COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 15 September 2014

T-PD(2014)07

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD)

MEDICAL TECHNOLOGIES AND DATA PROTECTION ISSUES

Directorate General Human Rights and Rule of Law

FOOD FOR THOUGHT[1]

1. Introduction

The work programme 2012-2013 of the Consultative Committee of Convention 108 included in the section entitled ‘other work’ a proposal to review the implementation of Recommendation N° (97) 5 on the protection of medical data in order to recommend, “where necessary, an update”.

In order to start this work, it was proposed that a questionnaire be prepared in order to obtain from Parties to the Convention information on the implementation of Recommendation N° (97) 5 on the protection of medical data and assess the emerging trends and new forms of processing of medical data. It was decided that the questionnaire should not aim at assessing comprehensively how the Recommendation is implemented at national level, but rather to identify emerging trends in the area that should be tackled on the update of the recommendation.

Such a questionnaire should encompass the following topics:

- Electronic Health Records (EHR);
- Data integrity;
- Data security, including place of storage;
- Outsourcing of processing;
- Data mining of electronic health records;
- Use of RFID and other communication technologies.

Furthermore, the questionnaire should allow for the delegations to provide information on situations which have already been experienced at national level, such as for instance:

- “Appfication” of the society;
- Medical devices v. Wearable devices;
- The eDoctor;
- Internet of Things;
- Data mining and profiling from data not related to medical data and EHR.

The present document aims at presenting some of those new trends and services, in order to stir reflexions and enable the Delegations, in preparing their replies to the questionnaire, to better identify the situations which are concerned, and related problematic.

2. Topics for discussion:

2.1 “Appfication” of the society:

- All of the following technologies can collect sensitive personal information that can be considered medical data:

[1] Prepared by Renato Leite Monteiro, Study Visitor, Data protection Unit

> "Most modern smartphones are embedded with a variety of sensors, including, but not limited to, a multitouch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras. New devices also feature fingerprint sensors. Biometrics is a field that is becoming increasingly prominent in the area of smart devices." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

> "A mobile phone can serve as an accurate monitor for several physiological variables, based on its ability to record and analyse the varying colour signals of a fingertip placed in contact with its optical sensor'" (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

- Specific requirements for applications, mainly mobile applications:

> "Manufacturers of medical apps that may incidentally be medical devices do not have to create them to the same standards required for conventional medical devices. Given that the regulation of medical devices is deemed necessary to protect those who use such devices, it is alarming that medical apps that are in reality medical devices are not subject to the same level of scrutiny as is the case with conventional medical devices. Whilst apps may represent an exciting area of innovation, it is difficult to see why they should be subject to a lower level of safety requirements than other more conventional requirements." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

2.2 Medical devices v. Wearable devices

- Some eHealth and mHealth devices and apps currently do not fall in the clear definition of medical device, therefore cannot be regulated by current Directives, Conventions and Recommendations. Requirements for an application and/or mobile application to be considered a medical device:

> "The basic idea behind the MDD framework for software is that all computer programmes that meet the definition of a medical device must comply with the MDF's requirements. A medical device is: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

> "All software that meets this definition, including software that works in combination with a physical device, for instance a smartphone, will be categorised as a medical device (Quinn et al., 2013)." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

> "The ability to augment smart devices with hardware attachments has also led to a rise in the number of attachments turning them into ad hoc medical devices, from otoscopes to portable EKGs." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

> “Take note of tracking mechanisms, weareable devices, intelligent clothes. Example: the AIRO wristband — launching in the fall of 2014 — will be able to track automatically both the calories you consume and the quality of your meals. With a built-in spectrometer, AIRO uses different wavelengths of light to detect nutrients released into the bloodstream as they are broken down during and after your meals.” (**5 Health Tech Trends to Watch in 2014 (http://mashable.com/2013/12/09/health-tech-trends-2014/**)

> “Scanadu’s ScanaFlo device — which is expected to launch in 2014 — can turn your smartphone into a urine analysis reader that will test for pregnancy, glucose levels, protein counts and more.” (**5 Health Tech Trends to Watch in 2014 (http://mashable.com/2013/12/09/health-tech-trends-2014/)**

> "The European Parliament voted on 22 October 2013, on two draft Regulations intended to replace the Medical Devices Directive (...) The new definition of ‘medical device’ provides that medical devices can have direct and indirect medical purposes, which would include products providing information with direct or indirect impact on health." **(eHealth Law & Policy, November 2013)**

2.3 The eDoctor

- Another increasing trend is to bring the doctor to you, as many other services, on line, for which the doctor does not need to be in physical contact with the patient. How should this be assessed?

2.4 Data mining and profiling from data not related to medical data and EHR.

- Data that can lead to the identification of an individual and his/her health situation is not limited to medical data *per se, but* also to data present on Electronic Health Records and on unsuspicious type of records:

> "We are now at a point where, based on your credit-card history, and whether you drive an American automobile and several other lifestyle factors, we can get a very, very close bead on whether or not you have the disease state we're looking at," said Roger Smith, senior vice president of operations at Horsham, Pa.-based Acurian, a unit of Pharmaceutical Product Development LLC. (**Data Mining to Recruit Sick People**, Wall Street Journal, 17.12.13, accessible at: http://online.wsj.com/news/articles/SB10001424052702303722104579240140554518458)

- The definition of medical data in the current Recommendation: does it include physical tracking data, such as pedometers or fitness data? Paragraph 38 of the explanatory memorandum states that medical data includes, inter alia, information relating to the general lifestyle:

> 38. The drafters of the recommendation further agreed that under the terms of the recommendation, "medical data" should also include any information - unless it is public knowledge - giving a ready idea of an individual's medical situation, for instance for insurance purposes, such as personal behaviour, sexual lifestyle, general lifestyle, drug abuse, abuse of alcohol and nicotine, and consumption of

> drugs. This was the reason for including in the definition of medical data the words "manifest and close", that is, having a clear and direct impact on the health situation of the individual.

- Lifestyle tracking apps and devices are one of the biggest market nowadays and also source of an immense amount of personal data. Paragraph 61 highlights this interpretation when stating that the processing of the data must be for the purpose of medical treatment:

> 61. In practice, this means that the principles are applicable to the collection or the processing of medical data for the purpose of medical treatment, the assessment of the health situation or the fitness of a person **(Explanatory memorandum of the Recommendation)**
>
> What about for instance of "Apps (that are currently described as existing for the purposes of well-being, but which could in fact be said to have a quasi or pseudo-medical purpose, such a pedometer for self-monitoring)" (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

2.5 Centralised EHR databases.

- EHR are the basis for large databases with medical records. Most of these databases are separate, independent, even with different types of health and sensitive information and their creation and use should thus be examined very carefully. When all the information of all different medical records of an individual are put together, centralised, the risk of damage in cases of unauthorised access raises exponentially. Even by applying anonymisation techniques, the chances of linking those records to an identifiable individual are huge. Nonetheless, where such centralised databases exist, stricter safeguards should be employed, such as access only after judicial review:

> "In the past, Davis said, police would need to track down the General Practice (GP) who held a suspect's records and go to court for a disclosure order. Now, they would be able to simply approach the new arms-length NHS information centre, which will hold the records. (...) The records will include mental health conditions, drugs prescribed, as well as smoking and drinking habits – and will be created from GP records and linked to hospital records. (...) In the case of the police, officers will be able to request all of the medical data held for specific suspects with their correct identities, regardless of whether they had opted out. (...) The extracted information will contain a person's NHS number, date of birth, postcode, ethnicity and gender. Once live, organisations such as university research departments – but also insurers and drug companies – will be able to apply to the new Health and Social Care Information Centre (HSCIC) to gain access to the database, called care.data. (...) If an application is approved then firms will have to pay to extract this information, which will be scrubbed of some personal identifiers but not enough to make the information completely anonymous – a process known as 'pseudonymisation'". (**Police will have 'backdoor' access to health records despite opt-out, says MP**, accessible at: http://www.theguardian.com/society/2014/feb/06/police-backdoor-access-nhs-health-records)

3. Possible actions

A number of elements could be considered in reflecting on how to update the Recommendation.

3.1 The question of consent

- Does the processing of medical data performed by apps fall under the need of health-care professional confidentiality? I.e., is it necessary for the collection to be in reference to a medical treatment? E.g., how would this be applied to fitness and daily-basis data? Maybe, apps with medical data should only be allowed to use with the indication and supervision of a medical doctor or a health professional.

  > "Only if apps are integrated in the doctor–patient relationship, one can hope that the patient truly understands that to which he or she was consenting. It is questionable if apps processing data for medical purposes can be used without any supervision." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)
  >
  > "In a real-life environment (in a hospital, for example) a healthcare provider would be able to guide users/patients through the process of consent, explain the consent form that needs to be signed and to answer possible questions. Current medical apps often leave the user alone and even require him/her to open up additional links to find information on external sites (Lie Nije, 2013)." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

  But this practice might have a big impact on the market. Current apps that collect personal data that can lead to a health context rely only on users' simple consent, which is provided when the app is installed.

- One possibility would be to ensure that the consent be only given after the data subject has been properly informed, i.e. by using granular consent:

  > "According to Article 29 Working Party, granular consent means that 'individuals can finely (specifically) control which personal data processing functions [are] offered by the app they want to activate.' Granular consent echoes the notion that consent to data processing ought to be 'specific', that is, users must give consent for each type of data the app intends to access." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)
  >
  > "Granular consent is about or would entail drawing up two separate consent forms: one consent form for the general provisions regarding the apps and its functions, and another separate consent clause for the purpose and means of the processing." **(FTC, 2013).**

- The principle of granular consent can also be applied to granular information, i.e., in cases where consent is not necessary, the data subject needs to be informed separately, and not only about the general purposes or in a fashion manner (e.g., when apps already have the consent and are going to process the data for a particular purpose):

> 107. But even in cases where his/her consent is not required - that is, when the collection and processing of medical data follow an obligation under the law or under a contract, are provided for or authorised by law, or when the consent requirement is dispensed with - the recommendation provides that the data subject is entitled to relevant information. **(Explanatory memorandum of the Recommendation)**

- Transfer to third-parties is one of the big issues, since the current recommendation foresees the transmission of data if the user has consented to it. But medical data, as a type of sensitive data, should be treated differently:

> 195. In the second place, the drafters of the recommendation have suggested that communication could take place if the data subject had given consent, and thereby had taken the responsibility in the circumstances envisaged for his/her medical data to be communicated outside his/her national territory to a country where it is impossible to monitor the fate of the data. **(Explanatory memorandum of the Recommendation)**
>
> "A recent study comparing 43 medical apps from the biggest app stores showed that many medical apps for mobile phones send data, connect to third-party sites, perform behaviour tracking, use unencrypted connections, allow for data collection by third parties and store data externally. Most of the time this happened without notifying the user or without the user's prior consent (Lie Nije, 2013)." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)
>
> 143. It is obvious that medical data, one of the categories of sensitive data for which the convention requires special protection, should not be communicated outside the medical context in which they were collected, unless they are made anonymous (in which case the data no longer fall under the definition of personal data). **(Explanatory memorandum of the Recommendation)**

- The possibility of derogation of the recommendation in order to fulfil contractual obligations might need to be clarified, since for non-European members the scope is broader than only labour obligations.

> 74. When medical data are collected and processed in the context of contractual obligations (Principle 4.3.b.iii and 7.3.b.iii), member states of the European Union will, after transposition of the community directive into their national legislation, be able to make use of this option only in the context of labour law; for the other member states of the Council of Europe these principles may be taken into consideration in other fields, such as sport, training or insurance. **(Explanatory memorandum of the Recommendation).**

3.2 Privacy by Design

- In the recommendation, when it comes to security, the situation of online unauthorised access or electronic security breaches is not included. It appears that the security measures were limited to physical aspects:

> "I have never seen an industry with more gaping security holes," said Avi Rubin, a computer scientist and technical director of the Information Security Institute at Johns Hopkins University. "If our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed." (**Health-care sector vulnerable to hackers, researchers say**, http://articles.washingtonpost.com/2012-12-25/news/36015727_1_health-care-medical-devices-patient-care)
>
> Search Engine of Vulnerable Medical Devices: http://www.shodanhq.com/search?q=xray
>
> "Healthcare fraud is costing American taxpayers up to $234 billion annually, based on estimates from the FBI. It's no wonder that a stolen medical identity has a $50 street value, according to the World Privacy Forum – whereas a stolen social security number, on the other hand, only sells for $1." (**World Privacy Forum**, http://www.worldprivacyforum.org/medicalidentitytheft.html)

- Privacy by design on the Application Programming Interface (API) of apps? APIs should:

    • Determine the means (and extent) of access to personal data;

    • Allow app users and the apps developers to have sufficient level of control on access, so that only data that are necessary for the functioning of the app are accessed (granularity);

    • Include the possibility of revoking access in a simple and effective manner.

- These issues mean that even where individual manufacturers wish to attempt to comply with the requirements of the medical device, they will find it difficult to do so unless the app in question is restricted to a few selected, potential accessories. This can be mitigated with privacy by design in the Operating System (OS):

> "The medical device directive requires that the testing of a medical device be performed with all the accessories with which it is to be used. The essential requirements of the directive must be met by the combination of the medical device and the accessory. Medical apps are somewhat different from conventional medical devices in so far as they are not designed to work with one or a few select accessories but a potentially enormous range of generic devices. This is because most apps are not designed to operate on one particular device but can run on any smartphone or tablet that functions using a given operating system. In order to be truly tested with all potential accessories, such programmes would have to be tested on every smartphone on the market that is capable of running it. In addition, given the versatility of operating systems such as Android, such apps may well be capable of being run on phones that did not even exist when the app in question was created. This apparent impossibility to test the medical device with all available accessories poses significant safety issues. It will be extremely difficult for manufacturers to foresee or avoid problems that arise due to the idiosyncratic nature of each smartphone." (**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

- Embed safeguards on the API of the OS, that it is basically the same for all particular devices such as smartphones, may be helpful for compliance:

> “Even if the designed software is in compliance with the regulations when created, how to guarantee that it will be in compliance with all the smart devices currently available and that will be available in the market.“(**eHealth to mHealth – A Journey Precariously Dependent Upon Apps?**)

References

Council of Europe - **Explanatory Memorandum on the Recommendation on the Protection of Medical Data**. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/EM_R(97)5_EN.pdf

Council of Europe - **Medical Technologies and Data Protection issues - Topics for Questionnaire and Interviews**.

Council of Europe - **Questionnaire on the implementation of Recommendation 97(5) in current member states**.

Council of Europe - **RecR(97)5e - Recommendation on the Protection of Medical Data**. Available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2

eHealth Law & Policy, issue zero, November 2013. Available at: http://www.e-comlaw.com/ehealth-law-and-policy/index.asp

European Medicine Agency updates on development of its policy on publication and access to clinical-trial data. European Medicine Agency. Available at: http://www.ema.europa.eu/ema/index.jsp?curl=pages/news_and_events/news/2013/11/news_detail_001954.jsp&mid=WC0b01ac058004d5c1

Legal frameworks for eHealth: based on the findings of the second global survey on eHealth.
(Global Observatory for eHealth Series, v. 5). World Health Organization. Available at: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

Mantovani, E, Quinn, P., Guihen, B., Habbig, A., Hert, P. **eHealth to mHealth – A Journey Precariously Dependent Upon Apps?** European Journal of ePractice. Vol 20, November 2013. Available at: http://www.epractice.eu/files/p5_2.pdf

Police will have 'backdoor' access to health records despite opt-out, says MP, accessible at: http://www.theguardian.com/society/2014/feb/06/police-backdoor-access-nhs-health-records)

Warsaw declaration on the “appfication” of society. 35th International Conference of Data Protection and Privacy Commissioners. September 2013 Available at: https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*In Switzerland an EHR law will be introduced in 2017/18. It does not cover mHealth.* *In general data protection law limits strongly the collection of sensitive personal data. Databases containing such data must be registered at national authority. In case of violation a fine must be payed.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information

	treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The swiss data protection law does not specify medical data itself. Any insightful data that will be collected of a person systematically will be taken under the category of particularly sensitive personal data and falls under specific regulated limitations. E.g. the person must be informed which data has been collected if the person asks for it. All data must be deleted or if not erroneous must be corrected on demand of this person. Any handover of these data to a third party must be agreed by the person itself. It does not make a difference who is adding the data. In the end it is the obligation of the provider holding these data to do this in line with the law. Collection of any data may only be done if the circumstance of usefulness is given.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	In a treatment relation the patient gives his consent for this specific treatment. All necessary health professionals may have access to these treatment specific healthcare data. *The new law for EHR enables to collect medical data from different treatments. In this context the patient has to define which date may be shared with which health professional.*
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The detailed rules are not yet defined. The idea is to keep relevant data as long as they are useful. E.g. medication data may expire very early whereas immunization data should be kept lifelong
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The rules to ensure the integrity of data are not yet defined. A certification procedure is foreseen to guaranty a certain integrity as well as a high level of security. Strong authentication is foreseen to all users accessing the EHR.

	Anonymous analyses of medical data shall be possible the detailed rules for anonymisation or pseudonymisation are not yet defined.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	A nationwide centralized storage is prohibited. EHR data shall be stored decentralized and only linked with specific keys allowing to split off again a datasources without losing all links to stored medical documents *The standards of security are not yet defined.*
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The rights of access can be exercised via a patient portal/interface where the patient can define his personal access rules to his data. The general swiss data protection law gives the right to any person to have any insightful data deleted or to have erroneous data corrected in any data collection holding insightful data this person. *If the provider does not follow the rules he may be punished by a fine*
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The swiss EHR law is based on a opt-in approach. The foreseen consent is based on 3 levels. *1. the person / patient has to agree that he wants to participate the EHR System and allows in general that useful medical data may be collected from all different sources to his EHR. He/she may not opt-out granular sources or different types. But* *2. the person/patient may select a preferred model (restricted, normal, open) which fits his needs (preconfigured set of access rules). In addition* *3. the person/patient can adjust individualy access rights up to document level and/or individual person to whom he/she wants to show or hide documents. Any data may be declared secret (no access for anybody) or stigmatizing (access for a very limited number of persons). In addition the person/patient may declare different data sources where all data must be declared as secret or as stigmatizing to prevent or limit automatically any access to these documents.* *In this system not the collection of documents is limited only accessing documents will be limited by authorization rules.*
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?

	The person/patient may withdraw at any time the access to a specific document or change rules for users accessing the EHR. The patient/person may hide temporally all his documents to any health professional. As the documents are still exist but marked as secret. These documents may be visible again later on if the person decides to grant access again. *If the patient decides to quit his EHR his record must be deleted according the general data protection law.*
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is common as long as data is held in Switzerland. As in this case sensitive data are passed to a third party the patient/person must be informed to whom this outsourcing will take place. If any sensitive data is outsourced abroad the person must agree/give his consent to outsource abroad. *The company collecting data is responsible to keep compliant even if the operations are outsourced to another party*

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of

care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*The general data protection law limits who may work with sensitive data in that manner, that any third party accessing sensitive data must be declared and announced to the person (data owner). Collecting data must in a useful relation to the object why data had been collected for.* *It does not matter how data are processed or stored. In the end the responsible provider collecting data is responsible to be compliant with the general data protection law. If this provider stores data on a third party system, this provider must declare this to all data owners (patients/persons). In addition the provider may be asked to proof that this data collection is safe and compliant to swiss data protection law. This obligation and the difficulty to proof that data in the cloud are safe and proper segregated from access of any third party will today prevent providers to store sensitive data in the cloud*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing is not specifically regulated. The general data protection law and its rules are applicable. Storing in the cloud means the same as outsourcing to a third party. The provider which outsources to a third party still is responsible and must be compliant with the data protection law. *If medical or sensitive data are made available for a retrieval process, means that many different persons (health professionals) may access medical or sensitive data in a automated way, a special legal basis /framework must be in place.* *To allow an EHR which makes a collection of medical data available for many different persons (health professionals) the swiss EHR law will be introduced in 2017/18*
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?

	Switzerland introduced 2014 a new human research act which regulates in detail the circumstances which data may be used for research, the rules for patient consent as well as what for these data may be used.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes they are allowed to do so if the patient gives his explicit informed consent to work with his genome or if he did not deny explicitly to work with non-genome data. *The government may put the public interest above private interest in given situations (e.g. epidemic) .*
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For medical date see above. As long as non-medical data are not sensitive data, a correlation is allowed.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law says that personal data must be protected against access from third party. A transfer of sensitive or personnel data must be protected by adequate encryption if a relation to a specific person may be done*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID is partially used in hospitals. As long as we know there are no sensitive contents linked to patients. Clinic information systems must be preotected against access from authorized third parties. For these systems the general data protection law is applicable. In addition some cantonal law regulates details how to treat medical data in public hospitals.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*For mobile devices the telecommunications act is applicable.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	There is no specific regulation to use mobile apps to deploy medical services or collecting data. *In the end the data protection law is applicable if any sensitive data is collected. If sensitive data is collected outside of switzerland the patient / person has to give his informed consent to every date (opt in) stored to the database.* *In practice most of the apps are not compliant.*
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Yes they do. For professional apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law).
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	For apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law) *If fitness and daily basis data is used for medical purpose same standards are applicable as for medical devices*

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: ‘any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease’ (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.

Legislation:	For medical devices the remedies act is applicable
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).

eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The remedies act covers all medical devices, software and all subjects which are intended to be used to influence positive a treatment. *Medical devices must not harm patients, must work as promised the positive effect of treatment must be evident and provable.*
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	If the device is not intended for medical purpose, it is not a medical device whereas the remedies act is not applicable. If a seller intends to sell the device for medical purpose the remedies act is a applicable.

	If non-medical data are used within a promise of a medical treatment and the app is sold for medical purpose the remedies act is applicable and the app will be treated as medical device.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	If the device collects sensitive profiles of a person the data protection law or/and the telecommunication act are applicable.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	It depends for what purpose the seller introduces the product. If the seller positions his product for medical purpose, it falls under the remedies act and will be treated as a medical device, independent of the collected data.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law is applicable if any data profiles are built up*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Security:	What are the security standards that need to be employed by these devices when collecting personal data?

	Not directly specified. An appropriate security standard depending on the confidentiality of the collected data / profile must be achieved. Some minimal standards are defined.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Yes it is allowed as long as these devices are not intended to be for medical purpose. It is allowed to cross medical with non-medical data as long as no profile are built-up. If a behavior profile is built up or if collected medical data have an impact on privacy to this person or are linked to a person and a medical result may be interpreted these data become sensitive. On collecting sensitive data the general data protection law is applicable.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	It depends in the collected data, the concept privacy by design is not known in swiss regulation.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The telecommunication act is applicable. If any medical advice or result is produced by a software which is intended for medical purpose the remedies act is applicable as well.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?

	In general a medical treatment is allowed via online service but the health insurances are not allowed to pay for medical services within the regular insurance model.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	There are no specific requirements, in general a medical doctor has to document the anamnesis, his decisions and treatments independent if he treats face to face or via online service.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

Urs Stromer, Walter Stüdeli, IG eHealth (info@ig-ehealth.ch)