Ref. Ares(2020)5621662 - 17/10/2020

Improving lives and managing diseases through a data driven EU healthcare system

Including recommendations on the

Common European Health Data Space

DIGITALEUROPE

12 October 2020

Improving lives and managing diseases through a data driven EU healthcare system

DIGITALEUROPE's key recommendations for the Common European Health Data Space (EHDS)

Executive Summary

Data-fuelled technologies will lead us to a society where better disease prevention, personalised medicines and faster, more accurate diagnoses and therapy become possible in more efficient care processes. The EU needs to leverage them fully across all Member States. COVID-19 has demonstrated that digital technologies can play an important role to enable health workers in combating the virus, ensure remote care for immunodeficient patients, keep communities informed and empowered, support health population management and accelerate research on treatments, vaccines and cures.

Digital technologies are also proving to deliver efficiencies of health services, reducing costs, duplication and waste. They can also play an important role to stimulate growth. The health sector is an economic heavyweight and securing its innovation and competitiveness is a cross-industry and societal concern. For example in Germany, the health industry contributed a full 12% to gross value added in 2018 and was an employer for over 7 million people, driving innovation on new prevention, diagnosis and therapy options. This benefits society as a whole, in the form of better patient care and highly qualified jobs for people.[1]

A truly connected, interoperable and sustainable Common European Health Data Space is a precondition to unlock the potential of health data in the EU. It will ensure that Europe's clinical research will pivot our society towards value-based healthcare models and systems.

For that to happen, the EU should focus on three main areas:

- A framework of trust and legal clarity
  - Harmonise the mechanisms by which personal health information can be shared (e.g. a common approach to pseudonymisation and/or anonymisation) in the EU

[1] German Health Alliance website

- Establish a consistent harmonised model for a central health data authority in each Member State to facilitate the processing of the secondary use of health data for both the private and public research institutions
- Build on responsible data sharing initiatives driven by industry, like YODA,[2] and guarantee private sector participation in the Data Space, while safeguarding Intellectual Property Rights

Interoperability and standardisation

- Advance federated data models
- Foster convergence and acceleration of deployment of Health IT (HIT) interoperability standards such as Fast Healthcare Interoperability Resources (FHIR) building on the Commission Recommendation on a European Electronic Health Record exchange format[3]
- Define a common EU health data classification to help organisations categorise identifiable, anonymised and pseudonymised data
- Confirm appropriate encryption tools and security standards that should be used to process sensitive health data

Increase the potential of digital through investments and ambition

- Use Next Generation (Recovery and Resilience Facility) funds and the next Multi-Annual Financial Framework (MFF) to radically upgrade the digital capabilities of health systems, including cloud technology, as a secure and economic infrastructure for driving digital transformation

[2] YODA stands for Yale Open Data Access (YODA) Project. More info here
[3] Accessible here

Table of Contents

1. A framework of trust and legal clarity

Trust remains the bedrock to build the Common European Health Data Space. Patients, consumers, healthcare professionals and society will unleash the potential of health data only if there is a clear and comprehensive framework of trust and clarity on how health data should be shared consistently across Member States. Addressing the following aspects is crucial for this framework of trust:

1.1 Privacy

A Common European Health Data Space requires a harmonised framework of health data privacy in Europe. The GDPR made possible the sharing and cross-border flow of health data by establishing the foundations of a trust framework for patients, consumers and other stakeholders. But its interpretation and implementation still diverge among Member States. COVID-19 exacerbated the negative impact from this fragmentation.[4] We need decisive EU action to harmonise conditions for health-data processing for primary and secondary use across Europe. We urge to:

- *Create an EU Code of Conduct (CoC) on the processing of genetic, biometric, or health data.* The CoC should accelerate the access and processing of such data within each, and across all, Member States in cooperation with all key public and private stakeholders. European cooperation to fight diseases and viruses, population health management at scale and support to safe cross-border travel are concrete examples of why we need a CoC. It must entail:
  - Public interest as legal basis for circumstances in Article 9.2 of the GDPR. The CoC should also give a common interpretation of what is considered "public interest" by national authorities across the EU. Unjustified, restrictive Member States' interpretations of public interest are preventing hospitals from sharing life-saving data with relevant organisations.
  - A consistent legal interpretation of 'personal data'. The value of data lies in its use and re-use, which strongly depend on the nature of the data involved (personal data vs non-personal data). Personal data falls under the GDPR and its processing is subject

[4] We also intend to highlight good practices:
- The OpenSAFELY platform researched risk factors for death from COVID-19 using an unprecedented scale of Electronic Health Records from 17 million NHS patients, all in a manner compliant with both the GDPR and the UK Data Protection Act of 2018. More info here.
- The World Health Organization (WHO) has a COVID-19 interactive map which gives a daily update on the latest global—and country-specific—numbers of COVID-19 cases. This draws on epidemiological data from around the world and relies on automatic web content extraction, data analytics, processing and storage. More info here and here.

to numerous data protection legal restrictions, which do not apply to non-personal data. Member States, however, do not hold a unique and aligned position on the legal concept of personal and non-personal data. No adequate and recognised standards exist on the anonymisation of personal (health) data. The CoC should fill this gap.

- A consistent anonymisation model that provides traceability back to the source records without representing a risk for subject identification, using the concept of k-anonimity based on existing international best practice standards. It would facilitate data sharing from institutions to researchers, between pharmaceutical companies (for example to limit the need for a placebo/standard-of-care arm in a clinical trial) as well as from pharmaceutical companies to government-funded research initiatives. Data Protection Authorities are adopting excessively strict and divergent interpretations of what constitutes anonymous or anonymised data. This hinders health data processing and makes very difficult for entities to agree on whether and how parties can use the data at issue.

- An opt-out model for secondary use of data in research fields with higher patient identification sensitivities. This model would suit areas like rare diseases, genomes and personalised medicine, with higher re-identification risks than normal and where complete anonymisation may impact the successful research outcome. A robust ethical and security framework with a strong transparency dimension would build necessary patient trust in this model and guarantee that vital identifiable data for research progress is handled properly. It would entail patient rights to actively object to their data being processed.

- Practical guidelines which can support practitioners along the healthcare value chain (including patients, physicians, healthcare managers, industry). They should provide a common data classification framework,[5] providing clarity on how identifiable, anonymised and pseudonymised data should be categorised and where it can be stored and processed.

- A reduction of fragmentation of local conditions on data processing for scientific research purposes. The processing of health data for scientific research purposes is authorized by Art. 9

[5] See section 2.3 for more details

(j) of the GDPR. Yet, Art. 9 (4) of the GDPR allows Members states to introduce further conditions and limitations to the processing of health data. This provision has resulted into the introduction of country- and region-specific constraints to the processing of health data for scientific research purposes, such as those around the concept of "public interest of the research", the "impossibility or disproportionate effort to obtain consent" and the concept of "research institute or body". The resulting patchwork of different rules across the EU is hindering health research. The CoC should create consistency on the use of health data for scientific research purposes and pave the way for a harmonisation of the local implementation of the GDPR.

- *Issue European Data Protection Board (EDPB) essential guidance on the GDPR in collaboration with industry, the European Medicines Agency (EMA) and relevant national authorities.* It is fundamental to bring harmonisation on:
  - the concept of personal data
  - the use of public interest, scientific or historical research purposes, legitimate interest and consent as legal basis
  - the compatibility of primary and secondary use of data
  - the interaction between the GDPR and local and national regulations affecting health data processing
  - the use of Real-World Data (RWD) for medicine discovery and development. Data collected in real life settings[6] can help drive new understandings of value.

1.2 Data infrastructure

The exponential proliferation of data has the potential to transform healthcare and deliver unprecedented levels of quality and efficiency of care. Although multiple initiatives exist across Europe, we observe a lack of coordination and scale, as well as a fragmentation of resources and funding and an abundance of legal and privacy-related boundaries. The Common European Health Data Space requires a robust, secure and interoperable infrastructure with a clear governance framework and defined services. This is key to unlock the potential of health data in Europe.

[6] RWD can include a range of routinely collected data sources from EHR, hospital databases, electronic registries and insurance claims to wearables, apps, and device-generated data, amongst others.

A well-defined, common data infrastructure is fundamental to facilitate a consistent and secure secondary use of health data. The EU should therefore establish a central health data entity at EU level to select standards and profiles for interoperability, as well as a health data entity in each Member State to implement those standards. The role of the national entities should be to provide controlled data services, like healthcare information sharing and analysis. FinData in Finland and France's Health Data Hub could inspire the creation of the entities in each Member State.

The Commission should use the planned legislative governance framework for the European Health Data Space to create this infrastructure. It should establish the legal foundation of both the EU-level health data entity as well as the national health data entities, and mandate national health entities' adherence to the same set of rules, standards and profiles of standards selected at EU level, and in line with FAIR principles in data sharing and access.[7]

A common, pan-European infrastructure as here suggested would help remove health data-sharing obstacles, boost the exchange of cross-border health data across the EU and guarantee health data interoperability, while optimizing scale advantages in global supply markets for healthcare IT and medical devices by building on leading, internationally developed standards and profiles.

Finally, for such governance framework to be effective, it is also crucial the Commission institutes a broad definition of what constitutes scientific research. In today's AI and big data age, a broad range of commercial activities may qualify as scientific research.

1.3 Data altruism

We support health data "altruism" and donation schemes to give clear, easy and secure ways for citizens to give access to their health data for the public good, in compliance with the GDPR. Control over personal data should remain with the patients/citizens themselves. They should be empowered to access and manage their own health data. Policymakers have an important role in making data donation and altruism a driver for healthcare innovation. We recommend them the following:

- For regular or continued data donation, to create GDPR-compliant, European standard forms between data donors and recipients so to establish a legal basis and a strong foundation for long-term data processing activities in areas like research.

[7] FAIR stands for Findable, Accessible, Interoperable, Re-usable

- For one-off donations, to develop a standard, GDPR-compliant European consent form so to make the approval process by donors quick and efficient. The form could foresee data portability requests where necessary.
- To illustrate data donation use cases for citizen awareness and educate citizens about the benefits of data donation for their health and lives. This is crucial to convey to potential data donors why aggregated data is important to advance research and innovation for society's benefit.
- To encourage data altruism via model contractual clauses or data sharing agreements agreed by individuals.

1.4 Transparency and confidentiality

Data transparency contributes to the framework of trust to unlock the potential of health data in the EU. It can advance medicine knowledge and ultimately improve public health. The biopharmaceutical and medical device industry are playing their part to advance that, by promoting clinical research data sharing that benefits researchers and, ultimately, the healthcare community at large. A relevant example is the Yale Open Data Access (YODA)[8] Project, founded to promote data sharing among the scientific community and develop to advance responsible data sharing. YODA provides increased access to anonymised pharmaceutical and medical device clinical trial data and clinical study reports provided by businesses supporting the initiative. A panel in the project independently reviews and makes final decisions on all requests from qualified researchers, physicians and investigators looking to access such data for the benefit of healthcare innovation.

We support industry-driven initiatives such as YODA which enhance transparency while respecting businesses' rights to data confidentiality.

1.5 Ethics

The Commission, Member States and all relevant key stakeholders (industry, academia, health institutions and patients) should develop **ethical principles for healthcare data generation, use, re-use, and curation.** They should address security, transparency and privacy based on the Ethics guidelines for trustworthy AI developed by the European Commission AI High-Level Group.[9] These ethical principles should recognise citizens remain in control over their personal data.

[8] Johnson & Johnson, a DIGITALEUROPE member, is a member of YODA. It is currently making clinical trial data for pharmaceutical, medical device, and consumer products available. More info on YODA here

[9] Available here

1.6 Culture

Trust means also robust data understanding and awareness among officials, payers, practitioners, patients and citizens. As with all technological innovations, including data-driven ones, awareness-raising is key to build acceptance in society. Healthcare stakeholders and policymakers should take a holistic approach to digital health and data literacy. They should create a data culture that encompasses collaboration and partnership amongst healthcare practitioners, payers, patients and citizens. Policymakers should ensure that:

- Every citizen has access to digital literacy and skills training. Digital literacy is critical to ensure citizens and patients are empowered to manage their own data and capable of taking informed decisions. This should extend not only to the use of digital health technologies, but also to the ethics, governance and advantages of using healthcare data to benefit all citizens. They should leverage key stakeholder-driven initiatives such as Data Saves Lives.[10] There are existing training programs available from industry, many of which can be provided free of charge, which Member States could access.
- Health professionals have the necessary skills to unlock the potential of data. ICT specialists are just 1% of healthcare workforce and up to 70% of health professionals do not use digital solutions due to gaps in knowledge and skills in data analytics.[11]
    - Member States must prepare tomorrow's healthcare talent with digital-ready university curricula. Data science and artificial intelligence should be at the centre of a major reform of education systems in Europe, supported by the EU. No health system can be resilient without digital literacy and the necessary digital skills among health professionals.
    - The update to the Digital Education Action Plan, Erasmus +, Horizon Europe and the upcoming Pact for Skills should make sure no one is left behind in the healthcare workforce and that practitioners are able to make use of innovative technologies that benefit healthcare. National authorities should design ambitious digital skills programmes tailored to the healthcare workforce.

[10] More info here

[11] OECD Health Policy Studies, Health in the 21st Century: Putting Data to Work for Stronger Health Systems, 2019

- Local officials become ambassadors and ethical advocates of the digitalisation of healthcare in their communities. This is crucial to raise awareness of digital health innovation at local level across the EU.

2. Interoperability and standardisation

Achieving interoperability among healthcare systems and seamlessly exchanging information and data is critical to improving clinical operations and patient outcomes. 80% of health data remains unstructured and untapped after it is created.[12] Health data siloes prevent practitioners, researchers, authorities and businesses from capturing, analysing and applying valuable information to care delivery, improvements and decisions. Fundamentally, a lack of interoperability directly impedes health systems from providing effective care to citizens, and prevents data from being shared even within health systems. The Common European Data Space must ensure data systems are interoperable and therefore data sets are exchangeable and interpretable, and citizens have control of their personal data. Patient-generated data, clinical data[13] and data from other sources should all be seamlessly accessible and uniformly interpretable through interoperability of devices and systems to unlock the value of digital in this space.

2.1 Common data models

Internationally recognised standards are a critical element to achieve a more outcome-based healthcare systems across the EU. The Commission and Member States should advance federated data models, whose goal is to analyse RWD standardised to common data models. Such models would facilitate interoperability and connectivity while respecting GDPR requirements. Their advantage lies in unlocking access to healthcare data and thus facilitating learning healthcare systems,[14] all while ensuring the highest level of protection of personal data and commercial IP. Through a federated model, the different sources of healthcare data act as nodes in a network. Importantly, the data remain on site, unaltered and uncompromised. It is only the final output of the data analysis that is shared within the framework under secure, legally compliant conditions. Actors can use it to inform research, clinical treatment, hospital planning and payment models, and influence the effectiveness of the overall healthcare demand and supply value chain. EU citizens and patients should be at the core of such a network and remain empowered throughout, so no provider can prevent them from managing or accessing their data. A key example of

[12] Kong, Hyoun-Joong. (2019).Managing Unstructured Big Data in Healthcare System. Healthcare Informatics Research.

[13] Including high-dimensional (e.g. omics) data

[14] Healthcare systems in which knowledge generation processes are embedded in daily practice to produce continual improve in care

federated data model projects is the Innovative Medicines Initiative (IMI) initiative EHDEN,[15] which builds upon the Observational Medical Outcomes Partnership (OMOP) Common Data Model(CDM) launched in the US. The OMOP CDM standardises different structures across disparate health data sources into common tables which harmonise structure, field datatypes and conventions. There are also other projects on common data models focusing minds of policy-makers and the health community. The EMA and the Heads of Medicines Agencies (HMA), for example, have called[16] for the establishment of DARWIN,[17] a European network of databases of known quality and content associated by a strong focus on data security. DARWIN's role would be to extract valuable information from multiple, complimentary RWD databases to support regulatory decision-making.

2.2 European Electronic Health Record exchange format

Fulfilling the ambitions in Recommendation on a European Electronic Health Record exchange format[18] should be key for the Commission. Priority should be given to:

- The completion by 2022 of the exchange of electronic patient summaries and ePrescriptions between various Member States.
- Progress on the other baseline domains identified in the Recommendation. We need profiles providing specifications for interoperability also for laboratory results, medical imaging and reports, and hospital discharge reports. These information domains showed to be vital in the fight against COVID-19 across Europe. The Commission should complete these profiles before 2024 and support their practical implementation to meet clinical needs.
- Convergence on specifications selected for data exchanges between health applications. Convergence will provide strong investment incentives for vendors to comply with prioritised specifications and develop them further. One example are the Existing Fast Healthcare Interoperability Resources (FHIR)standards. They are consistent, easy-to-implement information models used by all major cloud providers and health technology application developers. They also build on similar specifications in related ICT health solutions. Other examples are the DICOM standards and the IEEE Xplore digital library.

[15] More info here
[16] More info here
[17] DARWIN stands for Data Analysis and Real World Interrogation Network.
[18] Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format

2.3 Common data classification framework

Europe should encourage a common health data classification framework to help organisations categorise identifiable, anonymised and pseudonymised data. This is especially important as the volume of global healthcare enterprise data is set to grow at a faster rate than the global average data volume.[19] Properly managing this growing amount of data becomes crucial as it helps organisations to consistently identify data which belongs to a special category or is potentially high risk for sharing, and take appropriate mitigating actions.

A notable focus area on data classification should be to enable the use of all classes of healthcare data with cloud technology, with appropriate levels of security and risk mitigation in place which corresponds with the type of data being processed. The use of cloud computing is growing in important scenarios like global research collaboration, predictive analytics for early disease detection and population health management. We need a more harmonised approach to utilising cloud technology for healthcare workloads. This could be enabled through a commonly adopted risk assessment framework for different types of health data. It would help data controllers to adopt cloud technologies with the appropriate architecture, security and privacy considerations, and ultimately benefit healthcare innovation. We highlight guidance from NHS Digital20 as one among existing good practices and encourage the Commission to also explore others. NHS Digital acknowledges cloud technology benefits, including for the use of data analytics environments pooling together anonymised data, which is a similar concept to the upcoming Common European Health Data Space. Other healthcare systems across Europe, Data Protection Authorities and the European Commission should define together similar guidance at European level. In Annex I below, we detail the main elements of the NHS Digital's Data Risk Assessment guidance to inspire policy-makers' thinking on this issue. We also encourage how the European Open Science Cloud initiative seeks to create a more common understanding of vocabularies and semantic registries to advance data analytics tools in research, including in health.

3. Investments in digital solutions

The EU has well-tested secure digital solutions from across the globe available for it to build capacity for the Common European Health Data Space. These technologies can deliver advanced services and address areas like interoperability of health IT systems, which require ambition from Commission and Member States to fulfil the goals in the 2019 Recommendation on a European Electronic Health Record exchange format. Large volumes of rich and

[19] IDC, The Digitization of the World: From Edge to Core, 2018

[20] NHS Digital is the statutory body in England with responsibility for national information and technology deployment in the health and care system

quality data will enable transformative technology like AI and machine learning to achieve a precise diagnosis, support personalised therapies, draw new patient- and disease-level insights and advance research in vital areas like genome sequencing. They will enable medicines to deliver on their full potential with personalised treatments, and ultimately revolutionise medical science.

We urge policymakers to:

- Recognise Next Generation EU offers an unprecedented opportunity to transform healthcare systems. On average, health sectors in developed economies spend just 10% of total expenditure on software and databases, less than other large sectors like finance and machinery.[21] Member States' Recovery and Resilience Plans should upgrade medical equipment, IT systems and software used in hospitals, medical centres and research labs. We need a paradigm shift in Europe from investments into legacy infrastructure to investments into future-oriented, well-tested technologies capable to project us towards the sustainable, digitalised healthcare systems we need. Data-driven, personalised care requires a strong technology infrastructure as much as a framework of trust and standardised, interoperable systems and devices.
- Prioritise resources for setting up EHDS governance. There should be ample funding reserved in the next MFF (i.e. Health Programme) that is dedicated to the setting up of the governance institutions that will be needed for the creation and functioning of the EHDS. Monitoring and coordinating the implementation of common standardisation will demand meaningful investment. This could be realised with an ambitious Health Programme.
- Accelerate privacy-preserving machine learning and confidential computing solutions. To run collaborative data analytics exercises that guarantee the privacy of datasets used. Techniques like homomorphic encryption minimise any risk of re-identifying anonymised patient data, allowing for AI computation directly on encrypted data.
- Use the Digital Europe Programme (DEP) to establish health-focused, world-reference AI testing facilities. Placed across the EU, they should partner with healthcare actors to test AI solutions in real operational environments. This is key for health organisations to nurture the growth of data scientists at the forefront of healthcare innovation.

[21] Investment in software and databases as a % of non-residential Gross fixed capital formation (GFCF). GFCF is a measure of spending on fixed assets. Source: Calvino et al. (2018[26]),:"A taxonomy of digital intensive sectors"

Annex: NHS Health and Social Care Risk Framework for data transfer to the cloud

NHS Digital (the statutory body in England with responsibility for national information and technology deployment in the health and care system) has published a risk framework[22] and associated risk model,[23] for organisations with health and social care data that wish to make use of public cloud technologies. This guidance acknowledges the benefits of using these technologies, including the use of data analytics environments containing anonymised data: a similar concept to the Common European Health Data Space. It advocates implementing a set of controls which are consistent with the assessed level of risk for processing each dataset. Whilst organisations can never fully remove the risk of processing data using cloud technology, they can build in appropriate controls which are consistent with the risk associated with the data being processed.

Individual organisations retain the responsibility to assess the risk of using public cloud technology with their data. The document provides a high-level overview of the risk classes that should be considered, all of which are relevant to a Health Data Space. The guidance also notes that the construction of the technology solution that is being used to process the data can support the mitigation of some of these risk classes. These risk classes and their description are defined below:

Risk Class	Description
Confidentiality	Data may be subject to loss of confidentiality through breach, through unauthorised access, or through unintended or accidental leakage between environments
Integrity	Data may be subject to loss of integrity through data loss or unintended manipulation
Availability	Ensuring that access to your data is available when required. Network connectivity to cloud becomes a critical dependency and there is a risk of introducing a Single Point Of Failure (SPOF). Public cloud cannot be assumed to be permanently available; cloud availability and SLA [Service Level Agreement] must match the need.
Impact of breach	We cannot assume there can never be any breach, so we need to consider the *impact* of any unintended breach (unauthorised disclosure into an uncontrolled, or less-well-controlled than intended, environment)
Public perception	There is some degree of public concern over the use of public cloud given that these are widely available, shared, computing environments
Lock-in	Flexibility may be impacted (resulting in increased levels of lock-in) by:

[22] NHS Digital, Health and social care cloud risk framework, 2018
[23] NHS Digital, Health and social care data risk model

	• The adoption of a specific public cloud provider's unique services • The difficulties involved in migrating large quantities of data may make it difficult, in time and/or cost, to migrate to an alternative in the event of future commercial or service changes • An architecture that is not sufficiently tailored to a public cloud model

Table 1. Risk Classes and Descriptions, from NHS Digital Health and Social Care Cloud Risk Framework, p 5. Copyright NHS Digital, 2018

The guidance then advises the impact of the risk to be considered in terms of the data type, data scale, and data persistence.

- Data type: organisations are advised to classify their data into the following categories[24]:
  - publicly available information
  - synthetic (test) data
  - aggregate data
  - already encrypted materials
  - personal data (including demographic data and personal confidential data)
  - anonymised data (including reversibly - and irreversibly)
  - patient account data
  - data choices
  - patient meta-data (identifiable and linkable)
  - personal user account data
  - audit data
  - key materials

- Data scale: organisations are also advised to consider the depth and breadth of the data items they are considering, so that the relative impact of a potential breach can be assessed
- Data persistence: the extent to which data will be stored for the long-term versus transitioning immediately out of the environment in which it is being processed. Generally, the risk reduces as the persistence of the data reduces

Organisations are then encouraged to enter information about their data type, scale and persistence into the associated risk framework tool, which generates an associated Risk Impact Score. These scores are mapped to one of five Risk Profile Levels, which provides organisations with an overall perspective on the "degree of risk or contentiousness" of the data they are considering processing in the public cloud. See Appendix C for a description of these risk profiles.

[24] More info on the Data classification scheme at page 7 of NHS Digital Health and Social Care Cloud Risk Framework

As part of implementing controls to support the mitigation of these risks, organisations are then asked to refer to the Health and Social Care Cloud Security Good Practice Guide[25] (see table below), which documents specific controls that should be put in place for the different Risk Profile Levels of the data that has been assessed. These controls include principles for:

- data in transit protection
- asset protection and resilience
- separation between users
- governance framework
- operational security
- personnel security
- secure development
- supply chain security
- secure user management
- (end user) identity and authentication
- external interface protection
- secure service administration
- audit information for users
- secure use of the service

Risk Profile Levels

Risk Profile Level	Governance Expectation
Class I	All organisations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organisations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes described in Section 4, requiring approval by CIO / Caldicott Guardian level.
Class IV	At this level, it is likely to become more difficult to justify that the benefits of the use of public cloud outweigh the risks. However, this case may still be made, requiring approval by CIO / Caldicott Guardian, and would be required to be made visible to the organisation's Board. Specific advice and guidance may be provided by NHS Digital on request.
Class V	Operating services at this level would require board-level organisational commitment, following specific advice and guidance from NHS Digital.

[25] NHS Digital, Health and social care cloud security - good practice guide

FOR MORE INFORMATION, PLEASE CONTACT:

[redacted]
Digital Transformation [redacted]
[redacted]@digitaleurope.org / +32 [redacted]

[redacted]
[redacted] **Manager for Digital Industrial Transformation**
[redacted]@digitaleurope.org / +32 [redacted]

[redacted]
[redacted] **Digital Transformation**
[redacted]@digitaleurope.org / +32 [redacted]

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK