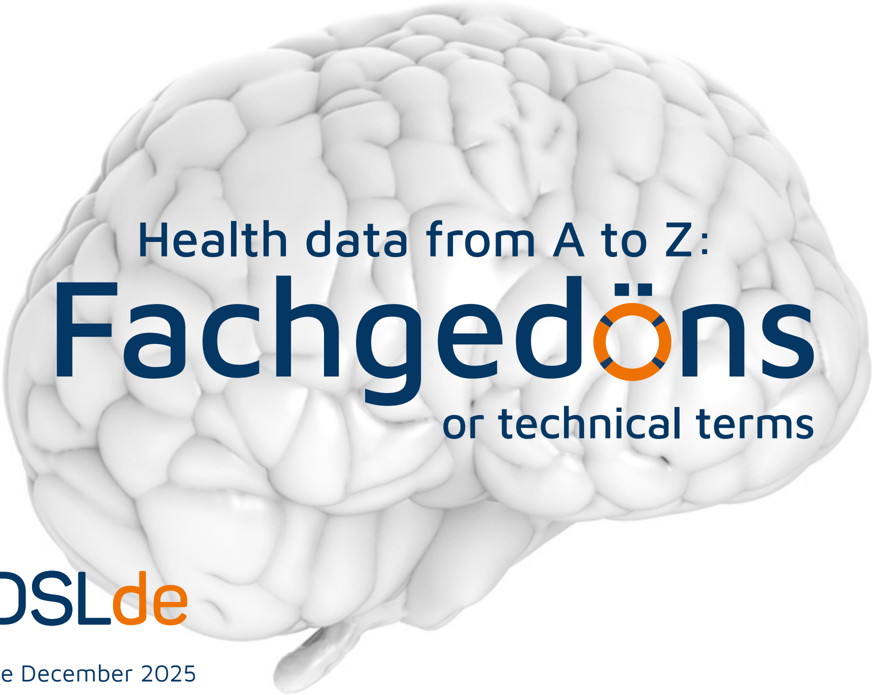


Health data from A to Z:
Fachgedöns
or technical terms

#DSLde

Update December 2025

Technical terms explained in an understandable way – for everyone

Digitalisation in healthcare has picked up speed considerably – and with it, the flood of technical terms. Being able to navigate healthcare and digital terminology is essential if patients, citizens and professionals want to talk together about data, security and benefits. This is exactly where DSL DE Fachgedöns comes in: making terms understandable, helping to classify them and encouraging people to ask questions. Because terms such as ‘data governance’, ‘data solidarity’ or ‘health data labelling’ are not dry buzzwords **– they influence how we shape health, care and self-determination today – and they can be understood.**

DSL DE Fachgedöns is based on the Data Saves Lives Europe glossary and has been further developed by us. It draws on content from international sources such as the WHO, the OECD, the European Commission, the Federal Ministry of Health, as well as existing glossaries, programmes and international standards. The terms are regularly reviewed, revised and supplemented. Our aim is clear: **comprehensibility, transparency and timeliness – on an equal footing.** **Data Saves Lives Germany** is a non-profit, patient-driven initiative. We provide **independent, neutral and free** information about health data and digitalisation. The project is funded by the **Bosch Health Campus. Patients have been closely involved from the outset.** Thank you to everyone who contributed their ideas.

Warm regards, Birgit Bauer and the DSL DE team

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Access control:

A measure that ensures that **only authorized persons have access** to all or part of a data set.

Aggregated data:

Aggregated data is created when **information from several individuals is summarized** to determine general trends or averages. This data provides insights into the behaviour or health status of a group without individual persons being identifiable. Such data is useful for gaining insights into the progression of a disease or the effectiveness of treatments without compromising the privacy of individuals.

Algorithm:

An algorithm is a **fixed sequence of steps that a computer executes to solve a problem.** Algorithms follow a precise logic and can be applied in a variety of ways, whether it be for calculation, sorting or recognizing patterns in data. An example from everyday life is the algorithm that determines the order of posts shown on social media, or the one used in medicine for evaluating X-ray images.

Anonymization:

Anonymization is the process of **modifying personal data in such a way that it cannot be traced back to an identifiable person.** This technique is used to protect privacy while still being able to use the data for statistical or scientific purposes.

Example: In an anonymized patient survey, all personal information is removed or encrypted so that no identification is possible.

Anonymized data:

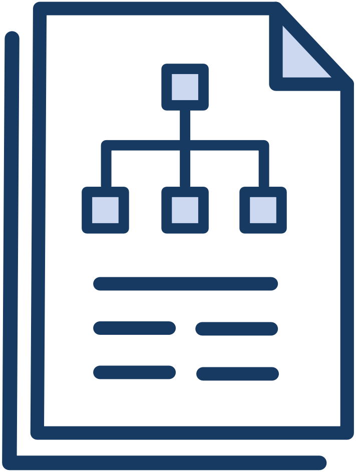
Anonymized data is **information that has been processed by modification in such a way that it is no longer possible to draw any conclusions about the person whose data was originally collected.** Anonymization involves removing names and addresses, for example, or replacing them with codes so that the person behind the data can no longer be identified. This data is important for research because it allows for secure analysis without violating the protection of the persons concerned.

Artificial intelligence (AI):

This term refers to **systems developed by humans that operate in the physical or digital world when given complex tasks.** AI perceives its environment, interprets structured and unstructured data and, based on the knowledge gained, makes decisions according to defined parameters. In medicine, AI is used to analyze medical data and support diagnostic or therapeutic decisions, for example in radiological images. It helps to identify patterns and relationships in large data sets, which improves the accuracy of diagnoses. Furthermore, AI plays an important role in personalized medicine, drug development and health data management.

Audit trail or audit log:

A record of all the people who have viewed or modified a data set. It notes why and when this view or change has occurred and what changes have been made.



Authentication:

Authentication is a process to ensure that the person or device requesting access to a system is actually authorized to do so. A common example is logging in to a smartphone using fingerprint or facial recognition. In this case, the device checks whether the captured biometric data matches the stored information before granting access. **Authentication protects against unauthorized access to personal data and applications.**

Bias:

Bias (pronounced "bees") means a **distortion or unequal treatment in data or decisions.** This can happen when a computer programme or study does not treat all people equally.

Example: If an AI system is only trained with data from men, it may deliver poorer results for women. In healthcare, it is important to **recognise and avoid** such distortions – so that technology treats everyone fairly.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Big Data:

Big Data refers to the analysis and processing of very large and complex amounts of data that are difficult to handle using conventional methods. In the healthcare sector, for example, extensive patient data from surveys or so-called patient-reported outcome (PRO) questionnaires are evaluated in order to gain important insights into the quality and methods of treatment. These analyses help to identify patterns, improve the effectiveness of therapies and optimize patient care overall.

Big data makes it possible to develop individualized treatment approaches and to better address the needs of patients.

Blockchain:

A blockchain is a secure way of storing information. It works like a digital notebook in which each new piece of information, such as test results, is stored in a block. These blocks are linked together and form a chain. **Since the blockchain is decentralized, no one has sole control over the data, which improves data protection. The information is encrypted and stored on many computers so that it cannot be changed.** Both doctors and patients have secure access to the data, which is transparent and immutable.

Carer:

A person who provides unpaid care to patients or users, usually relatives or friends.

Clinical audit:

A method for improving practice, patient care or services provided. A clinical audit involves reviewing current practice against standards or criteria, identifying areas for improvement and making changes to practice accordingly. A further audit is then carried out to ensure that improvements have been made.

Purposes:

- **Improving patient care**
- **Identifying areas for improvement**
- **Ensuring the effectiveness of changes**

Clinical trial:

A clinical trial is a scientific investigation in which human subjects participate. The purpose of these studies is to test the effect of health interventions, including drugs, diagnostics, medical devices and treatment protocols.

Purposes:

- **Safety**: to collect data on the safety of the interventions.
- **Effectiveness**: to verify the effectiveness of the interventions.

Significance:

Clinical trials are critical to ensuring that new treatments and products are safe and effective before they are used in regular health care.

Cloud computing:

Cloud computing refers to the **storage, processing and use of data on external servers that can be accessed via the internet.** Instead of storing data locally on one‘s own computer or in one‘s own database, users can store it in the ‘cloud’. This allows access to data and applications from different devices, no matter where you are. Cloud services often offer additional benefits such as flexibility, scalability and cost-efficient use of resources, which is particularly useful in healthcare for managing patient data or exchanging information between professionals.

Consent:

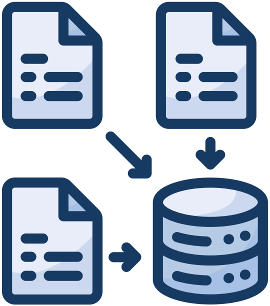
See explicit consent.

Confidentiality:

Means that information is not made available or disclosed to unauthorised persons or companies.

Database:

A database is a **structured system for storing data on a computer.** It allows for easy retrieval and analysis of information, making the search and processing of data more efficient. Databases are usually designed for specific applications, such as managing patient data.



Data breach:

A data breach occurs **when the provisions of the General Data Protection Regulation (GDPR) are violated.** These include illegal disclosures or misuse of personal data that may result in inappropriate intrusion into an individual's privacy. Examples include theft of data or unauthorized access to personal information.

Data controller:
The data controller is the person or organisation that determines why and how personal data is processed. It is the responsibility of this **person to ensure that all data processing is based on a legal basis and complies with data protection regulations.**

A B C **D** E F G H I L M N O P R S T

Data governance:

Data governance describes how data is handled responsibly.
It involves clear rules, responsibilities and quality standards to ensure that health data is used securely, correctly and fairly.
This includes, for example, who is allowed to access which data, how it is protected and how it is stored.
The aim is to build trust and ensure that data is used for the benefit of patients.

Data linkage:

Data linkage is a method by which data from **different sources is collected and analyzed.** Often, this involves information about a person, that is combined from different data sets to get a more comprehensive picture or to recognize patterns.

Data literacy:

Data literacy means **understanding data and being able to use it responsibly.**
People with a high level of data literacy know, for example, which health apps are trustworthy or what happens to their data when they give their consent. Data literacy helps patients make informed decisions – for example, about whether and how they want to share health data. It strengthens personal responsibility and protects against misunderstandings.

Data processor:

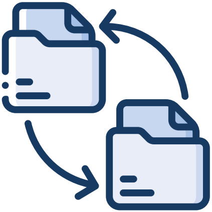
A data processor is **a person or organisation that processes personal data on behalf of the data controller, but is not an employee of the data controller.** The data controller must ensure that these processors are carefully selected and have a written agreement that clearly regulates the data processing requirements.

Data security:

Data security refers to measures taken **to protect data and information systems** from unauthorized access, misuse, disclosure, interruption, modification or deletion. This is particularly important in the healthcare sector, where confidential patient data is stored.

Data sharing:

Data sharing refers to the disclosure of data between different organisations or within an organisation. This can include the sharing of patient data between doctors` offices or clinics, or the sharing of data between different departments within an institution. The aim is **to promote collaboration and improve the flow of information in order to optimize healthcare.**



Data solidarity:

Data solidarity means **sharing health data for the benefit of all,** provided this is done securely and responsibly. The idea behind this is that if many people make their data available – anonymised, for example – for research or health projects, **this can lead to insights that benefit everyone.**

Data solidarity does not mean releasing data in an uncontrolled manner, but rather making a conscious and informed decision to help others by donating your own data. It combines data protection with social benefits.

Data steward:

A data steward is a **person who ensures that data is managed correctly, completely and securely.**
In healthcare, they ensure that health data is correctly anonymised, up to date and traceable.
They know the origin of the data, check its quality and ensure that it is handled in accordance with the FAIR principles.
In short, **data stewards are the guardians of data quality.**

Data subject:

A data subject is **a known or identifiable person whose personal data is being processed.** This means that information about this person, such as their name, address or health data, may be stored and used.

Deep learning:

Deep learning is an advanced machine learning technique that allows computers to recognize complex patterns in data. **It involves using multiple layers of a neural network, which allows the machine to learn independently how input data is associated with output.** This technique is used in areas such as image and speech recognition.

De-identification:

De-identification is the process of editing personal data in such a way that the link to a specific person is broken. This means that **all information that could reveal a person`s identity is removed or deleted.** This ensures that the person can no longer be re-identified, even if the data remains.

De-identified data:

This is data that cannot be used to identify a person because the identifiers have been deleted or encrypted. However, it is still an individual's data, so it still needs to be protected. In theory, it would be possible to identify the person via the data if it is not sufficiently protected, e. g., if it is combined with data from other sources.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Digital Act (DigiG – German Digital Gesetz):

The Digital Act, also known as the Act **to Accelerate the Digitization of the Healthcare System**, is intended to make everyday life in the healthcare system easier for doctors and patients. A central component of the law is the introduction of the electronic patient file (ePA), which will become mandatory from January 2025.
The ePA promotes the exchange and use of health data so that findings can be shared more easily and duplicate examinations can be avoided. This leads to faster diagnoses and well-founded therapy decisions.

Digital health applications (DiGA):

Digital health applications are apps or software solutions that can be prescribed by doctors, similar to a prescription. **These applications, which are used to treat diseases such as multiple sclerosis, insomnia or depression**, can be used on smartphones or computers. The Federal Institute for Drugs and Medical Devices (BfArM) approves DiGA so that they can be prescribed by doctors.
Further information and an overview of the approved applications are available on the BfArM website.

Digital health literacy:

Digital health literacy means **finding, understanding and correctly assessing health information on the internet.** It helps patients distinguish reputable offers from questionable ones – for example, in health apps, online forums or AI-supported symptom checkers. Those who have digital health literacy can navigate the digital health world more confidently, make informed decisions and actively participate in their own health management.

In short, **it strengthens self-determination and trust in digital services.**

Digital twin:

A digital twin is a virtual representation of a real person, organ or device. **It shows in digital form how the body or certain processes might behave.**

In medicine, a digital twin can help to plan treatments or test therapies – without any risk to patients. For example, it can be used to see how a heart would react to a new medication. This makes medicine more personalised and safer.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Digitalisation and digitization:

In healthcare, digitization refers to the comprehensive **process of converting analogue information into digital formats in order to improve the efficiency and quality of healthcare.**

Digitization is a sub-aspect of digitalisation and refers specifically to the conversion of analogue data into digital formats. Examples include the transfer of paper documents into electronic files or the digitization of medical images.

In short: digitalisation is the general process, while digitization describes the specific conversion of analogue data into digital data.

Edge computing:

Edge computing means that **data is processed directly where it is generated** – i.e. at the edge of the network.

For example, a smartwatch can evaluate your pulse or sleep patterns on the device itself without first sending the data to a remote server.

This saves time, conserves internet bandwidth and protects privacy. In healthcare, this is particularly useful in emergencies, telemedicine or wearables that constantly collect data.

Electronic Health Card (eGK):

The electronic health card (eGK) was introduced as part of the 2004 health reform and has been the only valid health card in Germany since 2015. It contains a personal identification number (PIN) that is required for the electronic patient file (ePA). It is important to keep this PIN; if it is lost, you should contact the health insurance company immediately to take the necessary steps. **The eGK enables e-prescriptions to be redeemed in three different ways:** by **scanning the card** at a reader in the pharmacy, via the **E-Rezept App** or by using a **printed QR code.** The eGK has an integrated NFC chip that enables data to be exchanged between the card and the reading device. This chip is also used when transferring data from an old smartphone to a new one, for example.

Electronic patient file (ePA):

The electronic patient file (ePA) has been available to everyone insured under the statutory health insurance (GKV) since 1 January 2021. From 15 January 2025, the ePA will be gradually rolled out to everyone with statutory insurance. It is available as an app from the health insurance company and will in future contain all of a person`s important health data and help them to receive better care.

All data is, so to speak, in one place and can be shared by people (patients) with doctors or therapists. This means that patients can, for example, receive a diagnosis or therapy recommendation more quickly.

Encryption:

A process that protects the integrity and confidentiality of data by **using an algorithm to create a secret code from plain data.** The reverse process, decryption, restores the original data. Only authorized users with a key can decrypt encrypted data. Encryption is an effective method of preventing IT misuse, identity theft and the unauthorized disclosure of confidential information, and ensures cyber security, data protection and privacy.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

European Health Data Space (EHDS):

The European Health Data Space (EHDS) is a **European Union initiative** adopted in 2024. **It promotes the electronic transfer of health data between different countries and health service providers.**

The main goal is to create a common data space that enables seamless cross-border healthcare. This will make it easier for patients to access medical information and receive appropriate medical care when they need it, even when they are abroad.

Explainable AI:

Explainable AI is a form of **artificial intelligence that makes its decisions comprehensible.** For example, when an AI suggests a diagnosis, it can also show which data and clues it used to arrive at that conclusion.

This is important so that doctors, researchers and patients understand why a result was reached. Explainable AI ensures greater trust, transparency and security.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

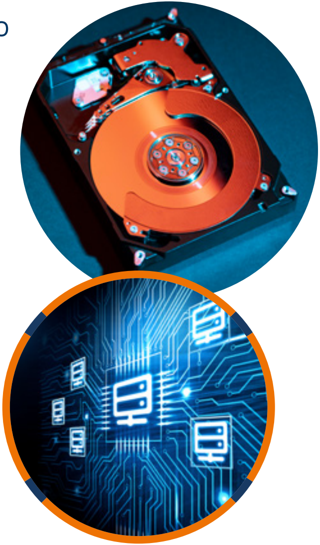
FAIR data:

FAIR data refers to the principles developed to improve the description, storage and publication of scientific and administrative data.

The term 'FAIR' stands for:

- **Findable**: data should be easy to find.
- **Accessible**: Data should be accessible to authorized users.
- **Interoperable**: Data should be compatible with other systems to facilitate sharing.
- **Reusable**: Data should be provided in a way that allows others to use it for new purposes.

These principles promote the effective use and sharing of data in research and government.



Federated learning:

Federated learning is a **machine learning method that does not require data to be shared.** Instead of centralising data, computer programmes learn directly where it is generated – for example, in hospitals.
Only the results of the learning, i.e. the new findings, are shared. This allows many institutions to train AI together without passing on patient data. This protects privacy while still promoting medical progress.

General Data Protection Regulation (GDPR):

The General Data Protection Regulation (GDPR) is a comprehensive regulation of the European Union that governs data protection. It concerns the **processing of personal data by companies, organisations and public authorities within the EU.**

Aims of the GDPR:

- **Strengthening and standardizing** the right to data protection for all individuals within the EU.
- **Creating a uniform level** of data protection in all EU member states.
- **Ensuring the free movement** of data within the European single market.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Generative AI (Generative artificial intelligence):

Generative AI or generative artificial intelligence (generative AI) is a special type of AI that is able **to generate new content using existing data.** This includes, for example, texts, images or music. This technology analyses patterns in the data and uses them to create original and creative results. Generative AI is used in many fields, from art to medical research.

Generative AI in healthcare:

Examples of use:

- **Medical reports**: Creation of reports based on patient data.
- **Image analysis**: Support for diagnosis by analyzing X-rays.
- **AI-powered chatbots**: Apps like Ada Health help to decide whether a visit to the doctor is necessary.
- **Early detection**: Identification of health risks through wearables and health apps.
- **Comprehensible information**: Provision of clear information about illnesses and treatment options.
- **Personalized therapies**: Adaptation of therapy suggestions to individual needs.
- **Robotic surgery**: da Vinci robot performs more precise procedures.
- **Imaging**: AI detects abnormalities in mammograms.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Risks:

- **Diagnostic deficiencies**: possibility of errors if AI is not sufficiently trained.
- **Ethical concerns**: the use of AI raises important ethical questions.

The development of generative AI in healthcare is promising, but requires careful research and monitoring.

Genome sequencing:

Genome sequencing is a process in which the **entire DNA of an organism**, such as a human, is analyzed. The aim of this analysis is to determine the exact sequence of the genetic building blocks (nucleotides). This can provide important information about genes and their functions. Genome sequencing is constantly being developed and it is expected that its scope will become even more diverse in the future.

Areas of application for genome sequencing:

- **Research into diseases**: to identify genetic causes of diseases.
- **Development of personalized therapies**: treatments tailored to the genetic characteristics of a patient.
- **Prevention and health care**: early detection of risks for certain diseases.
- **Areas of application**: Today, genome sequencing is used in oncology (cancer), in the diagnosis of rare diseases and in genetic counselling for families with genetic diseases, among other things.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Health app:

A health app is **a programme on a smartphone or tablet that helps users monitor and improve their health or stay in touch with doctors.**
Some apps remind you to take your medication, measure your steps or pulse, while others can also assess symptoms or accompany therapies. Some apps – known as DiGA – can even be prescribed and are therefore considered part of medical care.
It is important that health apps are trustworthy and comply with data protection rules.

Health data:

Health data includes various types of information that play a role in healthcare:

- **Clinical data**: Information that comes directly from patient care, also known as primary health data.
- **Administrative data**: Administrative information collected by healthcare organisations, such as billing and appointment management.
- **Behavioral data**: Data relating to a person‘s lifestyle and behavior, such as eating habits or exercise behavior.
- **Genomic data**: Information about a person‘s genetic makeup that allows conclusions to be drawn about health risks and characteristics.
- **Environmental and social data**: factors related to living conditions, such as housing and socioeconomic status.

- **Research data**: data collected from clinical studies and scientific research to gain medical insights.
- **Patient-reported data (PROs)**: Information provided directly by patients about their health, e.g., about symptoms or well-being.
- **Emergency data**: Information that is helpful in an emergency to ensure proper treatment. This data is often stored in an app on a smartphone and can include important information such as allergies or chronic conditions.

Health Data Quality Labelling:

Health data quality labelling means **attaching standardised “labels” to health data** so that it is immediately clear what the data is, how sensitive it is and under what conditions it may be used.

It is a central component of the European Health Data Space (EHDS) because such labels make data findable, understandable and trustworthy and enable its legally compliant secondary use.

Note: The EU-funded QUANTUM project is developing a quality label for health data that harmonises these requirements and makes them transparent.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

A B C D E F G H I L M N O P R S T

Health Data Usage Act (GNDG):

The Health Data Usage Act (GDNG) is a new law that regulates the handling of health data in Germany. **It defines how health data may be used to protect the personal health information of citizens.** Doctors and researchers can only use the data under strict rules. One example of how health data is used is in medical research. These data help us to learn more about diseases, improve therapies, accelerate diagnostic procedures and make the healthcare system as a whole more efficient. Health data are also important for preventive measures.

Health literacy:

Health literacy describes **a person‘s ability to obtain information about their health, make informed decisions and apply this knowledge in their daily lives.** It is important for actively managing one‘s own life, especially when living with an illness, and for improving quality of life.

The World Health Organization (WHO) refers to this concept as ‘health literacy’. The WHO emphasizes that people should acquire the skills to ask questions and actively participate in conversations about their health. A high level of health literacy enables people to better understand and manage their health.

Identifiable data:

See ‘personal data’.

Identifier:

An identifier is a piece of data that can be used, either alone or in combination with other identifiers, to identify a person.

Examples:

- **Single identifier:** A social security number can serve as an identifier because it is uniquely assigned to one person.
- **Combination:** The combination of first name, last name and date of birth can also be an identifier used to identify a person.

Identifiers are particularly important in healthcare to ensure that patient data is managed accurately and securely.

Implied consent:

An implicit agreement between patients and medical or social personnel that allows **the collection, processing and sharing of patient data for medical and care purposes.** This is done on the assumption that the data will be treated confidentially and that patients have not objected.

Indirect care:

Indirect care includes all services that are not provided directly to the patient. These include activities that support the general provision of health services to the population or to specific patient groups.

Examples of indirect care:

- **Health service administration**: organisation and management of health services.

- **Preventive medicine**: measures to prevent disease.
- **Medical research**: studies to improve diagnoses and treatments.
- **Risk prediction and stratification**: assessment of health risks and classification of patient groups.
- **Performance evaluation**: analysis of the quality and effectiveness of health services.
- **Needs assessment and financial audit**: Determining health needs and auditing financial resources.

These services contribute significantly to improving healthcare and promoting public health.

Interoperability:

Interoperability refers to the ability of different **IT systems, devices or applications to communicate with each other** and exchange data.

Significance in healthcare: In the healthcare sector, interoperability enables systems such as the computers in a hospital or the software in a doctor`s office to exchange information about patients or patient groups and use it in different processes. This is crucial to **ensure a smooth flow of information.**

Example: When different systems in the hospital can communicate with each other, data about a patient is shared quickly and efficiently. This reduces the need to repeat tests or fill out questionnaires for multiple times.

Result: faster information and better, more efficient medical care.

Interoperability standard:
An interoperability standard is a **common language for computer systems.** It ensures that different programmes in the healthcare sector – for example, software in practices, hospitals or health insurance companies – can exchange data correctly with each other. A well-known example is HL7 FHIR, an international standard for the secure exchange of medical information. **This ensures that health data arrives where it is needed in a complete, understandable and secure form.**

Linking:

The merging of information and data from two or more sources to combine information about a person or event that is not available in a single record.

Machine learning:

Machine learning is a subfield of artificial intelligence (AI) **in which computers learn from data and experience rather than being controlled by direct programming.** Based on the data with which they are trained, these systems continuously improve. Applications of machine learning can be found in everyday life, e.g., in spam detection for e-mails or in language assistants such as Alexa and Siri, which are becoming more and more precise through user interaction. In medicine, machine learning supports, for example, the analysis of radiological images and contributes to the diagnostic process.

Medical devices:

Medical devices are **objects or materials that are used to diagnose, monitor, treat or alleviate illnesses and have a physical effect** without triggering pharmacological or metabolic processes (how drugs or chemicals work in the body and how the body breaks them down or uses them). Examples include infusion cannulas, pacemakers, wheelchairs and X-ray machines. They support medical treatment and are regulated in Germany by the Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM / Federal Institute for Drugs and Medical Devices).

Medical gaslighting:

Medical gaslighting refers to **the devaluation or trivialization of symptoms by medical personnel**, so that patients are not taken seriously or their complaints are classified as psychosomatic (how the mind and emotions can cause physical symptoms in the body). People whose illnesses are rare, difficult to diagnose or not well researched are often affected. Certain groups, such as women or overweight people, also experience this phenomenon more often than average. The consequences are a lack of or delayed treatment, which often means that those affected have to fight for recognition and adequate medical care. A study by the Free University of Berlin (2022) describes this phenomenon and its effects in detail.

Medicinal products:

Medicinal products, such as tablets, creams, syrups or injections, are used **to cure, alleviate or prevent diseases.** They work in the body by influencing how medicines work, how the immune system responds, or how the body uses or breaks down substances. Unlike medical devices, which work physically (e.g., bandages or infusion needles), drugs directly intervene in the body`s biological processes. In Germany, the Federal Institute for Drugs and Medical Devices (BfArM) is responsible for the authorization and monitoring of medicinal products, ensuring the safety and efficacy of the preparations.

Meta Data Catalogue:

A meta data catalogue is something like a **table of contents for health data.** It describes which data sets exist, where they are located, who uses them and for what purpose.
This helps researchers find data instead of collecting it again and ensures that health data can be better understood and used fairly.
This makes research faster, more transparent and more efficient.
Sounds a bit dry? Yes, sometimes it does – but without metadata there is no overview, and without an overview there is no good data usage.

Mobile Health (mHealth):

Mobile health encompasses the **use of mobile devices such as smartphones and smartwatches to collect, monitor and provide health data.** Apps and sensors allow users to record health parameters such as heart rate, activity level or sleep quality and share this data with health-care professionals or use it for their own health care.

Network security/ cyber security:

Cyber security encompasses **measures and processes for protecting digital data and systems from theft, attacks or unauthorized access.** The aim is to safeguard sensitive information from threats such as hacking, malware or data leaks and to ensure the integrity, confidentiality and availability of data.

NFC chip (Near Field Communication):

This little chip is found in smartphones, for example, and is activated when we transfer data from the old device to the new one. You can also find the NFC chip in reading devices and on bank cards that we use to pay. This chip is also in the electronic health card. **It ensures that the communication works when patients want to use the health card to get an e-prescription at the pharmacy by swiping it over the reader.** So, it‵s the mediator that helps you get the right medication.

NLP (Natural Language Processing):

NLP is a branch of artificial intelligence that **deals with the processing and analysis of natural language.** NLP converts clinical records and patient reports into structured data. For example, it can transform free-text notes written by doctors into organized information. This technology makes it possible to extract unstructured information from medical documents, enabling better analysis and use of health data.

Non-disclosure:

Means that information is not made available or disclosed to unauthorized persons or companies.

Opt-in:

To register for something. In 2024, the opt-in procedure was introduced for organ donation. People who wish to donate their organs can register on a special website.

Opt-out:

An opt-out is the option **to object to a measure.** For example, before the introduction of the electronic patient file (ePA) in January 2025, there is the option to refuse the ePA. This means that the statutory health insurance company will not create an ePA for the person in question.

Patient portal:

A patient portal is a **digital platform where you can view and manage your own health information.** It contains, for example, findings, doctor’s letters, vaccinations or laboratory values. The portal is often linked to the electronic patient record (ePA).

Patient portals empower individuals to take responsibility for their own health because they can decide for themselves who can see which data – and when. This makes cooperation with doctors easier and more transparent.

Patient data:

Data collected by patients when they see a doctor or use social services. This includes **information on physical or mental health**, such as height, weight, allergies, social care needs, social or care services used, and details of next of kin.

A
B
C
D
E
F
G
H
I
L
M
N
O
P
R
S
T

Personal data:

This term refers to **personal information about identifiable individuals that must be protected and may only be used for approved, legally permissible purposes.**

According to the General Data Protection Regulation (GDPR), this is any information relating to a living individual who can be identified, either on the basis of this data or by combining it with other data held or likely to be held by the data controller.

Personalized medicine:

Personalized medicine means that the **treatment or care of a patient is tailored to their individual needs and characteristics.** Genetic characteristics, lifestyle, environmental factors and personal health data are taken into account in order to find the best possible therapy and prevention. One example of an application in oncology is the use of genetic testing to identify tumors and develop personalized treatment plans.

Primary Care:

This term refers to services provided by organisations such as family practices, dental practices, community pharmacies and opticians.

Primary health data:

Primary health data is **information collected directly from patients or doctors during a visit or conversation. It comes directly from patients and is documented in the patient file.** This data is the basis for immediate medical care, such as diagnoses or therapy recommendations.

Examples:

- Clinical Fundings
- Laboratory results
- X-ray findings
- Information generated during patient care, such as experiences and symptoms

PRO – Patient Reported Outcome:

Patient-reported outcome (PRO) refers to the **assessment of health conditions, symptoms or treatment effects from the patients` own perspective.** This method allows patients to report their own experiences and assessments of their health and quality of life. PRO collects important information to improve patient care and treatment.

PROMs – Patient-Reported Outcome Measurements:

Patient-reported outcome measurements (PROMs) are **standardized questionnaires used to measure patient-reported health outcomes.** While they used to be developed mostly by experts, patients are now also involved in order to make the questionnaires practical. PROMs capture the patient`s perspective on symptoms, functional limitations, quality of life, and satisfaction with treatment, and provide important information for evaluating the effectiveness of interventions and improving individual patient care.

Pseudonym:

A unique identifier that does not reveal a person`s true identity but is used to distinguish different people in a data set. This identifier can sometimes be generated by encrypting the actual identity.

Pseudonymized data:

The distinction of persons in a data set by means of a unique identifier that does not reveal their true identity. This is related to the anonymization of data.

Public interest:

Matters or subjects 'of public interest' **serve the interests of society as a whole.** The 'public interest test' is used to determine the extent to which the benefits of disclosing personal patient data are greater and more important than the personal interest of the individual and the public's trust in the confidentiality of the services.

RWD – Real World Data:

Real-world data (RWD) is generated daily when **patients collect data about their illnesses, symptoms and the tolerability of medications in their everyday lives.** This data, which is not collected in clinical studies, can be structured and analyzed to provide important insights that help improve treatments, promote research or change habits and rituals to improve the quality of life of people with illnesses. **Real world data forms the basis for real world evidence.**

RWE – Real World Evidence:

Real world evidence refers to data and information from patients` everyday lives that does not come from clinical studies. When patients share their experiences with medications, important insights into their effectiveness and benefits can be gained. This information helps to better understand and improve medications in real life.

Secondary care:

Medical care provided by specialists, either on an outpatient basis by specialists in private practice or on an inpatient basis in a hospital.

Secondary health data:

Information derived from primary health data that is not used directly for patient care. It supports research purposes, health analyses and policy developments. Examples include patient registries, databases for clinical research, health statistics and reports on healthcare expenditure.

Sensitive personal data:

Data that can identify a living person. This includes information such as ethnicity, political and religious views, membership of trade unions, health status, sexual preferences, and (criminal) legal proceedings or accusations.

Subject/Study participant:

Any person who participates in a research study, whether or not it is a clinical trial. The term refers to both patients and healthy volunteers, but not to medical professionals.

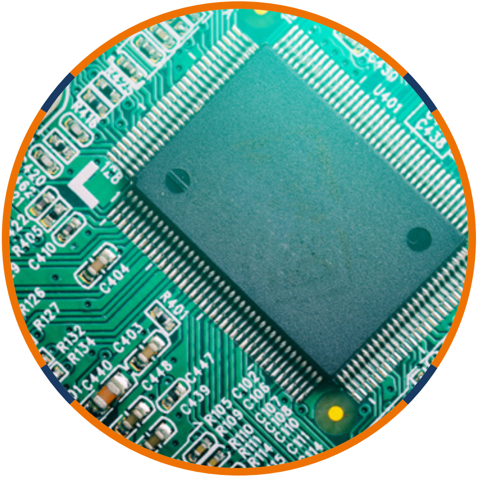
Synthetic comparison group:

A synthetic comparison group consists of **artificially generated data sets that resemble real patient data.** They are used to compare treatment outcomes – especially when there is little real data available on a disease.

This allows researchers to **test whether a drug is effective without exposing additional patients to a new treatment.** This saves time, reduces risks and expands knowledge about rare diseases.

Synthetic data:

Artificially created data that is not based on actual events. It is generated by algorithms and used as a substitute for test data sets to verify mathematical models and, increasingly, to train machine learning models.



Telemedicine:

Telemedicine means **offering medical advice or treatment via digital channels** – in other words, without having to visit the doctor’s surgery in person. This can take the form of a video consultation with a doctor, a digital prescription service or remote monitoring of vital signs. Telemedicine saves time, facilitates access to specialists and is particularly helpful for people with limited mobility or those living in rural areas.

Important: The same data protection and quality standards apply here as in a local doctor’s surgery.

Is there a term missing from the collection that should definitely be included?

We are always working on expanding and completing our collection.
We welcome additions, comments or questions by email to:
DSL.DE@edha.academy

European Digital Health Academy edha gGmbH
Mohnblumenweg 1
93326 Abensberg

Commercial register: HRB 19050
Register court: Amtsgericht Regensburg

Represented by: Birgit Bauer

E-Mail: DSL.DE@edha.academy

Sales tax ID: DE 349 725 486

With the kind support of Boehringer
Ingelheim International GmbH,
Ingelheim am Rhein