information Commissioner upholds information rights as the independent regulator dealing with the Data Protection Act 2018 and the UK General Data Protection Regulation. The Information Commissioner investigates complaints of breaches of data law and can issue fines where complaints are upheld.

The Information Commissioner also provides guidance on the operation of the DPA and UK GDPR which can be found on its website.

In England, the National Data Guardian for Health and Social Care is a statutory role established to advise and challenge the health and care system to help ensure that an individual's confidential patient information is safeguarded securely and used properly.

The previous National Data Guardian, Dame Fiona Caldicott, also established the Caldicott Principles which inform the use of confidential patient information in the health and care system. These principles are:

- justify the purpose(s) for using confidential information
- don't use patient identifiable information unless it is necessary
- use the minimum necessary patient-identifiable information
- access to patient identifiable information should be on a strict need-to-know basis
- everyone with access to patient identifiable information should be aware of their responsibilities
- understand and comply with the law

- the duty to share information can be as important as the duty to protect patient confidentiality

All NHS organisations and local authorities that provide social services in England must have a Caldicott Guardian to uphold these principles and protect the confidentiality of people's health and care information, making sure it is used properly.

All four nations have chosen to have Caldicott Guardians. These are represented by the UK Caldicott Guardian Council, which is a sub-group of the National Data Guardian's Panel.