educage.
info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Processing of Health Data
GDPR, UK GDPR and Related Legal Frameworks

1. Introduction

Health data represents one of the most strictly regulated categories of personal data in modern data protection law. Its processing touches upon the most intimate sphere of the individuals concerned: illnesses, genetic characteristics, mental health, treatment history – all information whose misuse may cause serious harm to the individual, whether through discrimination, insurance exclusion, or employment consequences[1].
With the advance of digitalisation - from electronic health records through telemedicine to AI-based diagnostics - the volume and complexity of health data processing has increased dramatically. This presents heightened legal risk for data controllers, while the need to enforce data subject rights is also growing[4].
This study reviews the most important legal frameworks governing the processing of health data: the General Data Protection Regulation of the European Union (GDPR),
the United Kingdom's independent data protection regime (UK GDPR and DPA 2018), and related sectoral and technological regulations.
The aim is to provide a comprehensive compliance picture that is equally useful for healthcare institutions, technology service providers, and data protection professionals.

2. Legal Definition and Classification of Health Data

Article 9 of the GDPR classifies health data as a special category of personal data and, as a general rule, prohibits its processing. According to the Regulation's definition, health data means any personal data relating to the physical or mental health of a natural person, including data concerning the provision of health services, which reveal information about that person's state of health[1].
The concept is to be interpreted very broadly. It includes diagnoses, prescriptions, laboratory results, hospital admissions, medical imaging, and therapeutic records. However, grey areas also exist: data on pulse or sleep collected by wearable devices, nutritional diaries, or data from general wellbeing applications do not always qualify as health data on their own the classification depends on the purpose and context of data collection. According to EDPB guidance, the principle of purpose limitation and the context of processing must be examined[1,4].
Related concepts: genetic data (DNA analyses, hereditary conditions), which also constitute a special category, and biometric data, insofar as they are capable of uniquely identifying natural persons (e.g. facial or fingerprint-based hospital identification). All three data types are subject to the same strict protection rules[1].

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

3. The EU General Data Protection Regulation (GDPR)

Prohibition of Processing and Exceptions:
Article 9(1) of the GDPR generally prohibits the processing of health data. However, paragraph (2) exhaustively lists the exceptions under which processing may be carried out lawfully. The exceptions particularly relevant in the health sector are[1]:

- Explicit consent of the data subject (point (a)): a legal basis particularly applied in research and mobile health applications; however, due to its revocability, it cannot be considered a stable basis for long-term health data processing[1,10].
- Healthcare and treatment (point (h)): the most commonly applied exception in clinical contexts; it requires that the processing be carried out or supervised by a health professional bound by a duty of confidentiality[1].
- Public interest in the area of public health (point (i)): the basis for epidemiological surveillance and vaccination registries[1].
- Scientific research and statistics (point (j)): pursuant to EDPB Guidelines 5/2019, the application of anonymisation or pseudonymisation is a necessary condition where the original consent did not extend to the research purpose[1].

Principles of Processing:
Under Article 5, all health data processing must comply with the following principles: lawfulness, fairness, and transparency; purpose limitation (data may only be collected for specified, explicit, and legitimate purposes); data minimisation (only necessary data may be processed); accuracy; storage limitation; and integrity and confidentiality. The latter carries particular weight in the health sector, where hospital systems are regularly targeted by cyber attacks[1].

Data Protection by Design and by Default (Article 25):
The principle of privacy by design and by default is a mandatory consideration when designing healthcare IT systems. This means that data protection aspects must be built in at an early stage of system design, and only the necessary data may be processed by default. This principle is particularly relevant in the development of hospital information systems, patient portals, and telemedicine platforms[1].

Data Protection Impact Assessment
The processing of health data, particularly in large-scale, automated, or especially sensitive cases, generally requires a DPIA to be carried out. The assessment must include an evaluation of the necessity and proportionality of the processing, identification of risks, and a description

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

of risk-mitigating measures. If the DPIA identifies a high risk, prior consultation with the supervisory authority is mandatory (Article 36)[1].

Data Protection Officer:
Organisations processing health data (hospitals, laboratories, insurers, and pharmaceutical companies) are obliged to appoint a Data Protection Officer. The DPO's role is to monitor processing activities, train staff, and liaise with the supervisory authority. The role may be outsourced, but the obligation cannot be waived[1].

Personal Data Breaches (Articles 33–34):
A security incident involving health data must be reported to the supervisory authority within 72 hours if it is likely to result in a risk to the rights and freedoms of data subjects. If the incident is likely to result in a high risk (which is almost invariably the case with health data) the data subjects must also be notified without undue delay, unless the data were protected by strong encryption[1].

4. UK GDPR and the Data Protection Act 2018

As a result of Brexit, the United Kingdom has applied an independent data protection regime since 1 January 2021. The UK GDPR essentially transposes the content of the EU GDPR into UK law; however, it contains a number of divergences and must be read in conjunction with the supplementary provisions of the DPA 2018[2].

Key Differences from EU GDPR

- Supervisory authority: the ICO (Information Commissioner's Office) carries out supervisory functions. The ICO issues its own guidance, which in some cases regulates the health sector in greater detail than EDPB recommendations[2,8].
- DPA 2018: the Schedule to the Act specifies the exceptions and conditions applicable to the processing of health data, including processing for healthcare or social care purposes, for which it is sufficient that the controller operates under an appropriate duty of confidentiality[3].
- Common Law Duty of Confidentiality: beyond the GDPR, health professionals are subject to a case-law-based duty of confidentiality. This constitutes an independent legal obligation, the breach of which may give rise to a civil claim even where GDPR compliance is otherwise maintained. (Campbell v MGN Ltd [2004] UKHL 22; NHS Confidentiality Code of Practice)
- UK adequacy: in 2021, the EU recognised the UK's data protection adequacy, enabling the free flow of data between the EU and the UK. However, this status is not permanently guaranteed and may be subject to review if UK law diverges

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

significantly from EU standards. (EU Commission Implementing Decision 2021/1772)

NHS-specific framework:
The NHS (National Health Service) applies its own data processing policies, which are binding on organisations contracting with the NHS, in addition to the UK GDPR. NHS Digital (now NHS England) operates a data access request process for secondary-purpose research use of data under the GPDPR (General Practice Data for Planning and Research) system. Patients may exercise an opt-out right against the use of their data for research purposes[9].

5. Related Legal Norms and Sectoral Regulations

European Health Data Space:
The EHDS Regulation entered into force in 2024 and introduces fundamental changes to the EU framework for health data processing. The EHDS is built on two pillars: primary use (patients' access to their own data, cross-border healthcare) and secondary use (research, innovation, public health, policy-making). The Regulation applies progressively from 2025, and Member States are required to establish Health Data Access Bodies (HDAB – Health Data Access Body)[5].

NIS2 Directive (2022/2555/EU):
The health sector qualifies as an essential service provider under the NIS2 Directive, and is therefore subject to the Directive's highest-level cybersecurity obligations. These include risk management measures (network segmentation, encryption, access management), an obligation to provide an early warning of security incidents within 24 hours, and rules on managerial liability. The incident reporting requirements under NIS2 and GDPR apply in parallel, but with different deadlines and content requirements[6].

AI Act (2024/1689/EU):
The EU Artificial Intelligence Act classifies AI systems for healthcare decision support as a high-priority category: AI systems used for diagnosing diseases, determining treatments, or allocating healthcare resources fall into the high-risk category. This entails mandatory conformity assessments, registration, transparency and human oversight requirements, which are closely linked to GDPR DPIA obligations[7].

Medical Devices (MDR/IVDR)
Regulations 2017/745/EU and 2017/746/EU also apply to the processing of data collected by healthcare devices. Where a software or device qualifies as a medical device (e.g. a diagnostic

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

algorithm or data analytics platform), compliance obligations apply cumulatively to both the GDPR and the MDR/IVDR.

6. Data Subject Rights in Health Data Processing

The data subject rights conferred by Chapter III of the GDPR have a number of specific features in a healthcare context[1].

- Right of access (Article 15): patients are entitled to obtain information about the health data processed about them and the details of such processing. This broadly corresponds to the right of inspection previously existing in domestic law (e.g. under the Health Act in Hungary), but the GDPR also requires deadlines and electronic accessibility.
- Right to erasure (Article 17): this is limited in respect of health data; where a statutory retention obligation exists (e.g. hospital documentation in Hungary is typically subject to a 30-year retention requirement), erasure cannot be requested.
- Data portability (Article 20): particularly important in health applications; the HL7 FHIR standard is increasingly used as a technical solution for interoperable data exchange. The EHDS Regulation makes data portability mandatory for a defined set of health data.
- Right not to be subject to automated decision-making (Article 22): decisions based solely on automated processing that significantly affect the data subject – including AI-based healthcare diagnostic decisions – are, as a general rule, prohibited. Healthcare AI systems therefore require human oversight and the possibility of human intervention.

7. Data Security and International Data Transfers

Security Obligations:
Article 32 of the GDPR requires controllers to implement technical and organisational measures appropriate to the risks. For health data, the following are regarded as minimum requirements: encryption of data (both at rest and in transit), pseudonymisation where possible, access logging and strict role-based access management, regular security testing, and a disaster recovery plan. Healthcare is one of the most frequent targets of cyber attacks: ransomware attacks can paralyse hospital systems, and therefore the preparation and regular testing of incident response plans, in line with NIS2, is indispensable.

International Transfers of Health Data:

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Health data may only be transferred to third countries where the European Commission has adopted an adequacy decision in respect of that country, or where appropriate safeguards are in place (Standard Contractual Clauses - SCC, Binding Corporate Rules - BCR). The EU-US Data Privacy Framework (DPF) entered into force in 2023 but its lawfulness continues to be challenged before European courts. When using cloud services, organisations processing health data must pay particular attention to the physical location of servers and the content of data processing agreements.

8. Sanctions and Regulatory Practice

Under Article 83 of the GDPR, infringement of the rules on special categories of data – which include health data – may attract a fine of up to €20 million or 4% of total worldwide annual turnover. Real-world enforcement practice offers a number of lessons:

- Portugal: in 2018, a hospital system was fined €400,000 because administrative staff and external persons had access to medical records a typical source of error involving unauthorised access and inadequate access controls.
- Italy: the Italian data protection authority (Garante) imposed sanctions on several health data controllers for failure to carry out DPIAs and for inadequate handling of data subject requests.
- ICO (UK): in connection with incidents involving the NHS and healthcare providers, the ICO has emphasised the importance of staff training and an internal data protection culture, not merely technical solutions.

Civil liability should not be overlooked either: under Article 82 of the GDPR, a data subject may seek compensation where a data protection breach has caused them material or non-material damage. In the case of breaches involving health data, non-material damage (such as mental distress or fear of discrimination) must also be compensated in monetary terms.

9. Compliance Recommendations and Conclusions

Legal compliance in health data processing is a complex, multidisciplinary task requiring the integration of legal, IT, and organisational perspectives. The following measures should be treated as priorities:

- Legal basis identification and documentation: for each processing activity, the applicable Article 9 exception must be clearly identified and recorded in the processing register (Article 30 record of processing activities).

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

- Mandatory DPIA: for large-scale health data processing, the introduction of new technology (AI, wearables, genomic analysis), or the processing of particularly sensitive data, processing may not commence without a prior impact assessment.
- Appointment of a DPO and ensuring adequate authority: the Data Protection Officer must have genuine decision-making oversight and resources, and must not occupy a merely formal position.
- Review of data processing agreements: an up-to-date DPA (Data Processing Agreement) is required with every service provider that may have access to health data (laboratory systems, cloud, HR systems).
- Incident response plan and NIS2 compliance: internal processes must reflect the 72-hour GDPR reporting deadline; the 24-hour early warning obligation under NIS2 applies in parallel.
- EHDS preparedness: with the progressive application of the EHDS, organisations processing health data must monitor Member State implementation relating to the establishment of Health Data Access Bodies and secondary use.

The regulatory environment for health data processing is evolving dynamically: the EHDS, the AI Act, and NIS2 together form an intertwined set of obligations that will deepen compliance expectations further in the years ahead. Organisations that treat data protection not as a burden but as the foundation of patient trust will gain a competitive advantage whilst also avoiding serious sanctions.

References and Legal Sources

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)
2. UK General Data Protection Regulation (UK GDPR)
3. Data Protection Act 2018 (DPA 2018)
4. European Data Protection Board (EDPB) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research
5. European Health Data Space Regulation
6. NIS2 Directive (2022/2555/EU)
7. EU AI Act – 2024/1689/EU rendelet
8. ICO: Guide to the UK GDPR – Special Category Data (health data)
9. NHS England Data Policy Framework (2023)
10. EDPB Guidelines 05/2020 on consent under Regulation 2016/679