the voice of the NHS in Europe

NHS European Office

Briefing

May 2016 Issue 23

Protecting and managing personal data

Changes on the horizon for hospitals and other health and care organisations

Who should read this briefing?

- This briefing is intended for staff working on privacy or information governance in hospitals and other health and care organisations. It highlights the main changes that can be expected for the health and care sector when meeting the data privacy requirements laid out in the newly approved EU Data Protection Regulation. At the end of each section there are also recommendations for national and EU implementers on how to prepare for a smooth transition to the new law in the health and care sector.

What this briefing is for

- The briefing looks at the most significant changes which have been made to the current 1995 EU Directive on Data Protection and focuses on the key areas of change for the health and care sector.

Key points

- Understanding the EU Data Protection Regulation (the Regulation) is of critical importance to hospitals and other health and care organisations in Europe, as every organisation which handles personal data will have to comply with the new law when processing personal data on patients.
- The Regulation strengthens the principles of data protection by putting more focus on accountability and security. Organisations processing personal data will now be obliged not only to comply with the new law, but also to demonstrate they have complied.
- Hospitals and other health and care organisations need to be prepared for some new requirements which are highlighted in this briefing. In the area of health and social care, there are also opportunities for national laws, guidance and rules.
- The new Regulation was adopted on 27 April 2016 and must be implemented across the EU by 25 May 2018.

Produced in partnership with hope European Hospital and Healthcare Federation

Part of NHS CONFEDERATION

Background

Why has this change come now and what will it mean for the health sector?

Understanding the EU Data Protection Regulation (the Regulation) is of critical importance to hospitals and other health and care organisations in Europe, as every organisation which handles personal data will have to comply with the new law when processing personal data on patients.

The Regulation keeps the same objectives as the 1995 EU Directive on Data Protection (1995 Directive), but aims to make it more suitable for our current technological environment and to ensure the same level of protection of data privacy across the EU. This is important to support the EU's Digital Single Market and ensure consumer trust in technologies.

A regulation (as opposed to a directive) means that each EU Member State will be obliged to introduce the rules as they are decided at EU level, with less scope for interpretation at national level. However, in health and care there will be some opportunities for national implementation laws, guidance and rules, as this is an area where the EU allows national law to apply alongside EU law. Therefore, as long as the boundaries set by the Regulation are maintained, there is scope for national law to apply.

The new Regulation was adopted on 27 April 2016 and must be implemented across the EU by 25 May 2018. **For further information, see the EUR-Lex website**.

Why does data privacy law matter to the health sector?

The use of data is critical not only for providing quality care to individuals, but also for the management of health and care systems, and making life-saving medical discoveries.

Those working in hospitals and other health and care settings not only use data for direct care purposes but also to:

- better understand diseases and improve treatments
- understand patterns and trends in public health and disease
- plan services that make the best of limited resources
- monitor the safety of drugs and treatments
- compare the quality of care provided in different areas.

The NHS European Office and the European Hospital and Healthcare Federation (HOPE) have engaged significantly with EU decision-makers to put forward the interests of hospitals and other health and care organisations on this legislation and have ensured the right balance is struck between safeguarding privacy and protecting the interests of individuals, while enabling health and care systems to collect and connect information to benefit us all.

> "In health and care there will be some opportunities for national implementation laws, guidance and rules."

Main changes for the health and care sector in the new EU Data Protection Regulation

Scope of the legislation: Changing definitions

For the first time the process of pseudonymisation is explicitly defined in the Regulation.

Article 4(5)

'Pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

Recital 26 *(A recital is an explanatory text which is part of the legislation that sets out reasons for the provisions of an Article*)

Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person, to identify the individual directly or indirectly. To ascertain whether means likely to be used to identify the individual are reasonable, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.

The direct implications for some of the data used by health and care organisations are unclear. Recital 26 can be interpreted in a way that suggests *all* pseudonymised data should be considered personal data. However, the reference to "means reasonably likely to be used" suggests a risk-managed and proportionate approach which could take into account the robust security arrangements in place across different sectors.

The Regulation also introduces new definitions for data concerning health, genetic data and biometric data:

- **data concerning health** means personal data related to the physical or mental health of an individual, including the provision of health and care services, which reveal information about his or her health status
- **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **genetic data** means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question
- **biometric data** means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data.

Recommendations to EU and Member State implementers

- Review existing guidance on pseudonymisation and/or anonymisation.
- Consider issuing sector specific guidance.
- Further explore pseudonymisation through codes of conduct.

Principles (Article 5)

The principles relating to personal data processing remain largely the same as the 1995 Directive, only with increased focus on **transparency** and on ensuring appropriate security measures are taken. Data controllers are now not simply expected to comply with the principles, but must be able to **demonstrate** their compliance in an accountable manner. This is an important and significant shift change from passive to active compliance and one that data controllers in the health sector should take note of.

Adoption of codes of conduct detailing internal policies and procedures for data processing could be a way to demonstrate such compliance.

Keywords to encapsulate the main principles of personal data protection in the Regulation are:

Recommendation to EU and Member State implementers

Provide hospitals and other health and care organisations with sector-specific advice/guidance and training by national supervisory authorities on what will be necessary for them to demonstrate compliance with the Regulation.

Lawful processing (Article 6)

The legal basis for lawful processing of personal data remains largely consistent with the 1995 Directive. However, one significant change is that **legitimate interests** can no longer apply to processing carried out by public authorities in the performance of their tasks. 'Legitimate interests' can often be used by companies when the data subject is a client or in the service of the data controller.

In the Regulation, public bodies (including public hospitals and health and care providers) need to define their lawful basis for processing. In principle this should not be a problem, as public health institutions should be able to find an appropriate legal basis for processing personal data in another provision. However, anecdotal evidence suggests that a lot of controllers use 'legitimate interests' as a catch all legal basis, and there will need to be some culture change and possibly training guidance to explain what this change means for public sector data controllers. Some EU Member States may choose to give some additional clarity on this through national legislation. This change may also add to the complexity of data-sharing across public and private organisations, such as hospitals and health and care providers, if the legal basis under which the data are being processed was not clear from the onset of the initiative.

The other lawful bases to process personal data are:

- the data subject has given **consent**
- processing is necessary for the **performance of a contract** to which the data subject is party
- processing is necessary for compliance with a **legal obligation** to which the controller is subject
- processing is necessary in order to protect the **vital interests** of the data subject or of another natural person (life or death scenarios)
- processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

There is also a change to further processing for another purpose than that for which the data have been initially collected. Some thought needs to go in to the scope of 'compatible purposes' in a health and care setting. Hospitals and other health and care organisations will need to spend time understanding the new requirements for defining when their further purpose for processing of personal data can be considered 'compatible'. These requirements are defined in Article 6(4) of the Regulation.

Recommendations to EU and Member State implementers

- In the implementation phase, ensure the relevant national legal frameworks, especially around 'public interest', are sufficient to allow hospitals and other health and care organisations to continue to process personal data where necessary.
- Provide clarification on the new provisions contained in Article 6 (including 6(4)) for hospitals and other health and care organisations on how to go about the process of establishing a legal basis for both the initial processing of personal data and also for further (secondary) processing.

"Hospitals and other health and care organisations will need to spend time understanding the new requirements."

Processing of special categories of data (Article 9)

As in the 1995 Directive, health data remains a special category of data and processing is therefore normally prohibited. Added to the list of prohibited forms of personal data for processing are: genetic data, biometric data and sexual orientation data.

However, as in the 1995 Directive, the prohibition of processing is lifted in a number of clearly defined circumstances. It is worth noting that there is in fact increased scope and flexibility compared to the 1995 Directive in the health and care sector. More specifically, for the first time, there is a specific mention of the provision and management of health *and* care services and the area of public health as reasons for lifting the prohibition on the processing of special categories of data. This could be helpful for new integrated care models and also for public purchasers and planners of care (commissioners). However, it should be noted, that these areas need to be considered by EU or national law.

Consent

Where consent is used as a legal basis, the conditions around consent have been enhanced. Consent needs to be given through a clear, affirmative action, establishing a freely given, specific, informed and unambiguous indication of agreement. Silence, pre-ticked boxes or inactivity does not constitute consent. For processing special categories of data (ie health data), the data subject must give explicit consent – so the bar is raised.

Where consent is used as the legal basis, it is important to note that the 'dual consent' mechanism remains consistent with the 1995 Directive. So *unambiguous* consent is required for processing of personal data, and *explicit* consent will be required for processing of special forms of data (ie health data and genetic data). However, in both cases, alternatives to consent are available.

For the health sector, the most important exemptions from the prohibition on processing of special forms of personal data are as follows:

- explicit consent
- protecting vital interests (life or death scenarios)

- substantial public interest
- preventative occupational medicine, medical diagnosis, provision of **health and social care** or treatment or management of health or social care systems (it is the first time social care has been added and this could facilitate integrated models of care) – based on national law or EU law
- public interest in the **area of public health** – this is specifically mentioned in the Regulation – based on national or EU law (not in the Directive)
- archiving purposes in the public interest, **scientific and historical research**, statistical purposes (subject to Article 89 and national or EU law).

Importantly, Article 9(3) of the Regulation will allow for broadening of the scope of professionals allowed to access data to accommodate new ways of working and new models of care being employed across Europe. Currently health data can only be processed by "a health professional subject under national law, or rules established by national competent authorities, to the obligation of professional secrecy or by another person also subject to an *equivalent* obligation of secrecy". However the new Regulation extends the scope to include a broader spectrum of individuals who could be allowed to process health data. More precisely, the text says that health data and other sensitive categories of data may be processed for preventative occupational medicine, medical diagnosis, provision of health and social care, or treatment or management of health or social care systems when those data are processed "by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies, or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies".

One note of caution is that there is a provision in the Regulation (Article 9(4)) for each country to "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data".

Recommendations to EU and Member State implementers

- Member States should ensure that national rules and laws are fit for purpose to enable appropriate sharing of data across the health and social care workforce, where necessary, for the purposes outlined in the Regulation.
- Encourage Member States to discuss with hospitals and other health and care organisations before introducing any further conditions or limitations with regard to the processing of genetic data, biometric data or health data.

Impact of the Regulation on research

Broadly speaking, the new legislation will maintain the status quo for research in many areas. This includes the provision that further processing for scientific research, statistical or historical purposes can be considered 'not incompatible' with the original purposes for which the data are processed. Further processing for research is therefore permitted, consistent with the 1995 Directive.

However, as with the provisions for health data, there is still scope for national interpretation. The article on processing for historical, statistical and scientific research purposes (Article 89) introduces a dual regime of safeguards and derogations which can be used to support research. This will require member states to legislate the derogations (exemptions from or relaxation of the rules) and safeguards. In order to facilitate cross-border research, it will be helpful here to encourage member states to work together to promote compatibility between national approaches.

The safeguards introduced should also take into account and work with current regulatory approaches, such as ethics committee approval. So at this stage there is quite a lot of work to be done in terms of testing and applying the Regulation at a national level and in providing clear guidance for the research community.

The guidance and conclusions on pseudonymisation (see page 3 of this briefing) will also be of critical importance to researchers.

Recommendations to EU and Member State implementers

- Introduce clear laws for research, with safeguards and exemptions that support research, while respecting people's privacy.
- Develop clear guidance to promote proportionate and consistent interpretation of the Regulation for research.
- Work across national ministries and with the research community to ensure that laws and guidance are practical and proportionate to any risks.
- Work together to promote harmonisation and compatibility between national systems where possible, to facilitate cross-border research.

"The right to be forgotten and erasure of data does not apply to an individual's health record, or for public health purposes or research purposes."

Rights of the data subject (Chapter III)

The chapter on the rights of the data subject has been significantly strengthened in the Regulation, although the basic principles of this chapter remain consistent with the provisions of 1995 Directive. It is worth noting that these rights have always been a challenge for the health sector, with many organisations facing legitimate hurdles in providing clear information to patients that will be helpful and support their data privacy, without bombarding them with dense legal texts every time they enter a hospital or care provider to receive treatment or care.

Information provided by health institutions must be concise, transparent, intelligible and easily accessible (a detailed list of information to be provided is contained in Articles 13 and 14). The information provided to data subjects may also be provided in combination with **standardised icons** when the Commission introduces them through delegated acts (Article 12(8)). For example, there could be a icon used across Europe to symbolise that no personal data are rented or sold to third parties.

The **right to rectification** has been included for the first time as a stand-alone right in Article 16 in the Regulation.

Article 16 of the Regulation

The data subject shall have the right to obtain from the controller without an undue delay the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

This is an extension of language in the 1995 Directive, but it could give more legal weight to the right. In terms of practical implications, it depends how 'accurate' or 'inaccurate' are defined, and whether a medical opinion could be deemed 'inaccurate' if the patient disagrees with it. However, in practical terms, it is difficult to prove that an opinion is inaccurate. Therefore, for example, the supervisory authority in the UK is of the view that opinions are by nature accurate to the person holding the opinion, so a professional opinion is defined as accurate. The **right to be forgotten and erasure of data** (Article 17) does not apply to an

individual's health record, or for public health purposes or research purposes.

The right to **data portability** (Article 20) is an entirely new right and this will need to be considered by all sectors, including the health sector. The data subject will have the right to obtain any automated data which are processed using consent as the legal basis for processing in a "structured and commonly used and machine readable format". This could mean hospitals and health and care providers being asked by patients to receive their electronic data in an appropriate format so they can chose to go to another provider of care (for example, a private provider) or to receive care in another European country.

As with the 1995 Directive, there are certain situations when it is considered necessary and proportionate to **restrict data subject rights**. Article 23 of the Regulation expands on the situations when restrictions could be appropriate, which include national security and defence reasons. These restrictions must be on the basis of EU or Member State law. The list of potential restrictions includes a restriction for professional bodies in the "prevention, investigation, detection and prosecution of breaches of ethics for regulated professions". It also includes a restriction for "other important objectives of public interests of the Union or the Member State, in particular an important economic or financial interest... including public health and social security".

One aspect that could be a challenge for health and care providers is that copies of medical records will need to be provided **free of charge**. Charges can only be made for further copies (Article 15(3)) or where requests for information are "manifestly unfounded or excessive" (Article 12(5)).

Recommendations to EU and Member State implementers

- Ensure national law is clear on when it is considered necessary and proportionate to restrict data subject rights (Article 23).
- Provide sector-specific guidance/advice on how the enhanced and new data subject rights will apply to hospitals and other health and care organisations.

General obligations on data controllers and processors (Chapter IV)

This is basically a new chapter of the revised legislation, where previously this level of detail was left to national governments when preparing their implementing national legislation for the 1995 Directive.

This chapter introduces the obligation to **data protection by design and by default**, also known as 'privacy by design'. It is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether. Data protection cannot be considered a last minute add on – it has to be considered from the start of a project (Article 25). Considering the obligation of data controllers to demonstrate compliance with the Regulation (Article 5), this obligation is an important new requirement. The Regulation gives clearer definitions on 'controllers' (Article 24), 'joint controllers' (Article 26) and 'processers' (Article 28) in this chapter than in the 1995 Directive.

Data Protection Officers (DPOs) are now mandatory for public authorities (Articles 37–39) or when the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data.

The Regulation also makes it obligatory to perform a **prior impact assessment in case of large scale processing of special categories of data (ie health data and genetic data)** (Article 35). This could help to ascertain the legal basis for processing, which will be helpful for public authorities now that the open door of 'legitimate interests' is closed. It is also important to note that "a single assessment may address a set of similar processing operations that present similar high risks". This could significantly help in reducing the administrative burden for hospitals and health and care providers when performing such an assessment.

Notification of breaches (Article 33) to the data protection supervisory authority should normally happen within **72 hours**, and to the data subject without undue delay.

Article 30 ensures the obligation of controllers and processors to maintain an internal record of all data processing activities.

Two potentially interesting opportunities for the health and care sector are the self-regulatory **codes of conduct** which are encouraged in Article 40, which may have general validity across the EU in certain conditions.

Also, controllers will be encouraged to apply for **certification** of compliance with the Regulation – this could be of interest to hospitals and other health and social care organisations. This certification process will be worked out in 2016 by the European Data Protection Board (currently Working Party 29) and the national supervisory authorities.

Stronger enforcement of the rules

Article 82 on the right to compensation and liability is stronger than the 1995 Directive. Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation, shall have the right to compensation from the controller or processor for the damage suffered. A controller or processor is exempted from liability if they can prove that they are not in any way responsible for the event giving rise to the damage. Again, the emphasis here is on the data controller or processor needing to demonstrate the proof that they were not responsible.

Heftier administrative sanctions can also now be imposed by the national supervisory authorities in cases of non-compliance with the Regulation. Depending on the severity of the infringement, this could be up to 4 per cent of the global annual turnover or 20 million euros. It is important to maintain that these percentages and figures are not mandatory fines and will remain at the discretion of the supervisory authorities, as with the 1995 Directive.

Recommendation to EU and Member State implementers

Provide sector-specific guidance on how the enhanced and new obligations of controllers and processors will apply to hospitals and other health and care organisations.

"Data protection officers are now mandatory for public authorities."

Overview of key changes and what they could mean for the health and care sectors

At a glance	Checklist
Scope of the legislation Some of the definitions have been amended and expanded, such as personal data, health data, genetic data and biometric data. For the first time pseudonymisation is defined as a privacy enhancing technique.	☐ Familiarise yourself with the new definitions and consider if this will impact the way your organisation works.
Principles (Article 5) The principles relating to the processing of personal data remain broadly the same, but there is now an obligation for data controllers to demonstrate compliance with the Regulation.	☐ Ensure your organisation is aware of the changes coming up and think about possible training and awareness-raising needs. Think about what you will need to demonstrate compliance with the data protection principles, eg certification, signing up to and applying the relevant codes of conduct mentioned in Article 40, audit trails, data privacy impact assessments.
Lawful processing (Article 6) Public organisations will no longer be able to rely on 'legitimate interests' to legitimise their data processing activities in the discharge of their public functions. When processing data for a new (secondary) purpose, there is a non-exhaustive list of factors which need to be taken into account to consider if the new purpose is compatible with the initial purpose of processing.	☐ Ensure you are clear about the grounds on which you can rely to process personal data lawfully. Don't presume you can rely on the legal basis you relied on previously, as the framework has changed for public organisations. If you were using 'legitimate interests' previously as a basis, this will no longer be an option for you in the discharge of your public functions. If you are using 'consent' as a legal basis, think about how you will be able to demonstrate how that consent has been given (which now has to be an affirmative action, rather than gathered on the basis of silence or inactivity). Make sure you are clear on the further/secondary processing (for additional or different purposes) your organisation performs with personal data and be ready to demonstrate that you have considered the relevant factors to ensure it is compatible with the original purpose, or if it isn't, that you have a legal basis for the additional processing.

At a glance	Checklist
Processing of special categories of data (Article 9) Sensitive categories of data include health data (as with the 1995 Directive), but have been expanded to include genetic data and biometric data. Consent now must be an affirmative action, rather than on the basis of silence or inactivity; for sensitive data this consent must be explicit. The EU has given broad boundaries to EU Member States to apply this Regulation across health and social care. There will be a need for national laws or statutes to confirm the lawful basis for processing of data.	☐ If you are relying on consent to process these forms of data, you need to demonstrate that explicit consent has been given. Follow developments and changes to national law and/or guidance to ensure you are clear on the national conditions around processing of health data and other sensitive forms of data. This may include restrictions.
Rights of the data subject (Chapter III) There is now a more robust framework of data subject rights. This includes: Enhanced rights on issues such as information to patients, which must be provided to demonstrate transparency of processing. The right to rectify inaccuracies in personal data (for example in a medical record) has been given more prominent attention. There is also a new right on data portability (the right to transfer an individual's data to another service provider). Data subject rights can be restricted in certain situations defined in the Regulation.	☐ Be aware of the changes in place and the more robust data protection rights for patients. Consider in particular how to provide information to patients during episodes of care. Keep informed of data portability and how this could impact your organisation. This is a new provision, so there will be guidance on this. For health-related restrictions to data subject rights, these will need to be defined in law and it will be important to follow national developments.
General obligations on data controllers and processors (Chapter IV) The Regulation requires all organisations to put in place a series of measures to ensure they are taking data protection seriously, which includes 'data protection by default and design'. They are required to demonstrate accountability. There is also a requirement to perform data protection impact assessments and to appoint data protection officers.	☐ Be aware of the new requirements for your organisation. Ensure that you have clear processes in place for the performance of data protection impact assessments. Consider the role of the data protection officer and their reporting mechanisms.

HOPE, the European Hospital and Healthcare Federation, is an international non-profit organisation, created in 1966. It represents national public and private hospital associations and hospital owners, either federations of local and regional authorities or national health services.

HOPE's mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.

Today, HOPE is made up of 36 organisations coming from the 28 Member States of the European Union, Switzerland and the Republic of Serbia. **www.hope.be**

The NHS Confederation represents the NHS in HOPE.

The NHS European Office

The impact of the EU agenda on the NHS is constantly increasing, bringing with it both challenges and opportunities. The NHS European Office is the conduit for the NHS to engage with the EU agenda. Hosted by the NHS Confederation, we are the representative body for the range of NHS organisations in England on EU affairs. Our work includes:

- monitoring and influencing EU policy and legislation in the interest of the NHS
- facilitating access to EU funds for NHS bodies and their partner organisations
- supporting pan-European collaborations and sharing successful EU practices.

For more information on EU affairs of importance to the NHS and to get in touch with the NHS European Office, visit **www.nhsconfed.org/europe** or email **european.office@nhsconfed.org**

If you require this publication in an alternative format, please contact publications@nhsconfed.org. We consider requests on an individual basis.

Further copies can be requested from:

Email publications@nhsconfed.org
or visit www.nhsconfed.org/publications

Registered Charity no: 1090329
Stock code: EUR03501

NHS European Office

Rue Marie Thérèse, 21 B 1000 Brussels
Tel 0032 (0)2 227 6440 Fax 0032 (0)2 227 6441
Email european.office@nhsconfed.org
www.nhsconfed.org/europe

Follow the NHS Confederation on Twitter @nhsconfed
Follow the NHS European Office on Twitter @NHSConfed_EU