



European Commission's proposal for a General Data Protection Regulation

EPF Position Statement

December 2012

The European Patients' Forum is a not-for-profit, independent organisation and umbrella representative body for patient organisations throughout Europe. We advocate for high-quality, patient-centred, equitable healthcare for all patients across Europe. EPF currently represents 54 patient organisations, which are national patients' platforms and chronic disease-specific patient organisations at EU level. Together they reflect the voice of an estimated 150 million patients affected by various chronic diseases.

Methodology: EPF's position was formulated after consultation of our European-wide membership. This statement centres on the sharing of personal data for healthcare and research purpose, and patients' rights as regards the protection of their personal data.¹

Introduction: why personal data protection matters for patients

The European Patients' Forum welcomes in principle a stronger and more coherent framework for the protection of personal data. Patients' fundamental right to protection of their data concerning health is an important issue in diverse contexts, such as healthcare, care given through eHealth or in a cross-border context, and clinical trials. Patient organisations may also process² such data in their research and advocacy activities. EPF strongly believe that taking into account the patient perspective is essential to ensure that the Regulation preserves quality and safety of care while protecting individual rights to confidentiality of personal health data.

¹ Personal data are information about a particular natural person that allows, or could allow identifying the person. To be covered by the Regulation they need to be collected and processed by someone else (a person or legal entity). It may be any information relating to an individual, whether it relates to his or her private, professional or public life.

² *Processing of data*: any operation performed on personal data.

E.g. collection, recording, organisation, structuring, storage, adaptation, retrieval consultation, use, disclosure by transmission, making available or disseminate, erasure, destruction.

Health data belongs to the category of sensitive data³: unauthorised disclosure of personal health information could negatively impact on an individual patient's personal and professional life. Maintaining health data in an electronic format might also increase the risk that patients' information could be accidentally disclosed to or accessed by unauthorised users. Effective security frameworks need to be put in place to minimise threats to data confidentiality, data authenticity, data integrity and accountability.

On the other hand, the smooth processing of health data is fundamental for the good functioning of healthcare services, patients' safety, and to advance research and improve public health. This is why, for reasons of general interest, several exceptions to the rules apply for health data. However, this tends to result in a greater fragmentation of rules for protection of personal data as regards health and healthcare.

New technologies are offering a wealth of opportunities to collect, use and share health data more efficiently, e.g. to empower patients in managing their diseases, for research, and to improve the quality, safety, and efficiency of healthcare systems. But they set new challenges for privacy and data security, which need to be addressed through appropriate common safeguards in the Regulation in order to ensure transparency for patients and users, and preserve trust.

Summary of recommendations

EPF and our members call on the European Commission, the European Parliament and Member States to:

- 1) Ensure that the Regulation protects **patients' rights** as data subjects and as owners of their health and genetic data, and contains measures to enable patients to benefit from these rights effectively (e.g. access to data, data portability, right to information and transparency). Any restriction due to the special nature of the data processed or legitimate reasons for processing of such data should be justified and limited to what is necessary for public health, or the patients' vital interest.
- 2) Make the necessary adaptations to the Regulation in order **not to hamper provision of care, the conduct of research and public health activities**, including patient registries and activities carried out by patient organisations to advance research and patients' rights, with clear and explicit provisions to ensure the good implementation of this Regulation in the health sector.
- 3) Put in place **effective cooperation measures between Member States and minimum security requirements to ensure an equivalent level of protection of personal data** shared by patients for healthcare and research purposes across the European Union, and facilitate cross-border healthcare and research.

³ *Sensitive data*: A category of data in the data protection framework, which includes health and genetic data, and for which processing is as a rule forbidden, except for exception (healthcare, research, general interest and public health).

4) **Involve patient organisations** in decision-making and activities at policy and programme level for questions that relate to the processing and sharing of patients' personal data, transparency towards patients and informed consent, to ensure the processing is carried out ethically and in a transparent manner throughout the European Union.

1. Principles for the legal processing of personal data

1.1. Data concerning health and genetic data: definition and classification as sensitive data (Article 4)

Data concerning health

EPF welcomes the inclusion of a comprehensive definition of data concerning health in the Regulation. This brings legal clarity and is essential in ensuring patients' trust in their healthcare providers, as it encompasses all data shared as part of the provision of services.

However we believe the definition in the proposal⁴ should be re-worded as "any information which relates to the physical or mental health of an individual or to the provision of *health services and care* to the individual" to be consistent with Recital 26 and encompass all health services.

Genetic data

EPF also welcomes the classification of genetic data as sensitive: we strongly believe discrimination on the basis of genetic information should be prohibited. In particular, **the Regulation should explicitly prohibit the collecting and processing of genetic data for commercial use**, including by insurance companies – instruments such as moratoria and codes of practices need to be used to prevent such discrimination. Consumers of such commercial services should be fully informed about what personal data companies are allowed and not allowed to ask for.

The definition of genetic data (Article 4(10)) should be limited to data that is related to genetic material, i.e. DNA, RNA, and the epigenetic status of both. The current definition can be interpreted much more broadly.

It should be clear to authorities in charge of implementing the regulation that this applies to genetic information that is "personal" in nature (i.e. that could identify the individual). The level of protection that should be accorded to genetic data is a key ethical debate: There are certain components of a person's genome which carry sensitive personal information, such as susceptibility to disease, and genealogy, and this should be protected at the same level as sensitive health information. Yet processing of genetic data is essential to health research and to disease management.

⁴ In the proposal, the definition is currently "data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;"

Genetic data should be judged based on what information it carries, rather than what form it takes. The information that someone is at risk of developing a genetic condition in the future should be treated in the same way whether it is in its raw genetic form or recorded in a database. The same logic should be applied to all forms of information that is obtainable from genetic information, such as gender, ethnicity, blood group, paternity, and risk of disease.

1.2. General principles for processing of data (Article 5)

EPF welcomes the general principles set out in the regulation that the processing of data need to be lawful, fair and transparent in relation to the individual concerned. We also welcome that the specific purposes for which the data are processed need to be explicit and legitimate and determined at the time of collection of data.

We are supportive of Article 5 (d), which states that all reasonable steps have to be taken to erase or rectify inaccurate data. But in areas such as healthcare or research, where several persons may have access to a patient's health record, it is important to define who has the right to perform these tasks.

We believe it should be acknowledged that certain situations may require more flexibility in the application of the principle of data minimisation for healthcare and research. While we agree that as a rule it is important that data controllers must have legitimate grounds to keep the data or share it, there may be a need to keep a patient's personal data for longer, with the patients' consent, and/or for vital or public health interests⁵: For example, it is in the interest of patients that all necessary elements for a diagnosis and for the management of their health are kept in their record. Further, with the patient's consent keeping the data even for a long period of time may be acceptable and useful to researchers.

This relates in particular to Article 5(c) that stipulates that personal data should be kept to the minimum amount necessary and only for the necessary amount of time, and to Article 5(e) which details the conditions to allow for longer storage, but solely for purpose covered in Article 83 (research). In our view this point should also be applicable to certain situations in healthcare: In addition, Article 5(e) should clarify which actor or authority is responsible for the periodic assessment of the necessity to continue the storage.

2. Specific rules for the processing of sensitive patient data, including for public health and research purposes (Articles 9, 81, and 83)

2.1. List of exceptions for health and research purposes (Articles 9, 81, 83)

EPF welcomes that health and genetic data benefit from a higher level of protection under this Regulation: processing of such data is as a rule forbidden, except for the list of grounds in Article 9 or if the subject has given consent. Article 9 details the list of exceptions and

⁵ Data can be processed/kept without patients' consent for grounds and under the conditions listed in article 9

conditions for processing of data without the subject's consent. In our view, these rules ensure that patient data can be processed for essential purposes, such as the provision of healthcare, public interest (e.g. social protection), for public health and research purposes.

In Article 9 2(b) the exception related to employment⁶ as regards processing of health and genetic data needs to be limited and proportionate to the necessary purpose – patients with chronic diseases may face stigma at the workplace or/and may not want their health status to be revealed⁷, therefore these information should not be disclosed without their consent.

Research

From the patients' perspective, secondary use of health data is vital to advancing health research. In our view, the regulation should clearly mention public health research, medical research and social science research (including psycho-social research), either in Article 83 or through inserting a comprehensive definition of "historical, statistical and scientific research". Health research (including medical research) contributes to our present level of understanding of the impact of strategies for improving prevention, diagnosis and treatment, and to evaluate policies for increasing the effectiveness and economic efficiency of health services. The ability to conduct health research, particularly research on health services and population health, depends on data accessibility.

Article 83 also provides for processing identifiable data without consent in exceptional cases when "the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests". While EPF agrees that asking for consent may represent an excessive burden in certain exceptional cases, we believe that the current provisions are too vague and need to be more detailed. The need to lift consent should be assessed on a case by case basis. Patient representatives should be involved in examining these cases.

Genetic data are also a key resource in research and for the provision of healthcare: yet these data tend to be considered as very sensitive and there is a risk to overprotect them (e.g. beyond the level of protection of sensitive health data). At the same time, EPF believes it is essential to ensure that genetic research is carried out in an ethical manner – the involvement of patient organisations at the policy level (e.g. to set guidelines) and in research projects is essential to achieve this. One example of a contribution the patient community can make in this area is Alzheimer Europe's research project "Ethics in dementia research". One of the focuses of this publication is genetic research: it describes existing ethical issues, and provides recommendations as to how to ensure ethics is respected.⁸

Clarifying the rules regarding the different levels of "anonymity" of data

Current practices for anonymising, obtaining re-consent, de-identifying and de-linking personal information (whether carried out by the original data-holder before releasing the

⁶ "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards"

⁷ See [EPF contribution to the reflection process on chronic conditions](#), p14-15

⁸ Alzheimer Europe "Ethic in dementia research" 2011. Also available at <http://www.alzheimer-europe.org/Ethics/Ethical-issues-in-practice/Ethics-of-dementia-research/Genetic-research#fragment-1>

data for research purposes or by the researchers themselves once in possession of the data) tend to vary significantly according to what is considered as 'identifiable'. More clarification on this is needed, particularly in order to ensure the highest protection of patients' privacy and confidentiality when undertaking cross-border research.

Article 83 point 1 (a) as worded encourages definitive anonymising of data – yet pseudonymised data, which can still be linked to the person presents added value in terms of amending, updating, enriching and aggregating the data. Thus their appropriate use should not be discouraged.⁹ Pseudonymised data are considered to be within the scope of the Regulation, but it is important that the regulators take account that while re-identification is technically possible, conditions have been established to minimise the risk. The purpose of the research should also be taken into account in the assessment of risks. **It is important that the degree of anonymity of the data is made clear to patients at the time of consent.**

Tackling fragmentation of rules on patient registries (Articles 81 and 83)

We welcome that the Regulation explicitly refers to patient registries (Article 81): in some Member States, current data protection frameworks make it difficult to put in place these vital tools. Patient registries are used for different purposes: to study prevalence and incidence of diseases, for monitoring the safety of products and interventions, assessing clinical effectiveness of new interventions in real world settings, in planning services or assessing their quality etc.¹⁰ They play an essential role in creating contact between patients and researchers or authorities for clinical trials and other purposes.

A 2011 report on patient registries highlighted that different legal requirements at European, national and regional levels for using health information for research purposes presents a difficulty in setting up such registries – further, it can affect the selection of data, and their secondary use.¹¹ It must therefore be clarified at EU level that patient registries are lawful, and procedures to protect the data of patients should strike the right balance for patients' interests and safety. **The Regulation should require further cooperation between Member States in this area to exchange information, share good practices, and set common data security requirements.** This would facilitate the setting-up and the interoperability of patient registries.

⁹ Please see the Joint Statement on the draft European Data Protection Regulation case study on pseudonymised data by Genetic alliance UK and others for further information [here](#)

¹⁰ S. Aymé, A. Kole, C. Rodwell "RDTF Report on Patient registries the field of rare diseases: Overview of the issues surrounding the establishment, governance and financing of academic registries", June 2011, pages 5-9. <http://www.eucerd.eu/EUCERD/upload/file/RDTFReportRegistriesJuly2011.pdf>

¹¹ S. Aymé, A. Kole, C. Rodwell "RDTF Report on Patient registries the field of rare diseases: Overview of the issues surrounding the establishment, governance and financing of academic registries", June 2011. <http://www.eucerd.eu/EUCERD/upload/file/RDTFReportRegistriesJuly2011.pdf>

2.2. Delegated acts to further specify criteria and safeguards for the processing of patient data for health and research purposes

The Commission proposes to adopt a number of delegated acts¹² to work out specific aspects of the legislation. The Commission would adopt such delegated acts to:

- *further specify the criteria, conditions and appropriate safeguard for the processing of the special categories of personal data (including health and genetic data) (Article 9);*
- *to define the criteria and requirements for the safeguards for the processing of personal data for each of these purposes (public health and research)*
- *further specify other reasons of public interest in the area of public health (Article 81)*
- *to define any necessary limitations on the rights of information to and access by the person, and detailing the conditions and safeguards for the rights of the data subject under research circumstances. (Article 83)*

As regards the delegated acts, EPF concurs with the European Data Protection Supervisor¹³ in the reservations expressed regarding limiting data subjects' rights through a delegated act: we believe that as far as possible the rules should be specified in the Regulation. In addition, EPF strongly believes that specific rules and conditions regarding health data, public health and research should be defined with the involvement of relevant stakeholders, including healthcare providers, professionals, and patient organisations. This is vital to ensure that rules and obligations set in the Regulation:

- do not in practice hamper the good conduct of healthcare services and research,
- are not detrimental to patient safety and quality of care,
- reflect the needs of patients and the health sector,
- do not result in excessive restrictions of patients' rights as data subjects.

For these reason, stakeholders should be involved by the EU institutions during the drafting of the delegated acts and implementing measures. Further, we believe that the Commission should provide a clear timetable for the drafting and implementation of these delegated acts.

It should also be made clear that delegated acts of Articles 9 and 81 are not intended to allow further limitations to the rights of data subjects.

¹² Delegated acts are a new instrument created by the Lisbon treaty (article 290 TFEU), which allow the Commission to adopt quasi-legislative measures, which need to address "non –essential elements" of the legislation: The commission will need to consult Member States and is likely to use (national) expert groups to draft these measures. It must present its proposal directly to the legislators (the Council and the European Parliament) and they have the possibility to object to the act, or revoke it.

¹³ Opinion of the European Data Protection Supervisor on the data protection reform package, page 49 paragraph 304,

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

3. Patients' rights and data protection

Patients are data subjects, and as such they benefit from the rights set out in the Regulation¹⁴. Legal certainty and transparency about the rights of individuals is essential, in particular where sensitive categories of data such as health and genetic data are concerned – any restrictions set out through Article 83's delegated acts or on other grounds (Recital 59) need to be proportionate and justified.

We believe specific attention should be placed on potentially vulnerable people, such as patients with dementia, who may not be in a position to express their wishes as regards the processing of their health data, or to use their rights as data subjects to obtain information on the processing of their data or access to remedies – in this case it should be possible to give that right to a proxy.

We welcome the principles for clear information provided in Articles 11, 14 and 15, as they set out the basis for a meaningful informed consent as regard data processing, although we recommend that patient organisations should be involved in reviewing information for patients on data protection in healthcare and research.

3.1. Consent (Article 7)

EPF welcomes the notion of "explicit consent"¹⁵ for the processing of sensitive data as introduced by Recital 41 of the proposal for a Regulation, as well as Recital 25 which explains that silence or inactivity cannot be considered as consent. We also welcome the right of the data subject to withdraw their consent. For research, explicit consent should as a rule be required. However, we believe that there should be legal clarity regarding what explicit consent entails (e.g. whether it should be written consent), and the situations where this type of consent is required or not.

In addition to this, for patients, the processing of personal health and medical data is inextricably linked with the patient's right to informed consent. For healthcare activities, "informed consent" is a more appropriate concept than explicit consent – requiring written consent within the course of an average medical consultation would for example be overburdening and take time away from the care of the patient. The Regulation should therefore refer to the right to informed consent in the provisions for or the definition of data concerning health.

Regrettably there are still large disparities in informed consent across the EU, both in terms of quality and quantity of the information provided, and the effectiveness of the process. EPF believes that guidelines should be developed for informed consent related to the sharing of health and genetic data. Furthermore, patient organisations need to be involved in the drafting of consent forms at national level, including provisions related to the processing of patients' data. EPF has developed its view on informed consent in the context of clinical trials.¹⁶

¹⁴.These include the right to information, to access, to data portability, to be forgotten, to rectification, to object to processing or profiling, and to lodge a complaint and to remedies, which are further detailed below

¹⁵ Recital 41, p24 of the proposal for a Regulation

¹⁶ <http://www.eu-patient.eu/Documents/Policy/ClinicalTrials/EPF-Statement-Clinical-Trials-May-2011.pdf>

EPF also acknowledges that secondary use of patients' health and genetic data can be potentially highly beneficial in research, yet different data protection rules and practices across Europe as regards consent can be an obstacle to this. We strongly believe that consent forms should be clear about potential future use of patients' data. Patients should be informed of the possibility that their data may be re-used, and it should be clarified if by giving their consent they agree to the re-use of their data by the same research team for the continuity of the study, or a broader consent for secondary use by other researchers and/or for other purposes. If the original consent form is not clear on the future use of patients' data, then consent should be as a rule sought again.

3.2. Right to transparency (Article 11)

EPF strongly welcomes the principle set out in the Regulation that the controller shall have transparent and easily accessible policies for processing and for the exercise of the data subject's rights (Article 11). The requirement that controllers shall provide any information and any communication relating to processing of personal data in an intelligible form, using clear and plain language, adapted to the data subject, is in our view essential.

Patient organisations need to be involved by Member States in the drafting of guidelines for the effective implementation of this principle, in particular as regards the provision of information on data processing and policies by healthcare providers, and by researchers to patients. This is essential to ensure that a patient's consent regarding the sharing of their sensitive health or genetic data is always fully informed.

Further to this, EPF believes that the European Commission and relevant national authorities or supervisory bodies should make available accessible, clear, high-quality information regarding patients' rights in data protection under this Regulation and under the national laws, for patients on the one hand, and for data controllers on the other hand.

3.3. Right to information (Articles 14 and 15)

Under the Regulation patients would automatically be provided, at the first collection of data, with the following information:

- *identity and contact details of the data controller,*
- *purpose and contract terms or general conditions for processing, the period for which the data will be stored, information about the recipients/ category of recipients of their data, the transfer to third countries*
- *their right to request access to and rectification or erasure of their personal data or to object to the processing of such data, their right to lodge a complaint to the supervisory authority*

Furthermore they would have the right to request from the data controller, at any time after the collection of data, information on the processing of that data.

For patients, it is essential to know for which purpose their information is shared, and that it is limited to what is necessary. Patient involvement in this area is essential to understand what patients want and need to know, to ensure they can have trust in their healthcare

professionals and providers and disclose to them all information that is necessary for their safe and effective care. This includes their involvement in the drafting of standard forms for providing the information mentioned in Article 14(8) specifically for the healthcare sector or medical research.

Providing this information may prove difficult for smaller healthcare providers, especially when data is not processed by automated means, therefore clear guidelines should be provided by data protection authorities to ensure data subjects can still benefit from their rights in this context.

Another key aspect which relates to health and genetic data in particular, is that **patients may not want to receive certain information or/and may not want this information to be disclosed to a third party** – for example the results of a genetic test. This right should be specified and protected by the Regulation.

Article 14(2) introduces the concept of “obligatory” provision of data. We believe that if the regulation makes a distinction between voluntary and obligatory provision of data, and the rights attached to these, these concepts need to be clarified.

3.4. Right to access and to data portability (Article 15 and Article 18)

For access: the data subject will have the right to obtain from the controller a copy of their personal data that is undergoing processing, and information as to the source of these data when it is not obtained directly from the data subject. Where the person makes the request by e-mail, he will receive it by e-mail unless that person has requested otherwise. The European Commission would be empowered to adopt delegated acts to specify the one criteria and requirements for the communication to the data subject of the data undergoing processing and information as to the source.

*For data portability: The data subject shall have the right to obtain from the controller a copy of data undergoing processing in an electronic and structured commonly used format that allows further use by the data subject (Article 18(1)). **This is particularly important as regards electronic health records.** The right to data portability means that individuals could easily transfer their data from one service provider to the other, but it applies only under the condition that the data is already in the right format.*

EPF strongly believes that for patients, access to their health records is a moral right, as well as a means for empowerment. Under Directive 95/46 this right was limited.¹⁷ Furthermore in practice, even where this right is established, patients face obstacles in accessing their health records: in many countries this is subject to a fee, and doctors have extensive rights to withhold parts of medical files.¹⁸ EPF welcomes that the proposal for a Regulation provides for patients to have access to their health record free of charge, and EPF calls for Member States to remove other obstacles that hinders access to health records.

¹⁷ The directive 95/46 states that it is for the protection of the data subject and of the rights and freedoms of others

¹⁸ Alzheimer Europe, Dementia in Europe Yearbook 2009.

Access to information about one's own health status is an essential element to enable patients to manage their own health, along with a coordinated health literacy strategy. It is our view that this will help empower patients and contribute to the sustainability of healthcare systems. For these reasons we would welcome a common framework defining the rules and procedures to enable access by patients to their records, which should be defined with the involvement of patients and healthcare professionals.

We also welcome the provisions in Article 18 for access by citizens to their data that are in a "portable" format, that is to say that are in such format that it can be easily transferred from one service provider to another. This is particularly important in the context of cross-border healthcare.

Data portability is a challenge. Patient data may sometimes be stored in "silos" at different places (GP, pharmacist, hospital), and not necessarily in a format that can be shared from one professional to another, or indeed with the patients. We call on Member States to take measures to ensure that electronic health records are in a structured and commonly used format, which can be shared with patients. The issue of *interoperability* of systems also need to be addressed in order to make the right to data portability effective. Patients should also be able to request that their data be transferred from one healthcare provider to another.

3.5. Right to rectification, right to be forgotten, right of erasure, and right to object to the processing of personal data or profiling (Articles 16, 17, 19, 20)

Under the proposal, citizens would have the right to have their data rectified and a right to be forgotten¹⁹ or have their data erased. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, or for exercising the right of freedom of expression.

The data subject would have the right to object at any time to the processing of personal data which was allowed for grounds of vital interest of the subject, public health interest, and legitimate interest of the controller (except for public authorities), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the person. This right also applies when processing is for direct marketing purpose.

EPF is supportive of exceptions for the further retention of data for public interest, research and healthcare purposes. We agree that exceptions are necessary as applying these rights could in some cases cause safety issues, including for the patient themselves. For healthcare professionals and providers, keeping information on file in the patient medical history is necessary in order to give the right diagnosis and to avoid adverse events, and this may include personal data.

We welcome the right to object as this can help to protect the fundamental rights of patients to object to the processing of their data on a case by case basis for particular situations, when it has been allowed for reasons of vital or public interest.

¹⁹ This means that if an individual no longer wants their data to be processed, and there is no legitimate reason for a company to keep it, the data shall be deleted

4. Data controllers: Patient organisations and Healthcare providers (Chapter IV)

Patient organisations are often taking part in research, and may also set up patient registries, despite sometimes limited financial resources²⁰ While we welcome the requirements on data controllers that clarify their responsibilities, EPF calls on the EU Institutions to ensure that this Regulation's requirements on data controllers do not become a burden that would hamper initiatives by patient organisations or other civil society organisations to advance health or the rights of patients. While the Regulation foresees specific rules for SMEs, **the contribution and situation of civil society organisations should also be clearly acknowledged**, for example in Article 9(2d) which refers to non-profit organisations. In our view this Regulation should be an enabler, providing tools and help to such organisations, to help them carry out these activities while ensuring the security of personal data.

Healthcare providers should have in place adequate measures to prevent data security breaches and protect the privacy of their patients, but this should not impede care or cause an unnecessary administrative burden. Special attention should be placed on not overburdening small structures (e.g. GP practices). We welcome the principle of 'privacy by design', which we think is key to improving the security of data processing. Having the right infrastructure is essential for this purpose.

Patients need to have confidence that they can share all necessary information with healthcare professionals safely. As healthcare providers are the ones providing information to the patients about the use of their data, we would suggest that guidelines for healthcare professionals on protecting patients' data and informing their patients on processing. Healthcare providers should be provided with adequate training (and update of their training) to ensure security of data. However, rules and procedures for data protection should not threaten patient safety, nor be an obstacle to timely care or to communication within the healthcare team.

5. An EU set of data security requirements for healthcare

As noted by the European Data Protection Supervisor (EDPS), the current Regulation suffers from an imbalance in that it details the grounds to allow processing of personal data concerning health, but does not provide "corresponding assurance of the protection of data

²⁰ One example from our membership the so called PsoCare centres for psoriasis in Italy. ADIPSO [Associazione per la difesa degli Psoriasici]– together with AIFA – The Italian Drug Agency– created these centres back in 2003 in order to have accurate data for each patient, including important issues such as side effects, previous experience with a specific treatment, etc. There are now 150 centres all around Italy to help psoriasis patients in dealing with their disease. This has also brought assistance to psoriatic patients also in parts of the country where it was not present before.

subjects in this area”.²¹ The EDPS recommends making further provisions on the question of consent, for the determination of responsibilities and security requirements.²²

There is currently no overall healthcare privacy policy defined at European level. The fragmented rules and legal uncertainties may be an obstacle to cross-border healthcare. In addition, the lack of regulation is one of the main barriers for the proliferation and acceptance of eHealth and telehealth.

EPF strongly believes that a common set of security requirements for healthcare and research data should be defined and commonly adopted by Member States’ healthcare service providers in a generic way, without imposing specific technical solutions to the Member States, **to set a basis for mutual recognition and acceptance.**

Ensuring that data processing is safe and respects patients’ confidentiality and privacy is one key element to ensure trust in healthcare. Furthermore, EPF believes that appropriate health stakeholders, including patient organisations and health professionals, should be involved in the drafting of such requirements.

6. Supervisory authorities and European Data Protection Board (Chapter VI)

EPF welcomes the setting up of supervisory authorities and a European Data Protection Board, as they can encourage more consistency in the application of data protection rules across Member States. However, the Regulation does not provide for any involvement or consultation of stakeholders in the functioning of this body. **We strongly believe that patient organisations should be represented on the European Data Protection Board, and consulted by relevant national authorities** on questions related to data privacy in the health sector. This is a requirement of good governance and transparency. Training should be provided to patient experts where needed. Patient involvement is essential to striking the right balance between patients’ preference for the use of their data (either for their own healthcare, to contribute to research, or to exercise their freedom of expression and association) and need for protection of their privacy. Working in partnership with healthcare providers is also essential to preserve trust and ensure the rules are meeting the needs and concerns of all end users in healthcare.

7. Conclusion

EPF is committed to contribute to ensuring that the future EU legislative framework on data protection strikes the right balance to ensure that patients benefit from the rights in this Regulation, while the framework enables the processing of data for healthcare services,

²¹ Opinion of the European Data Protection Supervisor on the data protection reform package, page 48-49
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

²² *ibid*

biomedical and public health research, and various other vital health activities for which the processing of data is necessary.

We are at your disposal for further information



This position paper arises from the EPF 2012 Work Programme, which has received funding from the European Union, in the framework of the Health Programme.

Disclaimer: The content of this position paper reflects only the author's views and the Executive Agency is not responsible for any use that may be made of the information contained therein.