COCIR Contribution to the General Data Protection Regulation[1]

To the attention of Members of the European Parliament and Representatives of EU Member States

COCIR represents the European Medical Diagnostic Imaging, Electromedical and Healthcare ICT Industry. Our members offer many technologies that support the safe, fast and seamless transfer of medical data to support quality healthcare.

COCIR supports an effective, clear and reliable data protection framework and welcomes the attempt to harmonies the legal framework through the adoption of a regulation. COCIR also recognises considerable improvements in the provisions for data concerning health. However COCIR recalls that quality healthcare depends on the availability of comprehensive health data at the point of care and throughout the healthcare cycle. COCIR feels some provisions could restrict the availability of health data, delay innovation, create legal uncertainty and increase compliance costs. We therefore recommend that the following aspects of the regulation be considered:

COCIR main recommendations:

1. Recognise that data which does not identify a data subject is not personal data (Art. 4)
2. Keep obligations of controllers and processors separate as per current regime (Art. 24-26-77)
3. Reduce administrative burden between Data Controller and Data Processor (Art. 26)
4. Allow processing of data concerning health by technicians and engineers for technical maintenance and equipment performance evaluation under adequate conditions (Art. 81-83)

COCIR secondary recommendations:

1. Extend the exemption to the right to be forgotten to healthcare data (Art. 17)
2. Allow the secondary use of anonymised and pseudonymised data for health purposes (Art. 20)
3. Delete privacy by design and privacy by default obligations (Art. 23)
4. Consider context and feasibility for Data Breach notifications (Art. 31-32)
5. Ensure data protection impact assessments and pre-authorisation obligations for 'high-risk' processings take account of the context and are not 'one size fits all' (Art. 33 – 34)
6. Keep certification industry led and voluntary for more efficiency (Art. 39)
7. Recognise compliance with non-EU frameworks, e.g. HIPAA Privacy and Security Rules, in the U.S., as adequate safeguard for transferring data beyond EU borders (Art. 42)
8. Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible either via restrictive contractual obligation(s) or via technical means (e.g. no key accessible to re-identify data) (Chapter V)
9. Introduce proportionality to Administrative Sanctions (Art. 79)
10. Limit the number and scope of delegated acts for more legal certainty:
    a. Ensure technical neutrality of delegated acts
    b. Provide for industry consultation or direct participation in the drafting of delegated acts
    c. Provide timeline for the adoption of remaining delegated acts

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

DETAILED BRIEFING

I. The sharing of health data increases patient safety, allows innovation and advancement in healthcare technologies, and facilitates medical research

- **Facilitating access to information and timely, collaborative decision-making:** Healthcare delivery in modern hospitals is a highly complex, labour-intensive activity. A large institution will have over 10,000 medical devices, each collecting different identifiable data elements contributing to the medical record.
  Behind every episode of care, there could be twenty to fifty persons who come into contact with one or more element of the medical record (nurse, laboratory specimen transport, laboratory technician, pathologist, pathology resident, clinical physician, intern, medical student, resident, primary care physician, physician office, physician practice administrator, etc.) - all with the common goal of improving patient health.
  Within and beyond the hospital environment, the electronic health record is fast becoming an essential requirement for modern, efficient and safe healthcare systems, linking all parts of the system to the patient. Appropriately controlled access to the health record is essential for primary and secondary care providers, pharmacies, some social care providers and the rapidly expanding area of home-healthcare where patients can be managed and monitored in their own homes.

- **Serving public health interests and leveraging the value of patient registries:** Patient registries are today's primary tool to systematically identify statistical correlations that indicate potential approaches to new ways of therapy. Patient registries are therefore invaluable for improving diagnoses, differentiating between similar types of diseases and preparing studies for therapies. High quality record capture procedures ensure comparability of findings. Studies with large numbers of patients ensure repeatability of findings. Both are cornerstones of scientific work in modern medicine. It has to be noted, that for certain diseases and for certain types of healthcare facilities, the use of clinical registries is already required by national legislation and with the growing use of Electronic Health Record, the future ability of countries to introduce large-scale, population-level data analysis for medical and health trends will increase.

- **Benefits of advancements in Telemedicine:** There is a major shift underway in the practice of medicine and healthcare enabled by technologies that allow remote patient management. Video and computer enabled consultations and diagnosis, in-home patient monitoring, referral of diagnostic images and laboratory reports, etc., for remote examination and expert analysis are increasing, globally. Use of these innovations cuts unnecessary patient travel, best utilizes limited professional resources and drives efficiencies in healthcare delivery-and all rely on the exchange of patient data, including transfer of relevant data outside of the country of origin.

II. Expected Impact of the Proposed General Data Protection Regulation on the Healthcare Sector

The Commission's goal of enhancing the single market by increasing harmonisation of data protection rules across the 27 Member States is to be welcomed. However the benefits of harmonisation are at risk of being outweighed by a number of measures that would result in delaying innovation, creating legal uncertainty, increasing compliance cost for industry and imposing significant burdens on healthcare providers. For eHealth and related domains that seek to innovate and continue to increase quality of care, challenges remain and new ones have emerged. While not an exhaustive list of the healthcare industry's concerns, COCIR seeks to address a select few issues, as follows:

A – COCIR main recommendations

1. Recognise that data which do not identify a data subject are not personal data (Art. 4)

The proposed definitions of Personal Data and Data Concerning Health are too broad and may result in overly-burdensome requirements.

The proposed Regulation defines "*personal data*" very broadly, as "*any information relating to a data subject*," including "*an identification number, location data, online identifier*." This definition fails to provide legal clarity and should explicitly require that context be taken into account in determining whether data identifies a data subject. Indeed, recitals 23 and 24 already recognise that context is a relevant factor, and that data which do not identify a data subject (e.g. the serial number of a device for the provision of telemonitoring in the home) are not personal data; this should be reflected explicitly in the definitions.

Article 4(12), on the other hand, defines "*data concerning health*" as "*any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual*." The inconsistent reference to "an individual," a concept that is not defined in the Regulation, as opposed to a "data subject," should be removed. This inconsistency would turn data that relate to "an individual" but do not personally identify a data subject into sensitive data requiring heightened protection under Article 81.

For instance, a telemedicine service provider may decide to outsource the maintenance of its medical devices to an external company. This company would need select information on the devices, such as serial numbers, in order to monitor their status, even though said information does not per se identify the individual. Considering the serial number of a device as personal data, or data related to the provision of health services to an individual, would bring additional burdens without improving patient privacy.

Moreover, following from Recital 23, the Regulation should expressly recognise in the definitions the category of "anonymised data." Anonymised data would be defined as personal data processed so as to render natural persons no longer identifiable. When personal data are processed with the sole purpose of rendering them anonymous and/or pseudonymous, the provisions of the proposed Regulation should not apply, with the exception of section 2 relating to data security.

Recommendations:

- In the definition of "personal data," recognise the importance of context in determining whether data identify a data subject.
- In the definition of "data concerning health," replace "individual" with "data subject".
- Add a definition for "anonymised" and "pseudonymised" data.
- Article 4 should explicitely recognise that data which cannot link to the data subject (e.g. anonymised data), data which are not directly associated to a data subject (e.g. technical data) or data which require unreasonable time and effort to identify a data subject (e.g. pseudonymised data) are not personal data and are not subject to the Regulation.

2. Keep obligations of controllers and processors separate as per current regime (Art. 24-26-77, etc)

New independent obligations on processors, which would create confusion as to obligations and responsibility between controllers and processors, should be reconsidered in favour of better applying existing requirements.

If independent obligations are placed on processors they will have a duty to better understand the information they process as opposed to relying on representation by the controller. That defeats the concept of data minimization as more entities will need to know more detail about data subjects. Furthermore uncertainty is increased if processors have to determine whether instructions of controllers are compatible with their interpretation of individual requirements. The relation with data subjects is established and maintained by controllers and this is why the existing legal framework foresees direct responsibilities for controllers whilst the responsibilities of processors are left to be determined bilaterally between controllers and processors depending on the circumstances.

Recommendation:

- Maintain the approach of the existing legal framework in Directive 95/46/EC. This would promote clarity as well as better enforcement from the point of view of the relationship with supervisory authorities.

3. Reduce administrative burden between Data Controller and Data Processor (Art. 26 - d)

Requiring each Data Controller (healthcare provider organisation) to agree, individually, to each sub-processor enlisted by a Data Processor (eHealth service provider) would introduce excessive administrative burden and increase costs to both the data controller and data processor.

Article 26 (d) provides that a *data processor* may enlist a *sub-processor* only with prior permission of the *data controller.* A Medical device manufacturer/service provider seeking to enlist a third-party processor to engage in, for example, data mining, data destruction or data storage services acts as *data processor*. Based on the text of the Proposed Regulation, each *data controller* (healthcare provider) would have to agree to such sub-processing. This would introduce excessive administrative burden to both the data controller and data processor, including, significant additional costs. The better approach would be a set of pre-determined conditions within a contract under which the *controller* agrees to allow the *data processor* to enlist the services of a *sub-processor,* this would also preclude inefficiencies caused by disparate opinions where more than one data controller is involved (e.g. data processor B provides services to many data controllers, and may enlist the services of a sub-processor).

Recommendation:

- Maintain the approach of the existing legal framework in Directive 95/46/EC.

4. Allow processing of data concerning health by technicians and engineers for technical maintenance and equipment performance evaluation under adequate conditions. (Art. 81 and 83)

The proposed exemption for processing data concerning health of Article 81 and 83 does not take into account maintenance of medical equipment by manufacturers and registry studies for the improvement of medical devices or medical services, like eHealth services effectively making it impossible for companies to meet regulatory requirements under the medical devices regulation.

Article 81.1(a) provides that data concerning health may by processed by a healthcare professional or a professional with an equivalent obligation of professional secrecy.
It is not clear whether this provision covers technicians and engineers employed by manufacturers, who may have access to data concerning health when maintaining medical systems, either onsite or remotely. The regulation should clarify that professionals who have signed a commitment of confidentiality by contract with their employer qualify as '*professionals with an equivalent obligation of professional secrecy'*.

The current envisaged regulation that will replace the Active Implantable Medical Devices Directive and the Medical Devices Directive will puts emphasis on manufacturer obligations to perform registry studies and post-marketing follow-up studies with respect to medical devices. It is unclear whether the exemption in Article 81(1) can facilitate such studies, as all data processing would need to take place by healthcare professionals. This presents

obstacles for healthcare industry relying on contractual obligations to meet the hightened confidentiality obligations imposed by the Regulation[2].

Article 81(b) and (c) only apply in cases of 'public interest', of which it is unclear that these would apply in the case of a manufacturer seeking to meet its regulatory obligations to improve its medical device.

The exemption in Article 81 (1) will also prevent the rapid roll out of e/mHealth services in Europe as it requires data acquired in "preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services" to be processed by healthcare practitioners (HCPs). Manufacturers and eHealth providers implement security measures at HCPs request and follow highest standards in their commercial practices. The result of requiring the additional HCP secrecy criterion, on top of existing security obligations, would impede the provision of quality m/eHealth services or to analyze health data without involving an HCP in the process.

Examples from other regions, e.g. U.S. HIPAA rules, could ease the reflection.

Recommendations:

- Extend article 81.1 (a) to professionals who have signed a commitment of confidentiality by contract to enable the maintenance on medical equipment by manufacturers.
- Extend to Article 81 (c) to "and services in the health insurance system and the provision of health services."
- Provide guidance/clarification on "public interest."
- Clarify that the processing "for historical, statistical or scientific research purposes" in the meaning of Article 83 includes processing for the purposes of the manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of a medical device, by clear guidance.

[2] *This concern falls is anonymised data are not subject to the Regulation.*

B – COCIR secondary recommendations

1. Extend the exemption to the right to be forgotten to healthcare (Art. 17)

Implementing the right to be forgotten and to erasure in healthcare requires careful consideration of the consequences. Deleting data from an electronic health record does not effectively protect individual privacy, and furthermore, can run counter to patient safety, public interest, health research, and eHealth deployment.

Under the proposed Regulation, Article 17, a patient can ask for the deletion of data in his electronic health record. Article 17.3(b) sets forth an exception to the "right to be forgotten" where retention of personal data is necessary for "reasons of public interest in the area of public health in accordance with Article 81" and for "historical, scientific research purposes, in accordance with Article 83." But it remains unclear to what extent this exception applies. Clarifying the scope for the exception is crucial, as deleting data from electronic health records poses a number of problems:

- Patient safety: Deleting all or parts of the information contained in an electronic health record would undermine the ability of medical professionals to treat the patient effectively. In Germany the 'Lipobay' episode revealed that many serious drug interactions could have been avoided if general practitioners had had access to information on drugs prescribed by specialists (e.g. interactions between Viagra and lowering blood pressure drugs). The Regulation should foresee at minima a mechanism to inform patients on the potential consequences of blocking access to or deleting data in their electronic health record.

- Medical professionals' liability: Clinicians might object to the deletion of data for liability issues: in case of investigation clinicians need to refer to the electronic health record to justify their decisions and treatment delivered. For example German doctors are obliged to keep records for thirty years.

- Risks to health research: Statistical analyses will be "depowered" if data is deleted (particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as paediatric). Further, this may mean that clinical trials and clinical investigations will be conducted outside Europe to avoid any such risk.

- Technical feasibility: Deleting data from an electronic health record may be technically challenging and costly:
    - Medical records are traced in logs. Logs might contain patient information. Browsing through logs to delete information elements could be a very lengthy and costly procedure.
    - Information elements are regularly extracted from the health record for various clinical activities. Each of these derived information elements constitutes distributed traces that take a variety of forms given the clinical activities performed. Thus they are difficult and sometimes impossible to track electronically.
    - The health record or parts of the record may be copied by a medical professional, or by the patient himself. Depending on the number of copies and the location of the copied information, tracking each copies of the record and deleting all copies automatically is almost impossible. For instance, a

patient may have copied his medical file on the Cloud or on his personal computer without the Data Controller knowing or having access to these systems for erasure. In addition, Article 17 requires that the controller have full control over all kind of installed (third party) subsystems. This is not realistic in a healthcare environment.

- Organisational feasibility: The regulation lacks clarity as to which healthcare provider/professional involved in the patient's care—where each contributes in some fashion to the EHR—is ultimately responsible for deleting the data.

- Contradiction with national eHealth programmes: Deleting data from electronic health records runs counter to the foundations of national eHealth platforms and health information exchange infrastructures in which governments are investing large amounts of public money in many European countries. Ministries of health leading eHealth programmes should be consulted and informed of the potential consequences of the right to be forgotten in an EHR context.

Recommendation:

- Clarify Article 17.3(b) exception to the erasure of personal data in the case of healthcare, or specify such exception with respect to electronic health records.

2. Allow the secondary use of anonymised and pseudonymised data for health purposes (Art. 20)

As formulated now Article 20 will become an obstacle to many existing practises with respect to secondary use of data in the health environment.

Health research, particularly in the areas of health services, population and public health, critically depends on the availability of existing data about people. However, most of this data can be anonymised and/or pseudonymised to serve the purpose.
COCIR is concerned about Article 20 not providing a distinction between data processing that identifies an individual and data processing that does not. As currently drafted, Article 20 - which uses the term "natural person" rather than "data subject," seems to broaden the overall scope of the regulation even further by not focusing on personal information and what would constitute a risk for the data subject. We believe profiling techniques per se do not need special regulatory treatment given the many safeguards introduced in the draft Regulation especially when incentives are provided for companies to anonymise and/or pseudonymise data. The current text of Article 20 might render legitimate use of data for health research impossible with great consequences for the social benefits in this area.

Recommendation:

- Delete Article 20 or, alternatively, revert to the language currently in force under Article 15 of the Directive 95/46/EC.

3. Delete privacy by design and privacy by default obligations (Art. 23)

The introduction of the concepts of 'privacy by design' and 'privacy by default' in the Regulation lack legal clarity and runs counter the principle of technology – neutrality.

COCIR believes the usefulness of introducing the concepts of "privacy by design" and "privacy by default" into legislation is dubious. These concepts are still being discussed internationally, and mean different things to different people – they are probably more effective as a policy or marketing, rather than legal, tool.

It is certainly true that organizations should consider the privacy implications of their products and services, both to meet users' expectations and needs and to comply with the relevant legislation. But the actual way it does so should remain flexible and leave room for adaptation based on each organization's business model, size and interaction with personal data. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies.

Introducing a separate legal obligation, by contrast, would be superfluous. In particular, it would seriously risk running counter to the principle of technology neutrality, notably if technical standards are mandated as proposed in the draft text. General-purpose legislation such as the proposed data protection Regulation should be strictly technology-neutral – it should not introduce specific technology or operational mandates, nor contribute to a differentiation between ICT and other economic sectors

Recommendation:

- Remove the concepts of "privacy by design" and "privacy by default" (Article 23) from the Regulation, together with the corresponding recitals (61). Alternatively, remove paragraphs 3 and 4 on delegated and implementing acts from Article 23 and allow for fully industry owned and led measures.

4. Consider context and feasibility for data breach notifications (Art. 31 & 32)

The scope of definition of breach and associated notification requirements, especially the concepts of reasonable timeframe and mitigating effects of safeguards (encryption etc) and potential for harm/adverse impact pose issues of practicability and undue burden. Specific problems in the breach notification requirements include the over-inclusive definition which includes inadvertent access to information within the organization by organization staff as well as the contemplated 24 hours for response/reporting. Breach notification requirements should be risk-based so that they apply only to sectors and/or data types where individuals face a real risk of harm in the event of a breach.

Recommendation:

- Recognise that 24 hours is not sufficient to acknowledge a data breach, analyse it and be able to notify it.
- Adopt a two step approach: require initial breach notification within a reasonable time frame, but allow additional time as necessary to submit the requested information as per current requirements for medical devices. This will allow more time for a qualitative impact assessment, and efficient corrective and mitigation actions.

5. Ensure data protection impact assessments and pre-authorisation obligations for 'high-risk' processings take account of the context and are not 'one size fits all' (Art. 33 – 34)

Impact Assessments should not be standardized. Different types of organizations may have equally effective means of performing such assessments, and unnecessary constraints may hinder improvements in the process, as technologies emerge, and contexts change. Further, consultation with authorities will prove overly burdensome in the context of healthcare, unless the Data Protection Officer has some decision-making authority based on the level of risk involved in the processing activity. This level of risk should be further defined, and a threshold set for when consultation with authorities is required.

Article 33 requires that the processing of personal data relating to health as well as processing of genetic data is subject to the data protection impact assessment requirement. The criteria for impact assessments are not yet clear (as the Commission may clarify them by implementing act under Article 33 (6)). While clarity is crucial to understanding under precisely what circumstances assessments are required, it is equally important that the processes used by varying types or organizations (medical device manufacturers, IT service providers, eHealth service providers, healthcare provider organizations, etc.) are not constrained by specifications under implementing acts. Industry notes that Data Protection Impact Assessments are already implemented by industry in varying forms.
Given that processing activities are often different, impact assessments should not be "one-size-fits-all," rather they should be relative to the scope of processing, volume and type of data, and organizational aspects of those entities performing the assessments.

In addition, while Article 34 provides for a prohibition to start the data processing before approval of the impact assessment, it does not specify timelines for processing of requests by national authorities. Legal certainty as to when a decision can be expected on the adequacy of impact assessment is crucial for stakeholders. Divergence between practices and procedure in this regard between member states will cause forum shopping and the divergences that were amongst the important reasons for the drafting of the Proposed Regulation (see Recitals 7 and 8).

Recommendations:

- Data Protection Impact Assessment should not be mandatory, but should be part of the accountability scheme which can be audited, for instance as part of a certification.
- The regime should allow organizations to construct their own assessment, based on their specific type of organization, legal requirements, contractual obligations, and, where appropriate, internal policies. These assessments should be relative to the scope and types of processing activities, and performed based on a more well-defined category of "high-risk" activity.
- Prior consultation should not be needed when processing is based on consent or contract. Where approval is required (Article 34), a clear time line for the approval should be clarified prior to effective dates.

6. Keep certification industry led and voluntary for more efficiency for more efficiency (Art. 39)

Certification mechanisms, data protection seals and marks, and similar frameworks developed and managed by industry should be favoured. They should remain industry-led as per current practice, and not via delegated acts, implementing acts and technical standards.

The certification process generally applicable in the EU should not be altered in the case of data protection. The current conformity mark procedure provides for full industry participation and the necessary legal certainty for companies both inside and outside the EEA[3] to be able to operate in the EU. A certification mechanism developed and managed by industry, with regulators having backstop regulatory authority, helps to improve trust while reducing compliance burdens and fostering competitiveness.

An alteration of the said framework through the adoption of delegated and implementing acts for the purposes of data protection certification, as proposed by the draft Regulation, would create regulatory imbalance and uncertainty. Moreover, the express provision regarding the possibility for the Commission to lay down technical standards in this area is too broad and risks endangering the principle of technology neutrality.

By contrast, COCIR strongly supports the view, incorporated in Directive 2002/58/EC, that "no mandatory requirements for specific technical features [should be] imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States."

Recommendation:

- Remove paragraphs 2 and 3 on delegated and implementing acts in Article 39.
- Rather than creating yet another certification scheme, authorities should consider promotion and adoption of existing and established frameworks (e.g. ISO/IEC 27001) which have proven efficient.
- The legal framework should provide for mutual recognition of national seals/certification schemes in the healthcare sector.

7. Recognise compliance with non-EU regulatory frameworks, e.g. HIPAA Privacy and Security Rules in the U.S., as adequate safeguard for transferring data beyond EU borders (Art. 42)

Consider HIPAA rules as adequate safeguard for transfer of health data to the USA.

Medical devices companies and companies providing eHealth services are often not only active in the EU and may need to process personal data of EU data subjects in third countries that may or may not have an adequacy finding in order to avoid to have to

[3] *European Economic Area*

duplicate processing means that are already available outside the EU. Many of COCIR's members, for example, have a strong presence in the US and may have invested in processing capabilities there. In this context, it should be noted that HIPAA is a tested and validated set of rules for the processing of health data in the US. HIPAA compliance could provide a mechanism similar to the adequacy findings for the current DOC Safe Harbour Certification as an adequacy finding for the export of personal data in the health field.

Recommendation:

- Recognize HIPAA compliance as "a processing sector within that third country [which] ensures an adequate level of protection within the meaning of [EU rules on adequacy finding for export of personal data]" in Article 41 (3).

8. Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible either via restrictive contractual obligation(s) or via technical means (e.g. no key accessible to re-identify data) (Chapter V).

The transfer of anonymised data should not require any further authorisation or consultation where the recipient does not reasonably have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects.

Anonymised[4] and pseudonymised[5] data which do not reasonably permit re-identification of a data subject, and encrypted data[6] which do not permit understanding of the information, are central to many data processing operations. Responsible data controllers and processors have invested heavily in a raft of data processing techniques to prevent the identification of data subjects and protect user privacy. These efforts should be recognised and encouraged.

Recommendation:

- Add anonymisation and pseudonymisation as recognised means for appropriately safeguarding personal data prior to transferring it to a recipient located in a third country. A transfer of anonymised data, while the key stays within the EU, should not require any further regulatory authorisation.

---

[4] *Previously identifiable data that have been de-identified and for which a code or other link no longer exists. An investigator would not be able to link anonymised information back to a specific individual.*

[5] *Pseudonymisation, a Privacy Enhancing Technology (PET), is essentially the replacement of Personally Identifiable Information (PII) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Information (PII) is earmarked by codes, while the link between the code and the PII (like name, date of birth, address, etc.) is kept separately.*

[6] *Encrypted data is information that has been transformed and made unreadable by the use of algorithms. Only those with the key can decrypt the data.*

9. Introduce proportionality to administrative sanctions (Art. 79)

While there is a general recognition of the need to enhance credible enforcement mechanisms, specifically sanctions and fines, the current proposal lacks proportionality and measureable criteria for legal clarity to prevent primarily a controller and if established secondly the processor as its representative.
This may result in making the EU less competitive in attracting investment in facilities or services. Furthermore the mandatory nature of the fine may not allow mitigating safeguards and the context of the acts to be properly taken into account.

The proposed regulation text currently lacks clarity and remains vague: A few concepts require clarification e.g. 'negligently', incomplete information', 'sufficiently transparent manner', 'does not take all necessary steps'.

Furthermore it is not clear who has the burden of proof for the following new obligations.

- Article 79/5 (b) refers to data subject's right of access (Article 15). Who has the burden of proof that a data subject obtained access or received information from the controller? (E.g. in case the request sent by email did not reach the controller.)
- Article 79/5 (c) refers to the right to be forgotten and to erasure (Article 17) and Implies that all third parties are known to the Data Controller, which is not always the case (see comments on Article 17). In the context of electronic health records, whose obligation is it to make sure that all "known" data are erased? How to ensure that all third parties publication is known?
- Article 79/5 (d) refers to the right to data portability (Article 18) but does not consider security aspects in controller/processor systems.

Recommendations:

- Propose administrative fines that are reasonable and proportional to the harm caused. Administrative fines should not be purely punitive but should encourage organisations to take all necessary steps to avoid repetition of similar situations.
- Add further clarity in the regulation text or provide guidance to clarify those terms to avoid disproportionate imposition of fines.

10. Limit the number and scope of delegated acts for more legal certainty

The number and scope of delegated acts in the proposed Regulation may undermine legal certainty of existing provisions and introduce too much specificity in requirements or implementation methodologies. Guidance on principle or framework level is useful, but limitations on choice of standards and additional certification mechanisms and processes will needlessly constrain cost-effective, scalable implementation of technological and organizational solutions. The number of delegated acts should be reduced, and clear timelines should be introduced for those delegated acts that remain.

A few examples:

11. Article 14(7) empowers the European Commission to adopt delegated acts to specify the criteria for categories of recipients of personal data. In a healthcare environment, categories of recipients of data vary, depending on healthcare provider or eHealth service provider practices, organizations, and workflows. It should remain under the power of these actors considering the case reference as required. The European Commission adopting prescriptive delegated acts (Article 14(7)) is not the right approach as it will delay the process and reduce flexibility in healthcare settings.

12. Article 30(4) – Security of Processing, allows the Commission to adopt implementing acts for specifying the requirements to prevent unauthorized access, disclosure, reading, copying, modification, erasure or removal of personal data. Care must be taken that any specifications pertaining the security requirements for processing personal data are technologically neutral, flexible, scalable and most important, applicable to the type of data being processed, the context for the data processing, and the potential implications to the processing activities. In the healthcare context, highly secure transmission and storage of data is desirable, however, access controls must be respectful of the need to access data in the provision of care, serviceability of medical devices and healthcare technology, etc.

13. Article 81–Processing of personal data concerning health—provides that the processing must be on the basis of Union *or* Member State Law—laws that could impose additional or conflicting requirements in the context of "safeguarding the data subject's legitimate interests." It is imperative that appropriate care be taken to ensure that those measures, criteria, requirements, etc., provided for either by Commission adoption of delegated acts (per 81.3) or by Member State law (81.1) be technology, service and business model neutral, industry-based, flexible, and appropriate to support innovation and technological advancement in the healthcare industry. In addition, additional or supplemental requirements must not impede the fulfilment of regulatory obligations under other EU legislation, such as the Medical Devices Directive.

Recommendations:

- Modify Article 14(7) to ensure that the identification of categories of recipients of data remains under the control and the responsibility of healthcare providers and/or eHealth service providers in a healthcare environment.
- Modify Article 81.1 as follows:
  81.1 – …must be on the basis of Union law ~~or Member State law~~ which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests (…).
- Seek healthcare industry input via direct inclusion of industry on the Board per Article 64(3), or at a minimum via regular consultation to develop scalable, technologically neutral guidance regarding safeguards for personal data processing. Consider industry-specific approach, taking into account the individuals' interest in safe, secure, timely and quality care.