COCIR Contribution to the General Data Protection Regulation[1] and European Parliament LIBE report[2]

COCIR calls for a single, clear and workable data protection framework that protects privacy and encourages medical innovation

COCIR represents the European Medical Diagnostic and Imaging, Electromedical and Healthcare IT Industries. Our Members develop, manufacture and supply innovative and essential medical technologies and solutions in Europe and many operate throughout the world.
COCIR welcomes the European Institutions' efforts to modernise existing data protection legislation and fully supports the goals to (i) harmonise the regulatory environment on the protection of personal data in the EU; (ii) strengthen the protection of personal data while maintaining the free flow of personal data; and (iii) provide exemptions for health and research purposes.
We remain concerned, however, that certain provisions in the Commission proposal and in the European Parliament LIBE report might restrict the sharing of health data, delay innovation, create legal uncertainty and increase compliance costs. We therefore recommend that the following aspects be considered.

COCIR calls for a single, clear and workable data protection framework that protects privacy and encourages medical innovation:

1. Provide for a harmonised set of rules across the European Union
2. Allow and support the sharing of health data for health and research purposes
3. Enable the secondary use of data for health and research purposes
4. Ensure only data related to a data subject are subject to the Regulation
5. Maintain clear and separate responsibilities between the healthcare provider and the medical technology provider
6. Simplify the conditions for sub-contracting between the healthcare provider and the medical technology provider
7. Avoid unnecessary administrative burden linked to impact assessment obligations
8. Clarify the exemption to the right to be forgotten for '*health purposes*'
9. Enable citizens' access to their health data

This list of recommendations is not exhaustive but limited to those most relevant to the healthcare sector. More general concerns remain.

[1] *Proposal for a Regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[2] *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//EN&language=en*

DETAILED BRIEFING

Benefits of data driven healthcare

COCIR members develop many technologies that support the safe, fast and seamless transfer of medical data to support quality healthcare. Diagnostic imaging, biomarkers, electronic health records, telemedicine, data storage and management, and clinical research tools and processes are critical to the development of state of the art prevention, diagnosis, and treatment and rehabilitation practices as a component of sustainable healthcare. COCIR members also develop and supply data collection and management systems used in the analysis of hospital and healthcare system productivity and efficiency in areas such as patient flow and planning, technology utilisation, optimisation of facilities etc.

Data collected, stored and managed by COCIR members' technologies is also a critical component in driving and informing Life Sciences and healthcare research in Europe.
COCIR knows that quality healthcare and medical research depend on the availability of comprehensive health data, collected at the point of care and throughout the healthcare cycle.
COCIR urges EU policy makers to carefully consider the whole new range of possibilities to improve citizens' health and healthcare systems through the use of modern data-driven approaches. The latter include telemonitoring, large disease databases, personalised medicine, medical imaging, human genome decoding, disease prediction, biobanks, biomarkers and many more. These revolutionary innovations rely on the collection; analysis and sharing of health data to better understand diseases and treat them as part of an efficient and effective healthcare delivery system.

The medical innovations described above are supported by data analysis techniques and tools: big data, data analytics, cloud computing, open data, data mining. These processes increase human capacity to understand the data available. Understanding health data means understanding the human body, understanding diseases, understanding our healthcare systems and making the right choices for medical treatment.

Protecting data, respecting privacy

Data processing techniques and practices developed above may incur risks to privacy by accelerating and multiplying data flows. These risks should be understood and evaluated in light of the advances of healthcare innovation and benefits to society. Data processing is too often associated with privacy intrusion. A modern and knowledge-based society like the EU should not hinder the progress of health and medical research on the fear that it might increase risks to privacy. Protecting individuals' privacy is critical but unwarranted fears over the use of aggregated and properly protected data should not compromise the uptake of innovations that will benefit patients and society. Privacy protection and innovation should go hand in hand.

New data processing techniques and tools are available to protect privacy through using the right security modules and the right data protection policies. Indeed, using such systems, COCIR contends, would increase levels of privacy protection in some areas where data is currently stored on paper or in unprotected formats. The medical technology industry has invested in robust data security systems and established comprehensive controls to protect sensitive data from intrusion, theft, loss and misuse.

Striking the right balance

Society needs to find the right balance between safeguarding privacy and encouraging healthcare innovation. We will not find this balance by accepting fear. On the contrary, we should understand these new opportunities and frame them with adequate and workable safeguards. As Commission Vice President Nellie Kroes said: '*Mastering big data means mastering privacy*'.[3]

The European Union wishes to create a vibrant life sciences and health technology sector in Europe, at the forefront of global innovation and job creation. COCIR supports this and believes Europe has the necessary skills and infrastructure to deliver provided the right policies and laws are in place to support the development of these assets. A clear, simple and workable data protection legal framework can achieve this for Europe. To this end, COCIR has developed ten key recommendations for Europe's policy makers considering the future framework for data protection and privacy in respect to health and life sciences.

COCIR detailed recommendations

This list of recommendations is not exhaustive but limited to those most relevant to the healthcare sector. More general concerns remain.

1. **Provide for a harmonised set of rules across the European Union**
   Provide for a high level of harmonisation so that business does not need to address different rules throughout the 28 countries. This will provide legal clarity and simplicity.

2. **Allow and support the sharing of health data for health and research purposes**
   Data collected and managed in Member States in compliance with harmonised legislation must be able to be securely transferred, within and across Member States for the purposes of patient care and relevant medical and healthcare research. 'Big data' promises to help empower better research and better patient care. It needs as much data as possible to do this and international and global databases will be essential in some instances.

3. **Enable the secondary use of data for health and research purposes by adopting a workable consent requirement**
   Ease the conditions for consent for health and research purposes. This will accommodate the secondary use of data in research. A 'broad consent' seems more workable than a 'specific' or 'purpose explicit' consent. Maintaining article 83 as proposed by the Commission would suffice.

4. **Ensure only data related to a data subject are subject to the Regulation by adopting a proportionate definition of personal data**
   The definition proposed in the European Parliament LIBE report is too broad and includes data that may help to identify or single out a data subject, directly or

[3] *http://europa.eu/rapid/press-release_SPEECH-13-1059_en.htm*

indirectly. For instance the serial number of a medical device may be regarded as personal data subject to the Regulation. This will increase the administrative burden for medical device manufacturers without bringing benefits for privacy.

5. **Maintain clear and separate responsibilities between the healthcare provider and the medical technology provider (data processor) as per the current regime to secure legal certainty**
   The healthcare provider (data controller) should be responsible and liable towards the patient data subject. The medical technology provider (data processor) should be responsible and liable towards the healthcare provider (data controller) by contract. Medical technology providers process personal data based on instructions from the healthcare provider. They do not maintain a direct relationship with the patient and should not be liable to him.

6. **Simplify the conditions for sub-contracting between the healthcare provider and the medical technology provider**
   The relationship between the healthcare provider (controller) and the medical technology provider (processor) should be established by contract, not by law. Requesting the 'prior permission' of the healthcare provider before sub-listing another processor creates additional burden and might create delays. In healthcare, delays in processing health data may be prejudicial to patient health and safety.

7. **Avoid unnecessary administrative burden linked to impact assessment obligations**
   The Commission proposal and the LIBE report provide prescriptive obligations for carrying out impact assessments. Healthcare organisations should be able to maintain their own assessment, based on their specific type of organisation, legal requirements, contractual obligations, and, where appropriate, internal policies.

8. **Clarify the exemption to the right to be forgotten for '*health purposes*'**
   Clarify the exemption to the right for erasure/right to be forgotten for '*health purposes*' rather than for *'reasons of public interest in the area of public health'* (as currently stated in the Commission and LIBE proposals). We are concerned that the concept '*reasons of public interest in the field of public healt*h' lacks clarity and may not include delivery of care. We therefore suggest using *'for health purposes'* to clarify the ambiguity and provide legal clarity.

9. **Enable citizens' access to their health data**
   Last but not least, the collection and processing of health data plays a central role in facilitating citizens' interactions with, and access to, the healthcare system. Indeed, the prompt availability and integrated use of health data are not only necessary for the better internal functioning of healthcare systems but ultimately serve the purpose of facilitating citizens' inclusion and empowerment. Citizens cannot be in control of their health if they do not have access to their medical data. More and more, this will involve innovative technologies such as mobile devices and applications. We urge policy makers not to lose sight of this fact in developing a data protection framework that effectively promotes citizens' engagement.

Annex 1: Frequently Asked Questions (FAQ)

Why and how are health data used for health purposes?

Why are health data used for health care purposes?

Personal data is used by health professionals to diagnose the patient condition, monitor the disease over time and select the best treatment. Personal data may be stored over time in an electronic health record to keep a record of patients' health history (medication history, vaccination, allergies, family antecedent, surgeries, etc). Health professionals include medical doctors, nurses and allied professions, midwives, laboratory technicians. They have a professional obligation to secrecy.

Personal data may also be processed by non-medical staff for administrative purposes (e.g. reimbursement, billing). Non-medical staff can include administrative staff from hospital, general practitioner's office, laboratories, etc. These staff members are trained to the sensitivity of health data and have signed a commitment of confidentiality with their employer.

Personal health data contained in electronic health records are also used by citizens to better communicate with providers, better understand their health and treatment options, and make sure health information is as accurate and complete as possible. Data from electronic health records can also be plugged into a growing number of eHealth tools and applications that help patients better manage their own personal health and wellness, often outside of the context of traditional healthcare.

Why are health data used for research purposes?

Personal data allow researchers to compare different factors, such as lifestyle, and the incidence of disease at an individual level. These observational studies have led to breakthroughs such as identifying the association between smoking and lung cancer and informing treatment of infection in unborn babies.

Research using personal data should only take place within a robust ethical governance framework to ensure that an individual's personal data are only used in research when this is proportionate to the potential benefits for society as a whole. Researchers are given access to personal data only under strict confidentiality controls, which have been effective at preventing misuse and harm to data subjects.

Why are health data used for the maintenance of medical devices?

Professionals employed by medical technology manufacturers (technicians, engineers, medical professionals), access health data for technical maintenance and equipment performance evaluation. This is a regulatory obligation under Directive 93/42/EC. They have a professional obligation to secrecy by contract with their employer.

Why are health data used for public health and epidemiology purposes?

Public authorities use health data to detect and model epidemic waves, evaluate the efficiency of treatments, make correlation between risks factors and the emergence of diseases (e.g. asbestos and cancer), define population at risks of poor health, and articulate informed-based prevention and public health policies.

How are health data used to deliver medical innovation? Examples of life saving medical innovations that rely on data processing:

Large diseases databases are crucial tools to increase knowledge on diseases by pooling data for fundamental, clinical and epidemiological research, and real-life post-marketing observational studies and allow the translation of research into therapeutic solutions. The

larger the database the better: studies with large numbers of patients ensure comparability and repeatability of findings, which are cornerstones of scientific work in modern medicine. Patient registries are particularly important for rare diseases, where little data is available. 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. For instance, England is considering creating a nation-wide database containing records of all patients in England (care.data).

Personalised medicines are medicines which are tailored to the patient, by opposition to conventional 'one size fits all' drugs (e.g. antibiotics). Personalised medicines use molecular profiling for determining the predisposition of an individual to disease, for tailoring the right therapeutic strategy for the right person at the right time, and for delivering timely and targeted prevention. Personalised medicine can improve prevention; improve treatment efficiency and improve patient quality of life.

Medical imaging is the technique and process used to create images of the human body to reveal, diagnose, or examine a disease. Medical imaging is critical for early diagnosis and better evaluation of the treatment effect for improved outcomes. Medical Imaging has become a cornerstone of modern medicine in many disciplines: oncology; traumatology, muskoskeletal disorders, etc.

Genome based prediction of diseases is an emerging science looking into a person's genome to understand the susceptibility of developing a particular disease. For instance common diseases such as type 2 diabetes and coronary heart disease result from a complex interplay of genetic and environmental factors. Recent developments in genomics research have led to the discovery of susceptibility genes for these diseases and opened new opportunities for genetic profiling for personalizing medicine.

Biobanks are repositories that store biological samples for use in research. Biobanks give researchers access to data representing larger numbers of individual people than could be analyzed in previously used systems. Furthermore, samples in biobanks and the data derived from those samples can often be used by multiple researchers for multiple purposes. Biobanks have become a key resource, supporting many types of contemporary research like genomics and personalized medicine.

Biomarkers are traceable substances that are introduced into an organism as a means to examine organ function, or indicate a particular disease state or other aspects of health. Used in medical imaging, biomarkers are an essential element of predictive, preventive and personalised medicine.

Telemedicine refers to the delivery of healthcare services remotely with the support of ICTs. Telemedicine cuts unnecessary patient travel, best utilises limited professional resources and drives efficiencies in healthcare delivery. Telemedicine relies on the exchange of patient data, including transfer of relevant data outside of the country of origin.

Electronic health records are a central repository of patient data. EHRs are quickly become an incomparable tool giving health professionals easy, timely and targeted access to patient data at the point of care. EHRs can also feed larger databases for secondary use (e.g. research) if the data has been de-identified. Citizens' access to their EHRs is one key method of sharing relevant information to help them navigate the healthcare system and make informed decisions about their health.

How can large volumes of health data be best exploited? Examples of techniques and tools to make sense of data:

Big data refers to the increasing volume of data available in different forms, from different origins, collected for different purposes but which can be pooled and analysed for a common purpose. In healthcare, 'big data' management systems offer great potential to drive clinical actions and outcomes from analysis of aggregated health, lifestyle, environmental, social, genetic and other factors. The larger the databases, the better the outcomes and in many cases, particularly when dealing with rare and uncommon diseases, this requires sharing and transfer of data across regional, national and international borders.

Data analytics refers to the discovery and communication of meaningful patterns in data, in order to make sense of the 'big data'. Data analytics techniques analyse datasets to describe, predict, and improve performance. Commonly applied in business, data analytics are increasingly used in healthcare.

Cloud Computing refers to internet-based computing, where shared servers provide computing power, storage, development platforms or software to computers and other devices on demand. In healthcare this means that patient data might be stored and processed in a virtual location (the cloud) as opposed to hospitals and/or research centres' servers. In healthcare cloud computing is increasingly recognised as the ideal back-end service to manage applications and enable collaboration.

Open data is data that can be freely used, shared and built-on by anyone – in both the public and private sectors – for any legal purpose. In healthcare, data that is machine-readable, downloadable and accessible via application programming interfaces, while rigorously protecting privacy and confidentiality – including clinical care provider quality information, health service provider directories, databases of the latest medical and scientific knowledge, consumer product data, community health performance information, government spending data and much more – has spawned a vast array of private-sector innovations that have created large-scale public benefit and economic value.

What are the existing tools and practices to protect health data?

Anonymisation
Anonymisation is the process used to strip personal data from all elements likely to help identify directly or indirectly the data subject (e.g. name, age, address, social security number, etc.). These elements are deleted to ensure re-identification is not possible.

Pseudonymisation
Pseudonymisation is the process of disguising identities - the aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity. This is particularly relevant in the context of research and statistics. Disguising identities can also be done in a way that no re-identification is possible, e.g. by one-way cryptography, which creates in general anonymised data.

Encryption
Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted.

What type of practices would be ruled out by the LIBE report if adopted, or by disproportionate data protection rules?

- The NHS in England is planning to establish a nationwide patient database including all electronic health records to be accessed by researchers and drug firms (unless patients opt out). The objective is to advance medical science by helping the medical community understand the causes of disease, spot side-effects to new drugs and detect outbreaks of infectious diseases. The Commission proposal and the European Parliament LIBE report would not allow such a system - because it requires that individuals give explicit consent, knowing the specific purpose for which data is being used.

- European Medical Information Framework (EMIF) is a €56 million collaboration to link together existing health data from 40 million European citizens across seven EU countries. EMIF will make health data from a range of sources - including hospital databases, cohorts and national registries - accessible to researchers for studies on obesity and Alzheimer's disease. The development and use of this powerful research resource would be seriously threatened if the LIBE report is adopted because the exemption from specific consent is very narrow

- Medical image processing software needs to be proven safe and effective before it can be placed on the market. The development and testing of such software requires actual patient data. Today hospitals can de-identify, or strip their medical images from all identifiers (e.g. patient name, address, social security number, etc.) before providing the images to manufacturers for development and testing purposes. Most national privacy laws consider that a medical image stripped from identifiable data is anonymous; therefore no patient consent is needed to use the image for research, development and testing purposes. However six European countries believe that it is not anonymised because the clinician can recognise the image and link it to his patient. As such, according to the law of those six countries medical images can never be called 'anonymous' and therefore always require patient consent. This implies a significant cost for manufacturers. Industry estimates a 25% cost increase:
    - The cost of collecting the patient consent is estimated at 100€ per image.
    - A new software algorithm may require thousands of images to develop and test.
    - Minor software updates are tested on about a hundred images. Often there are several releases per year of a particular application.

  Introducing a consent requirement will increase the development cost of medical image processing softwares, and slow it down, with no benefit to privacy.