Paper

Connecting for Surgery: The Belgian Use Case on the Legal Aspects of the Digital Operating Room

Niels Vandezande, Griet Verhenneman, and Jos Dumortier

Interdisciplinary Centre for Law & ICT – iMinds, Faculty of Law, KU Leuven, University of Leuven, Leuven, Belgium

Abstract—Telecommunications technology is making its way into operating rooms by new developments in e-health. However, conflicts arise with existing legal principles regarding data protection. This paper deals with key elements of the interactions between data protection and evolution in e-health. The scope will be the digital operating room, where different health services and activities converge through networked technology, raising a number of privacy-related issues. For instance, the patient's health records and tools for recording surgical procedures could be integrated within the same platform, potentially leading to sensitive personal data linkage. Also the possible duration and reason of storage of surgical recordings, is a matter that remains largely unresolved in current practice. First, this paper will analyze the data exchanges of the digital operating room. As these will include personal patient data, it must be assessed whether and how the European framework on data protection can apply. Second, the regulatory regime of the manufacturers of the devices of the digital operating room will be analyzed. Can the current legal framework relating to e-health provide for suitable regulation for such devices? Drawing from experience gained in research projects, this paper aims to provide practical answers to often theoretical questions.

Keywords—data protection, e-health, privacy, telecommunications.

1. Introduction

The nature of the Internet has undergone a number of drastic changes in the last few years. One of the most notable of such changes is the rise of what is referred to as the *Internet of Things*. This phenomenon can be described as being the pervasive and ubiquitous interconnecting of all kinds of everyday objects or rather: "things" that can interact with each other and cooperate to achieve common goals [1]. Relying on the use of new communication technologies including radio-frequency identification (RFID) and near-field communication (NFC) the *Internet of Things* aims to support data exchanges in the global supply chain, facilitating several aspects of daily life [2]. On a global scale, the *Internet of Things* could help track the movement of the many goods that are being transported every day, potentially supporting the identification of counterfeit goods. On a more personal level, a smart refrigerator could detect when it is running out of milk and add this item to the groceries list. This growing number of interconnections between ever more devices will of course result in further growth of the number of services that is already provided online. Also, the amounts of data exchanged in networked environments can be expected to increase exponentially.

Also in the field of healthcare, different kinds of services are gradually moving towards networked environments. In a first wave of e-health solutions, paper records were digitalized into electronic health records that could be shared between healthcare providers. A next step is to use the Internet as a medium for the delivery of healthcare services. As diagnostic services in the fields of pathology and radiology, for instance, are already widely delivered over the Internet, this step is very much unfolding right now. This use of the Internet for telemedicine purposes is only expected to grow, with trials already taking place in fields like nursing, pharmacy and even surgery.

The delivery of such telemedicine services requires the tools and devices that are equipped for use in a highly networked environment in which many services are provided over a distance. Especially in the field of telesurgery, this evolution requires an update to the regular equipment found in the current layout of operating rooms. In what can be regarded as a digital operating room, several types of services such as the provision of health data and the monitoring of vital statistics and different components such as cameras, wires and surgical tools will have to be integrated into a single device that is equipped to handle the data flow with which it will interact.

This convergence of different e-health services, relating to the use, transfers and storage of data can, however, also raise questions with regards to the protection of such data. Especially when the patient's health data is involved, it will have to be assessed what measures need to be taken to protect the patient's privacy. This paper aims to address the specific privacy issues that arise in the context of a digital operating room from a legal point of view. First, it will have to be addressed whether the current legal framework regarding data protection can be applied to the technological developments of the digital operating room. This analysis will shed further light on how the services expected from future e-health developments can be affected by this legal framework. In secondary order, this paper will address the regulatory regime applicable to the manufacturers of the devices of the digital operating room. More specifi-

cally, it will be analyzed whether these manufacturers can be subjected to the stricter regulations that generally apply to medical devices.

2. Applicability of the Data Protection Framework

The data exchanges envisioned within the digital operating room will be performed in a sensitive environment. The health records of patients will be handled, a number of persons will execute divergent tasks and a high degree of trust is bestowed onto the proper functioning of the devices that enable the use, exchange and storage of all data generated in the performance of the activities of the digital operating room. The collusion of these different factors raises a number of legal questions with particular regard to the protection of the patient's personal data. Therefore, it will first have to be assessed whether the current legal framework regarding data protection can be applied to the activities of the digital operating room.

Within the European Union, the legal framework relating to the protection of personal data relies on Directive 95/46/EC, also known as the *Data Protection Directive* [3] and the national implementations thereof by the Member States. This directive applies to the processing of personal data, whereby personal data needs to be understood as being any information relating to an identified or identifiable natural person. Important for the determination whether a piece of information constitutes personal data, is therefore whether this information can identify a natural person or at least make him identifiable. A person will generally be considered to be identified when his identity can be confirmed immediately so that he can be singled out from a group. This is the case with, for instance, public sector identification numbers, such as the identification number of a national identity card, which are supposed to be uniquely assigned to one citizen only. As a result, every one of such identification numbers will directly and solely identify one citizen.

The concept of identifiability, however, may raise more discussion. According to the *Data Protection Directive*, a person is identifiable when he "*can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". In this case, the citizen will not be identified immediately, but a number of elements, or a combination thereof, may lead to the indirect identification of the citizen. In such case, he will be considered to be identifiable [4]. As this broad definition encompasses an enormous amount of different elements and factors of information, it is clear that there is only a limited amount of information that could not be considered as personal data.

When information relates to a citizen, but cannot in any possible way be traced back or linked to that citizen, this information is considered to be anonymous [5]. It should be noted, however, that there is only a very limited amount of data that is truly anonymous. Even when certain information has been depersonalized or encoded, it could still contain information that could be traced back to the citizen, thus making the citizen identifiable and therefore making the information personal data.

In the context of the digital operating room, this could have implications for the recordings made during surgeries. In, for instance, an endoscopic procedure, the recorded images will mainly show a patient's abdominal and pelvic cavity. It is clear that these images alone will in most cases not be able to lead to a direct identification of the patient, unless the images show a specific disease or deviation that is so rare and recognizable that it leads to a specific patient. In that sense, the images recorded are generally not able to directly identify a patient. However, they could still make a patient identifiable, if they can be linked to other information that could lead to the effective identification of the patient. For instance, if the recorded images are stored or in one way or the other linked to the patient's electronic health record, they could be traced back to a specific patient. Also if the filename of the recorded images or the metadata stored in it makes any referral to information that could identify the patient, the recorded images will be considered as personal data under the European Union legal framework regarding data protection.

It can therefore be found that caution should be paid to the broad scope of application of the current legal framework on data protection. Even when particular data does not seem to identify a specific patient, the accompanying metadata and the way in which the data is handled, could still make the patient identifiable. Such would lead to the conclusion that personal data is processed in the digital operating room and that therefore the *Data Protection Directive* will be applicable to such data flows.

3. Recording, Storage and Later Use of Data

One of the main aspects of future e-health developments is that the use of pervasive and ubiquitous network infrastructures in the digital operating room will lead to a substantial growth in the amount of data that is generated during surgery. Such data will then also become more easily subjected to storage thereof in centralized servers. When stored, data could potentially be used at a later stage, for a variety of purposes. For instance, laparoscopic images recorded during surgery could potentially serve educational purposes. Alternatively, such images could also be stored in the patient's electronic health record. Vital statistics of the patient during the course of a surgery could also be added to that same electronic health record to provide a more complete account of how the procedure went.

These aspects, however, all hold considerable concerns under the applicability of the legal framework on data protection. In the following, it will be analyzed how the ap-

plicability of the *Data Protection Directive* influences the recording, storage and later use of personal data in the context of the digital operating room.

3.1. Recording Data

With regards to the recording of data including vital statistics and surgical images during surgical procedures, the first question to be answered is whether the patient's specific consent is needed to this end. Specific consent for the recording of data during a surgical procedure could be found unnecessary because it is assumed to be part of the surgery itself, to which the patient already consented. Such idea of "one consent fits all" should of course be treated with care as consent principally needs to be specific [6]. The patient can therefore not be assumed to have given his consent to the recording unless he was already clearly informed on this when giving his consent to the procedure and if the recording would fit within the scope of the purpose of the procedure itself.

This strict interpretation of consent, however, does not accommodate the importance of research in advancing medical practice. Medical research – including personal data processing – can benefit public health by identifying patterns of diseases and finding new treatments [7]. To facilitate such later research, it could be argued to have the patient provide a broad consent aimed at providing a legal ground for future research. But as such future research may not yet be designed or performed for months or years to come [8], it becomes difficult to provide the specific information required by the patient in order to provide his informed consent. Indeed, the broader and more general the information given to the patient, the less informed his consent will be, thus no longer satisfying this requirement in personal data processing [9]. As a result, broad consent, despite its importance for the medical and scientific community, can be considered as problematic from a legal point of view.

Specifically asking consent for surgical recordings could also be found unnecessary if the patient is considered to be unrecognizable on the recordings made by, for instance, an endoscopic camera. However, as indicated before, there are other ways in which such information could make the patient identifiable, such as when the recording's metadata could be linked to the patient's unique health record. Such would still qualify the recordings as personal data, thus requiring consent or another justification ground before being allowed to be processed. It should therefore be stressed that consent is in principle required for the recording of data during any surgical procedure and that such consent cannot just be assumed from the patient's general consent to the surgical procedure in itself. As genuinely anonymous data is extremely rare, it would be advisable to seek specific consent for the recording of surgical procedures.

This means that the patient needs to be informed on the purposes of such processing, the duration of the storage thereof, etc. Given the benefits of an integrated approach, the patient's consent to the recording could be given at the same time as his consent to the surgical procedure in general, but needs to be clearly differentiated thereof.

3.2. Storage of Data

In past times, operating rooms could be considered as isolated islands, where during a surgical procedure nothing could get in or leave. The use of networked equipment in the digital operating room will provide a direct and constant connection to the outside network, thus providing opportunity to send and receive information in realtime. One possibility that can be envisioned here is the direct recording of surgical images and the storage thereof on the hospital's network. Such storage is a practice already found in hospitals today [10] and should therefore be addressed from a legal point of view.

First, this practice raises questions with regards to the duration of the storage of what can be considered as being the patient's personal data. As can be found in the legal provisions of the data protection directive, personal data collected for processing cannot be stored longer than necessary for achieving the purposes for which they were collected. This means that personal data storage needs to have a clearly defined end-point, after which the data needs to be deleted. Apart from the specific purposes of the processing, the end-point of health data storage will also be determined by other factors. For instance, Belgian law requires patients' files to be stored for thirty years since the last contact between the healthcare professional and patient [11].

An important factor in the usefulness of such data storage is the advancement of the medical state of the art. As surgical practices and procedures are continuously improving, it would not make sense to use a particular recording of a procedure for a long period of time, as it will eventually show outdated practices and procedures. It would therefore seem advisable to predetermine a specific duration for the storage of recorded surgical procedures.

On another note, the storage of what can be regarded as personal data also requires the implementation of specific measures aimed at safeguarding the security and confidentiality of such data. Security can generally be understood to include a number of aspects [12]. Integrity, for instance, ensures that processed information remains accurate and that no unauthorized modifications are made. Also, availability ensures that the data is readily accessible and usable. Additionally, one can refer to data origin authentication, which guarantees the origins of the data and non-repudiation, which ensures that actions committed cannot be denied by their performers [13].

The general obligation to ensure personal data security requires the data controller to ensure an appropriate level of security taking into account the current technical state of the art, the cost of implementing such measures, the nature of the personal data to be protected and potential risks. As the digital operating room includes the processing of health data, the appropriate level of security should

be considered to be high. While the current non-digital OR also includes the processing of health data, it is precisely the advanced degree of interconnection between different devices in and outside of the OR that makes the Digital OR a more risk-bearing environment. Patient records are no longer physically transported from a secured archive to the OR when required, but can be consulted electronically at all times from anywhere in the hospital. Also the higher data flow resulting from the convergence and interconnection of equipment that is currently still used "offline" will augment the risk potential, for instance in terms of data breaches.

The *Data Protection Directive* calls for technical measures of security, which includes the physical protection of the personal data by ensuring that non-authorized people cannot get access to this data [5]. This is, however, an important problem in hospital settings, as most areas are open for public access and mobile devices are often not properly stored. Physical data security would therefore in this context also require a change in attitude of the actors involved. Therefore, more purely technical measures are also to be considered, such as protecting the devices and applications by encryption and passwords. Such would ensure that unauthorized people cannot get access to the personal data, even if they would get physical access to the devices containing or being able to access such data. More organizational measures include raising staff awareness and responsibility with regards to data security. As an obligation of means, the data controller is bound to deliver his best efforts rather than a specific result and must therefore demonstrate that he delivered the effort that another diligent controller would have delivered under the same circumstances.

Confidentiality requires the data controller to limit the access and processing competencies of the actors under his authority [5]. This duality requires the personal data to be off limits for unauthorized persons, but also holds that authorized persons cannot be given unrestricted access. In general, access to the personal data must be restricted to what the properly authorized persons need to know for performing their respective duties. For access provision, a regular authentication procedure can be followed [14]. This includes registration of the authorized persons, after which they can present their identification. Such identification can be made by information known only to the user such as passwords or by tokens only held by the user such as an identification card. Following the authentication verifying that the claimed identity is real the person will be authorized and granted access. Such authorization could be leveled, ensuring that a particular user is only granted access for as much as his role demands. Actors executing higher demanding roles will be given higher levels of access rights. Categorizing the patient's personal data can be useful in developing a modular access matrix. Logging and tracing mechanisms can be used to verify whether appropriate access levels were given and whether only properly authorized users accessed the data corresponding to their level of demand.

Additionally, with regards to education, employees should be instructed on their applicable organizational security policies and the importance thereof [5]. Given the particular status of healthcare work, employees should not only be instructed on general data protection requirements, but also on requirements stemming from their status as health professionals. One requirement is that health data must be obtained at the patient and can only be processed under the responsibility of health professionals, unless otherwise consented to. Also, given the importance of the networked infrastructure of the digital operating room, it is important to ensure that these networks are adequately secured in order to guarantee the security and integrity of the data transferred over them.

3.3. Later Use of Data

One of the main reasons to store data is to preserve the possibility of using such data at a later stage. According to the *Data Protection Directive*, personal data can only be used for the specific purposes for which it was collected. As a result, personal data collected for a specific and justified purpose cannot be used at a later stage for purposes that are irreconcilable with the purposes for which the data was first collected.

To judge whether the original and subsequent purposes of the data processing are reconcilable, all relevant factors need to be taken into account, in the first place the data subject's reasonable expectations. The difference between original use and later secondary use needs to be stressed in the context of the digital operating room as well. If, for instance, a surgical procedure is recorded for a specific purpose, then later use of those images will have to be reconciled with the original purposes for which the procedure was recorded. If such secondary use cannot be reconciled with the original purposes, the secondary use will have to be treated as a new processing, thus requiring the fulfillment of all data protection requirements such as consent, purpose statement, etc.

Further processing of data for historical, statistic or scientific purposes is principally not considered to be irreconcilable and will therefore be allowed, be it under specific conditions. To make this matter more concrete, the Belgian use case will be presented as an example of how the further processing of personal data can be regulated. Note, however, that this regulation may differ across the European Union. The reason for this is that there are no harmonizing legal instruments on this matter, apart from the *Clinical Trials Directive* [20].

In the Belgian use case, the Royal Decree of 13 February 2001, executing the *Belgian Data Protection Act*, deals with the concept of further processing for historical, statistic or scientific purposes [15]. In general, Article 3 of the Royal Decree prefers that anonymous data is used. As such data cannot be linked back to a specific data subject, it is by definition no personal data and therefore can be processed further. If anonymous data cannot suffice to satisfy the purposes of the processing, Article 4 of the Royal Decree

calls for the use of encoded data. This is data that can be linked to a specific data subject, but only by means of a code. Only when also encoded data does not satisfy the purposes of the processing, Article 5 allows the use of non-encoded personal data.

Note that there are three scenarios imaginable [16]. If personal data is primarily collected for historical, scientific or statistic purposes as original purposes of the processing, the use of this data for these historical, statistic or scientific purposes is no secondary use and therefore all sorts of specific national regulations relating to the issue of further processing such as the Belgian Royal Decree will not apply. If the data is collected for other purposes and used in secondary order for historical, scientific or statistic purposes that are reconcilable with the original purposes, the Royal Decree will also not apply as there is not incompatibility between the original purpose and the purpose of the secondary use for historical, statistic or scientific purposes. The Royal Decree only applies when data is collected for specific purposes and later used secondarily for historical, scientific or statistic purposes that are not reconcilable with the primary purposes.

4. Device Manufacturer Regulations

Apart from addressing the main concerns resulting from the application of the principles of the *Data Protection Directive* to the developments of the digital operating room, this paper also aims to look at this matter from the perspective of the manufacturer of the devices that make up such digital operating rooms. In the following, it will be analyzed to what regulatory regime such devices and their manufacturers are subjected.

While general healthcare regulations are mostly aimed at establishing the rights and responsibilities of patients, medical professionals and medical institutions such as hospitals, one should not forget about the legal position of the manufacturers of the many products that enable or facilitate the provision of healthcare, including the devices and applications that will play a role in the digital operating room. The reason why these product manufacturers are typically not included in general healthcare regulations is that they normally do not directly engage in contracts with the patient. Medical professionals or institutions engage with product manufacturers through contracts spanning from regular sales of goods contracts to elaborate service contracts that are mostly governed by standard contract law. Direct contact between patients and product manufacturer is generally only found in certain cases of the manufacturer's liability for faulty products.

However, certain sectors apply specific rules to manufacturers that aim to bring products on the market in that sector. Especially in the healthcare sector, one can understand the need to preserve certain standards of quality. Surgical scalpels and hypodermic needles need to be fully sterile, monitoring and diagnostic equipment needs to be reliable, etc.

At the level of the European Union, a number of directives provide the basic legal framework that needs to ensure a high level of quality of medical devices in order to guarantee the protection of human health and safety. Such directives provide basic lists of requirements that need to be met before medical devices can be put on the market. When devices are marketed, they must also bear the CE mark as a proof of certification, although self-certification is possible in certain cases. Devices are divided over four categories (I, IIa, IIb and III) according to the risks their use poses to the patients. The criteria used for such classification take into account the invasiveness of the device, the intended duration of its use, whether the device is active or passive, etc. [17].

While such requirements listed do provide a basic idea of what one should be able to expect from a compliant medical device, there are virtually no technical details included. For instance, it is stated that devices delivered in a sterile state must be manufactured and sterilized using an appropriate and valid method, yet apart from a reference to standards developed by standardization bodies such as the International Organization for Standardization (ISO) it is left open to interpretation by the Member States to further define such method. As a result, Member States need to incorporate and further develop these requirements in their national legal system. A Competent Authority reporting to the Minister of Health will be formed in all Member States to monitor the adoption and application of these principles.

In Belgium, the Federal Agency for Medicines and Health Products (FAMHP) evaluates, approves, follows and controls the requests for clinical trials for medicines and health products. This agency follows medical devices and medicines from their R&D phase to their introduction on the market and performs inspections to ensure the quality of these devices and medicines. Every product manufacturer aiming to bring a medical device or medicine to the Belgian market will therefore have to apply to the FAMHP. To this end, medical devices are defined as any instrument, equipment, material or other article used on its own or jointly, including software required for it to function correctly, which is intended by the manufacturer to be used on humans for the purposes of diagnostic, prevention, control, treating or diminishing an illness, an injury or a handicap, of studying, replacing or modifying part of the anatomy or a physiological process and of controlling conception and whose principal intended action in or on the human body is not obtained by pharmacological or immunological means or by metabolism but whose function can be assisted in such a way [18]. This includes accessories specifically intended by its manufacturer to be used with a device to enable the use of that device in line with the instructions of the manufacturer of the device.

Given this broad definition, taken literally from the European Union directive, the scope of the regulatory competence of the FAMHP spans from the simplest of tools such as tongue depressors to much more complex diagnostic and

monitoring devices and computer systems. The devices envisioned in the digital operating room and their accessories may therefore also have to comply with the existing regulations applied by the FAMHP.

Taken that a digital operating room could be defined as including the development of technologies for central external monitoring equipment and the network infrastructure that enables image distribution and collaboration, it will have to be assessed whether such can fall under the scope of the FAMHP. Here, Article 7 of the Royal Decree of 18 March 1999 refers to system manufacturers as "*all natural or legal persons reassembling devices with a CE marking, depending on their destination and the limitations of use granted by their manufacturers, in order to launch them as a system or a kit*". Such systems are subject to a mere notification and do not need to go through the whole certification procedure. However, if the system contains components that do not carry the CE mark or if they are used in a manner incompatible with their originally intended use, the system is considered as a separate medical device, thus subject to the standard procedure. As the digital operating room would integrate different medical devices into a central hub, such hub could be considered as a system. The envisioned network infrastructure for image distribution and collaboration will also be integrated in this hub and will be used in collaboration with medical devices, thus becoming part of the medical system. As the central hub in itself will not directly come into contact with the patient, it could be seen as a "Class I medical device".

Looking at the Belgian use case, one will have to refer to the Act concerning *Experiments on the Human Person* [19]. While this act is the Belgian implementation of the so-called Clinical Trials Directive [20], the Belgian legislator has chosen to expand the scope of the directive from "*clinical trials, including multi-centre trials, on human subjects involving medicinal products*" towards every type of experiment involving human subjects with the goal to expand knowledge on medical practices. As a result, every test, study or research involving human subjects that is aimed at expanding knowledge on the practices of health professions will be subjected to the scope of this act. Given this broad definition, one will have to assess whether trials concerning the digital operating room hub or other applications would constitute an experiment under the scope of the Act concerning *Experiments on the Human Person*.

While tests should be understood as referring to medicinal products, studies and research also apply to non-medicinal trials. However, nor the act, nor the preparatory works provide a clear definition of these trials. The act does, however, refer to medical devices [19]. Like trials involving medicinal products, studies and research focusing on medical devices should receive a positive advice from an ethical committee and from the Minister of Health. More concretely, it could be argued that one should follow the procedure stated in the Royal Decree on medical devices, which leads to notification to the FAMHP, as discussed before.

Two other conditions that need to be fulfilled for the application of the Act concerning *Experiments on the Human Person* include the goal to expand knowledge on medical practices and the involvement of human subjects. If the experiment is aimed at advancing the state of the art in medical practice, then the condition of knowledge expansion will be fulfilled. The condition of human involvement is fulfilled as soon as the experiment physically involves a born and living human subject. The mere processing of his personal health data, for instance, will not lead to the application of this act. When the Act concerning *Experiments on the Human Person* applies, the human subject participating in the study or research will have to grant his written prior informed consent [19]. He also enjoys specific protection, such as that that experiment needs to abide by the proportionality principle that risks and benefits need to be weighed off against each other, etc. Further responsibilities and liabilities are imposed on the promoter.

5. Practical Consequences

While the previous sections discuss the more theoretical aspects of this matter, the question remains what this means in practice. How are professionals in the telecommunications sector affected by the advent of telesurgery practices? Which dangers need to be heeded when engaging toward the implementation of a Digital OR solution? This section will summarily consider the practical implications of the evolutions discussed here. First, it is reminded that device manufacturers must comply with European and national legislation in order to deliver medical devices. Second, data protection concerns must be taken into account. Third, potential liability issues need to be minded.

5.1. Device Regulations

The manufacturers of the devices, tools and applications of the Digital OR must assess whether their product can constitute a medical device according to existing legislation in this field. As this legislation is not very much harmonized at the level of the European Union, it must be ensured that both the scarce European legislation in this field – for instance concerning the requirement to bear the CE mark – and the applicable national legislation of the Member States are complied with. In most cases, this will entail a submission to the competent national agencies concerned with monitoring medical devices and medicines. Only when the applicable rules and procedures are complied with and authorization – where required – is obtained, the medical devices can be offered to customers in the healthcare sector.

5.2. Data Protection

As noted before, the devices of the Digital OR are becoming more interconnected, meaning that devices that used to

perform their tasks isolated from other devices are increasingly becoming part of a network of data exchanges. Even a simple heart rate monitor could be modified to record its readings – or anomalies in particular – and store them on the centralized hospital network. The result of this is that the data flows in the Digital OR are very likely - or even certain - to involve personal data processing operations. These data flows and the subsequent use of that data must therefore comply with the requirements of European and national data protection legislation.

More concretely, this means that it is important to determine who will serve as the data controller to that personal data processing operation, as such data controller will hold the final responsibility over the processing. This data controller will have to determine the purposes of the processing, the duration of storage, ensure that no data excessive to the purposes is processed, etc. Another pivotal element to a fair and lawful processing of personal data is that of the legitimate justification ground. While specific justification grounds do exist for use in a medical context – for instance in case of medical urgency – the patient's consent will undoubtedly serve as the most important justification ground. Health data is considered to be sensitive personal data and the processing thereof must therefore comply with stricter regulations. At European level, for instance, it is stipulated that consent for the processing of sensitive personal data must be explicit. National implementations of this provision, however, may differ. In Belgium, for instance, written consent is required [3]. Another duty of the data controller is to ensure that the patient's rights as a data subject are respected and that proper notification is made to the competent national *Data Protection Authority*.

The data controller is defined as the party to the processing that decides the means and purposes of that processing. Within the context of the Digital OR, this will generally be the surgeon, or even the hospital. While recent evolutions make it difficult to apply static concepts such as that of data controller to complex data processing operations, it is clear that this role belongs to a medical professional and principally not to the manufacturers of medical devices. However, the fact that the hospital and the health professionals principally share the burden of the task of data controller does not mean that other parties, such as the device manufacturers do not need to mind data protection rules. If these manufacturers become involved in performing the processing on behalf of another party, they could still be considered as processors. If, for instance, a medical device assists in the processing of personal data, its service provider could be viewed as a processor if his device only serves as a means for the processing. And if the device requires additional data to be processed, it could even be viewed to determine the purposes of the processing as well, thus leading to its service provider becoming a (joint) controller [4]. Device manufacturers are therefore advised to clearly define their role within the personal data processing operations their devices will become involved in.

5.3. Liability

The manufacturers of the devices of the Digital OR will also have to mind potential liabilities for their products. Under general contract law, these manufacturers are bound to a duty of conform delivery, meaning that their products need to be without visible or hidden flaws and that they must live up to the expectations of the product agreed upon. Especially in a medical context, devices will need to demonstrate a high degree of reliability.

Outside of the strict contractual framework, product manufacturers can also be held liable for damages caused by their faulty products. This product liability can be considered as an objective liability, as it does not require a fault on the manufacturer's behalf. The party suffering damages will only have to prove that those damages were caused by a fault in the product. Given the extra-contractual nature of this liability, it serves as a means for patient to direct a claim for compensation for damages sustained directly to the product manufacturers, as they will generally not have entered into a contractual bond with this party.

By converging different services into fewer devices, the Digital OR is a much more complex environment. Device manufacturers will need to adapt to these complexities and ensure that their products are compliant to the standards expected in the medical sector.

6. Conclusion

Technological developments such as the *Internet of Things* will soon make their way into hospitals worldwide. In what can be referred to as the digital operating room, different devices will become interconnected and will create, store and exchange data on a larger scale than has ever been possible before. Such data flows can, however, also pose concerns with regards to the patient's privacy. To this end, this paper has first analyzed the applicability of the current legal framework on data protection to the data flows that can be found in such digital operating room. Here, the focus was put on the concept of identifiability. As the *Data Protection Directive* requires the data subject to the identified or to be reasonably identifiable in order for data to be considered as personal data, it is precisely this concept of identifiability that can determine the true scope of the notion of personal data. Indeed, in this context it was found that data that is often considered not to identify a patient and thus to be anonymous can still be used to lead to the identification of a particular patient, when coupled with other data such as metadata or when linked to the patient's health record. The applicability of the *Data Protection Directive* should therefore always be assumed, given the broad spectrum of its applicability. In particular, this paper focused on the recording, storage and later use of data in the digital operating room. Here, it was found that such data recording principally requires additional specific consent from the patient. Also the storage is bound

to particular requirements, such as that of limited storage duration and the adoption of specific security and confidentiality measures. When data is stored for future use, it needs to be ensured that such secondary use can be reconciled with the primary purposes for which the data was collected. Finally, with regards to the status of the manufacturers of the devices of the digital operating room, it was found that such devices can fall under the specific status of medical equipment, which means that they may have to comply with a number of specific requirements following from the sensitive nature of such equipment.

Acknowledgements

This research was performed as part of the *Telesurgery project*, funded by iMinds and the Flemish government agency for Innovation by Science and Technology (IWT).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Comp. Netwo.*, vol. 54, pp. 2787–2805, 2010.

[2] R. Weber, "Internet of things – Need for a new legal environment?", *Comp. Law Secur. Rev.*, vol. 25, pp. 522–527, 2009.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281 of 23 November 1995, pp. 31–50. In Belgium, this directive has been implemented as: Act of 8 December 1992 on the protection of the privacy against the processing of personal data, *Belgian State Gazette*, 18 March 1993 (Data Protection Act).

[4] C. Kuner, *European Data Protection Law*. Oxford: University Press, 2007.

[5] D. De Bot, *Verwerking van Persoonsgegevens*. Antwerpen: Kluwer, 2001.

[6] Article 2(h) Directive 95/46/EC.

[7] Academy of Medical Sciences, *Personal data for public good: using health information in medical research*, London, Academy of Medical Sciences, 11–12, 2006.

[8] T. Caulfield, R. Brown, and E. M. Meslin, "Challenging a Well Established Consent Norm?: One Time Consent for Biobank Research", *J. Inte. Biotechnol. Law*, vol. 4, pp. 69–74, 2007.

[9] V. Arnason, "Coding and Consent: Moral Challenges of the Database Project in Iceland", *Bioethics*, vol. 18, pp. 41–42, 2004.

[10] S. Elprama, P. Duysburgh, and A. Jacobs, "TeleSurgery D1.3.1 – Draft Desk and Key Observational Informant Research on Everyday Surgical Practices", *IBBT*, 2011.

[11] Article 1, 3 Royal Decree of 3 May 1999 defining the minimum requirements of the medical record, as defined in article 15 of the Act on hospitals coordinated on 7 August 1987, *Belgian State Gazette*, 30 July 1999.

[12] B. Van Alsenoy *et al.*, "GINI D3.1 – Legal Provisions for Deploying INDI services", pp. 29–30, 2011 [Online]. Available: www.gini-sa.eu

[13] S. Pearson and A. Charlesworth, "Accountability as a way forward for Privacy Protection in the Cloud", in *Proc. First Int. Conf. Cloud Computing*, Beijing, China, Dec. 2009, pp. 131–144.

[14] X. Huysmans, "Identity Management for eGovernment – Deliverable 1.2 Conceptual Framework", *IBBT*, 2005.

[15] Royal Decree of 13 February 2001 executing the Act of 8 December 1992 on the protection of the privacy regarding the processing of personal data, *Belgian State Gazette*, 13 March 2001.

[16] J. Vandendriessche, "De verwerking van persoonsgegevens voor historische, statistische en wetenschappelijke doeleinden", *TBBR*, vol. 9, pp. 534–543, 2006.

[17] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, *Official Journal* L 169 of 12 July 1993, pp. 36–40.

[18] Act of 25 March 1964 on medicines, *Belgian State Gazette*, 17 April 1964.

[19] Act of 7 May 2004 concerning Experiments on the Human Person, *Belgian State Gazette*, 18 May 2004.

[20] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, *Official Journal* L 121 of 1 May 2001, pp. 34–44.

Niels Vandezande is a Legal Researcher at the Interdisciplinary Centre for Law & ICT – iMinds, Faculty of Law, KU Leuven-University of Leuven, Belgium. He obtained his Master of Laws degree in 2009 at the same university, focusing on ICT-law, international law and corporate law. He currently conducts research in the fields of data protection, privacy, security & trust and public information availability. For his Ph.D., he researches the legal value of electronic information.
E-mail: niels.vandezande@law.kuleuven.be
ICRI – KU Leuven
Sint-Michielsstraat 6 (B3443)
3000 Leuven, Belgium

Griet Verhenneman is a Research Associate at the Interdisciplinary Centre for Law and ICT (ICRI), KU Leuven since 2007. She is working on different Belgian and European research projects with a strong focus on eHealth. She is preparing a Ph.D. on the patient's right to privacy and autonomy in a changing healthcare environment, an environment based on disease management techniques supported by ICT tools. She is also a part-time professional support lawyer at Time.Lex law firm where she deals with eHealth and privacy protection.
E-mail: griet.verhenneman@law.kuleuven.be
ICRI – KU Leuven
Sint-Michielsstraat 6 (B3443)
3000 Leuven, Belgium

Jos Dumortier is a Professor in Information Technology Law at the Faculty of Law, KU Leuven since 1989 and the founder and director of the Interdisciplinary Centre for Law and ICT since its start in 1990. He is also the co-founder and partner of Time.Lex, a Brussels-based law firm specializing in commercial, ICT and intellectual property law. Prof. Dumortier has been closely involved in the drafting of the Belgian personal data protection law and works regularly as an expert for the European Commission. With his research team in Leuven and his law firm in Brussels he has authored many European studies in the field of information security and data protection law.
E-mail: jos.dumortier@law.kuleuven.be
ICRI – KU Leuven
Sint-Michielsstraat 6 (B3443)
3000 Leuven, Belgium