Strasbourg, 2 June 2014

T-PD-BUR(2014)04rev

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

(T-PD-BUR)

MEDICAL TECHNOLOGIES AND DATA PROTECTION ISSUES- FOOD FOR THOUGHT[1]

Directorate General Human Rights and Rule of Law

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

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 to better identify the situations which are concerned, and related problematics.

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:

> "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