Emiliano Casalicchio[1], Sebastiano Filetti[2], Sabrina Grigolo[3], Luigi V. Mancini[1], Alessandro Mei[1], Giulio Pagnotta[1], Alice Ravizza[4], Angelo Spognardi[1], Silvia Stefanelli[5]

Data protection and cybersecurity in digital therapeutics

1. Data protection profiles in digital therapeutics

Digital therapeutics (DTx) consist of clinically validated software that carries out a therapeutic function. In other words, a DTx product processes incoming data and generates output data that can influence the patient's behaviour, thus providing a clinical benefit (e.g., an app which provides indications to the patient, with a view to addressing sleep disturbances).

In terms of legal classification, DTx come under the heading of "medical devices", pursuant to Article 1(a) of Directive 93/42/CEE (superseded, with effect from May 2021, by the definition of medical device set forth in Article 1(2) of the new Regulation (EU) 2017/745, more often referred to simply as the MDR). Therefore, manufacture and placing on the market of DTx have to comply with the regulatory requirements set out in the MDR.

As regards their intrinsic mode of operation, DTx function by processing data related to the patient's health that come under the heading of "*particular categories of data*" (according to Art. 4(15) of Regulation (EU) 2016/679, also known as the EU GDPR). It will therefore be necessary to analyse the legal profiles related to this type of processing in the light of the GDPR.

[1]*Computer Science Department, Sapienza University, Roma*
[2]*School of Health, UnitelmaSapienza, Roma*
[3]*European Patients' Academy/EUPATI Non-Profit Organization*
[4]*Use-Me-D, Torino*
[5]*Stefanelli & Stefanelli Legal Chambers, Bologna-Milano*

On the following pages, for reasons of space, we will examine only the main issues concerning detailed processing profiles related to DTx, without dwelling on the general profiles set out in the GDPR.

1.1 Roles and responsibilities in data processing

The first question to focus on is the identification of the different roles and responsibilities in data processing. In other words, which natural person or legal entity will be qualified as the data controller? And, downstream from that, where do other roles and responsibilities lie?

Pursuant to article 4(7) of the GDPR, the data controller is the natural person or legal entity that determines the *"purposes and means of processing"* and bears the general legal responsibility for guaranteeing correct data processing.

Based both on general interpretation of the discipline and the recent European Data Protection Board's *"Guidelines 07/2020 on the concepts of controller and processor in the GDPR"* (draft issued on 7 September 2020), it can be stated that the role of the data controller and, in general, all other roles within GDPR cannot be defined *a priori*, but depend on concrete data processing profiles.

In practice, attention must be paid to who concretely determines the purposes of the data processing and its concrete modalities.

Regarding DTx, we can identify two hypotheses:

- In the first hypothesis, the data controller is the healthcare organization or individual doctor who prescribes the DTx.

In this case, the DTx manufacturer will presumably be appointed as the data processor pursuant to Article 28, as the party that stores and organizes the data (though, in this case, admittedly not empowered to define the purposes of processing). However, it should be noted that the DTx manufacturer will nonetheless also qualify as data controller for all closely related processing activities, notwithstanding the role of data processor, and will have to process the data for some purposes that the MDR identifies as the medical device manufacturer's domain - e.g., postmarketing surveillance (Article 83 MDR), analysis of serious incidents and field safety corrective actions (Article 89 MDR).

- In the second hypothesis, the DTx manufacturer qualifies as the data controller and will, therefore, bear full responsibility for all aspects of GDPR compliance. In this scenario, the healthcare organization/prescribing doctor, while not having a specific role with regard to data processing,

will necessarily be able to access the patient's input and output data in order to monitor the continuing implementation and results of the therapy (presumably as parties processing data under the authorization of the data controller or processor, pursuant to Article 29 of the GDPR).

1.2 General principles of data processing

The subject who qualifies as data controller must guarantee that the data are processed in compliance with the data processing principles listed in Article 5 of the GDPR.

In DTx, compliance with these principles presents the following specific features:

a) *Principle of lawfulness*

Data processing can be carried out only insofar as it has a legal basis.

For DTx, processing is carried out on data related to health (which thus, conceptually, fall under the heading "particular categories of data"), consistent with the legal basis found in Article 9 of the GDPR.

It must also be borne in mind that the legal basis may change, according to which subject is identified as data controller.

Indeed, if the data controller is the healthcare organization or the doctor, the legal basis for data processing can be found in Article 9.1(h), which allows health data processing by healthcare professionals (Article 9.3) for purposes of *"diagnosis, assistance or medical processing"*.

On the other hand, if the data controller is the manufacturer of the medical device (a situation for which no legal basis is provided by Articles 9.2(h) and 9.3), the legal basis for data processing can presumably be only the patient's consent (Art. 9.2(a)).

b) *Principle of purpose limitation*

Another linchpin of the system is the principle of purpose limitation. Article 5.1(b) of the GDPR states that the data controller shall define the purposes of data processing beforehand, and that all data processing shall then be carried out for no purposes other than those previously chosen (which must be declared in the information provided to the data subject for informed consent - see point (c) below, 'Principle of transparency').

In the context of DTx, the main purpose will certainly be *"diagnosis, assistance or medical processing"*, and thus improvement of the patient's general state of health. Moreover, this purpose justifies healthcare use, and

thus the legal classification of DTx as a medical device.

However, the data collected can subsequently be used for other purposes, such as post-marketing surveillance of the medical device (Article 83 MDR), the legal basis for which - as already mentioned - can be found in the MDR itself.

Another purpose of data processing could be scientific research (in the broad definition of recital 159 of the MDR). In this case, bearing in mind the different possibities as to who will be the data controller, it will be necessary to define the legal basis for the data processing to which reference is made (e.g., Article 9.2(h), if the data controller for purposes of scientific research is a public body; or to acquire a separate patient's consent, if the data controller is a private sector DTx manufacturer).

An aspect that should not be overlooked is data processing for marketing purposes (of the patient's and/or the doctor's and healthcare staff's data): in this case, the legal basis for the data processing (irrespective of whether the data controller is a health organization or the manufacturer of the device) has to be the patient's consent. To this end, it must be pointed out that individual consent (of the doctor and/or patient) must be freely given (in other words, with no pressure of any sort) and informed (i.e., on the basis of a clear and comprehensible explanation) - see point (c), below, on the principle of transparency.

Finally, a few remarks of specific relevance to data processing by software. As known, software today can in some cases also operate on a self-learning basis (so-called machine learning): sometimes, the most advanced machine learning functions can lead to different data processing aims from those defined when the software is first used. This could, conceivably, give rise to a scenario of data processing for aims that have no suitable legal basis.

In this regard, it seems appropriate - especially in cases like that of DTx - that software running on a self-learning basis should be programmed so as to prevent its escaping human control.

c) *Principle of trasparency*

In the GDPR system, great importance is given to the principle of transparency. The data subject (in our case, the patient using DTx) is always and in any event the "owner" of their own data - hence the requirement that s/he shall be enabled to understand exactly *how* and *why* their data are being processed, so that s/he can take an informed decision in this regard.

Moreover, the principle of transparency set forth in Article 5.1(a) is

further developed in greater detail in Articles 12 *et seqq*. of the GDPR; in particular, Article 13 deals with the information to be provided to data processing for acquiring an informed consent.

In providing this information, the data controller is required to clarify to the patient the purposes for which the data are being processed, and also how the process itself is carried out (including data storage and an indication of the country where data are to be transmitted and/or stored).

In DTx, run by means of software, a number of profiles are worthy of attention. First of all, Article 13.2(f) establishes that the data controller shall provide the data subject with information about *"the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject"*.

Even though DTx can arguably not be considered an automated decision-making process in the strict sense of the term used in the GDPR (since either a doctor or a healthcare professional is always involved in the processing), the delicate nature of the type of processing concerned requires that the data controller acts in the most transparent manner.

In this regard, help is provided in recent guidance issued by the *Information Commissioner's Office* (ICO), the UK authority for upholding information rights in the public interest. While the document's clear relevance to artificial intelligence software is readily apparent in its title, *"Explaining decisions made with AI - Draft guidance for consultation"*, it can also be seen as an excellent source of best practices for software not falling within the AI category.

Very briefly, in the above-mentioned document, the ICO specifies that the data controller shall decide how to structure and communicate the information to be provided to the data subject, bearing in mind the following elements: 1) the sector in which the AI model is used; 2) the impact on the individual; 3) the type of data processed; 4) the urgency of the decision; 5) the subjects for whom the information is meant.

The information concerned can, according to the ICO, be divided into two macro-categories:

a. *process-based* explanations: according to which it is necessary to explain that all best practices on software design have been followed in the course of the decision-making process;

b. *outcome-based* explanations: according to which it is necessary to clarify the result of the specific decision, using simple and readily under-

standable language to provide information on the reasoning followed.

Finally, the ICO lists six types of information that, according to the specific case, can either fall under the *process-based or outcome-based* heading. Indications and checklists are also provided, to enable full and correct implementation in this regard.

Very briefly:

1) *Rationale explanation*: the reasons that have led to a decision should be explained, in an accessible, non-technical manner;

2) *Responsibility explanation*: it should be explained who is involved in an AI system's development, management and implementation, and who may be contacted for a human review;

3) *Data explanation*: an explanation must be provided as to which data have been used in a given decision, and how they have been used;

4) *Fairness explanation*: the basics of the software's operation, and how it guarantees fairness in data processing, should be explained.

5) *Safety and performance explanation*: information must be given about how the software works, illustrating its accuracy, reliability, security and the robustness of its decisions.

6) *Impact explanation*: specific information must be given on the steps taken, during an AI system's design and implementation, to take into account and monitor impacts on an individual and on society at large, resulting from the system's use and the decisions it takes.

As already mentioned, while the above indications are not mandatory, they are best practices recommended by the ICO for information to be provided to data subjects in relation to artificial intelligence. They can, of course, also be applied to software not definable as AI.

Finally, with regard to the means of providing the necessary information to the patient, which for DTx might be an app, useful sources are the WP 29 documents "Guidelines on transparency under Regulation 2016 679" and "Opinion 02/2013 on apps on smart devices", as well as the *European Union Agency for Cybersecurity* (ENISA) document *"Privacy and Data Protection in Mobile Applications"*.

d) *Principle of fairness*

Another principle to be upheld by the data controller is fairness, in relation to the data subject's reasonable expectations regarding data processing.

In our opinion, the data subject's reasonable expectations overlap with many aspects of software developer ethics. On that basis, compliance with

the principle of fairness for data processing as set out in Article 5 of the GDPR basically aligns with compliance with the ethical requirements of data processing.

This view finds corroboration in the ICO's *"Guidance on AI and Data Protection"*, particularly in the following extract from the section entitled *"How do the principles of lawfulness, fairness and transparency apply to AI?"*:

"…. if you use an AI system to infer data about people, in order for this processing to be fair, you need to ensure that:

- *the system is sufficiently statistically accurate and avoids discrimination; and*
- *you consider the impact of individuals' reasonable expectations."*

In the Italian setting, useful information in this regard can be found in the document *"Mobile-health e applicazioni per la salute: aspetti bioetici"*, covering bioethical concerns related to mobile health and health apps. This document was issued on 28 May 2015, by the *Comitato Nazionale di Bioetica* (National Bioethics Committee).

e) *Principle of data minimization*

The principle of data minimization calls for limitation of data collection and processing to such data as appear to be necessary in relation to the purposes stated in the explanation provided to the data subject. Compliance with the principle of data minimization is thus not an abstract or predefined issue, but it is closely linked to the purposes of data processing as stated by the data controller in the explanation provided to the data subject.

For illustrative purposes only, it is worth bearing in mind that the information collected and then processed could differ according to whether the purposes of data processing are limited to diagnosis and treatment, or also extended to marketing.

Accordingly, reference must be made to the stated purposes of data processing, so that it can be decided whether the information collected (in other words, "data") is indispensable for their achievement.

f) *Principle of data accuracy*

For processing carried out by software, the principle of data accuracy as stated in Article 5 of the GDPR takes on particular importance. This principle establishes, in general terms, that every data item processed must be accurate and up-to-date, and that all reasonable and necessary measures shall therefore be taken for rectification of inaccurate data.

In the specific field of software (and thus of DTx), data accuracy must

be seen both as an initial necessity and as a final aim, thus including accuracy in operation of the software itself: in other words, accuracy must be the leitmotif throughout the entire data path. There is no question that, if the input data are not accurate or correct, the entire process will be invalidated, and the software's output data will prove inaccurate.

Moreover, with regard to DTx, this concern is particularly relevant in terms of liability - whether product liability in relation to medical devices, or medical liability of the organization/doctor administering DTx. Inaccuracy of output data could invalidate the processing decisions, and thus jeopardize the patient's health and security.

Data accuracy has an even greater impact where software operates on the basis of machine learning and artificial intelligence systems.

g) *Principle of data storage limitation*

Finally, the GDPR states that the duration of data storage should not extend beyond the time at which the purposes of data collection are achieved. In DTx, given that the data are used for medical treatment, it is deemed appropriate that the length of data storage is governed by the same rules as for storage of medical records (in cases where the data controller is a public healthcare organization), or is at least 10 years (if not more), *inter alia* with a view to preserving evidence of possible civil, penal and administrative liability.

1.3 Automated decision-making process and profiling

A further point that should be briefly illustrated is automated individual decision-making and profiling, as dealt with in Article 22 of the GDPR. This has already been referred to above, under the heading "Principle of data transparency", in relation to information to be provided to the data subject.

For reasons of brevity, we intend here to focus solely on Article 22 of the GDPR, which states: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

The *Article 29 Data Protection Working Party* (WP) document, "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", defines "automated individual decision-making" as "*the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data*."

Strictly speaking, it can thus be argued that DTx does not come under the heading of "automated decision-making process", in that the decisions taken (which affect the patient's legal sphere) can hardly be defined as automatic and are mostly taken with the involvement of a healthcare professional.

On the other hand, it is understood that, where the software output can be considered to have an automatic effect on the patient's legal sphere and there is no direct involvement of a healthcare professional, the provisions of Article 22 can be fully applied. In particular, the processing modalities in this case require an ad hoc consent.

With regard to profiling, it should be pointed out that the GDPR deals with this aspects of data processing only in Article 22: consent in this regard seems to be required only if there is automated processing.

1.4 Impact assessment

Article 35 of the GDPR states that, where data are processed by the use of new technologies and the data processing involves high risks for the data subject's rights, the data controller shall carry out an impact assessment beforehand.

Basically, this is a document that must contain:

- a systematic description of the intended forms of processing and their purposes;
- an assessment of the necessity and proportionality of processing, taking into account its purposes (and thus evaluating the risk-benefit ratio);
- an assessment of how the data processing could impact the data subjects' rights (e.g., the right to health), and of related risks in terms of impact.

Data processing by DTx requires prior impact assessment, because carried out by software and likely to have a significant impact on the patient's health.

Finally, in the light of the overview offered on these pages, it should be pointed out that the data controller, when carrying out an impact assessment, can decide to ascertain the opinions of the data subjects or their representatives with regard to the scheduled data processing.

2. Security and integrity of data in DTx

The MDCG[1] and IMDRF[2] documents provide an overview of cybersecurity risks for medical devices and indicate the good practices to be adopted to guarantee data security during the design, implementation and post-production phases of a generic medical system or application.

In particular, the MDCG guidance presents cybersecurity requirements for medical devices as stated in European law, addressing specifically such concerns such as the efficacy of data security measures, risk analysis and management throughout the medical device's life cycle and, as already seen above, data protection and data management. The IMDRF guidance sets out principles and practices to manage medical device cybersecurity, with a view to guaranteeing full compliance with European regulatory requirements. Both documents present a systematic examination of practices to be adopted, starting with fundamental definitions in the field of information security before dealing extensively, but in general terms, with the management of risks and threats. While extensive, the two documents do not provide specific indications regarding DTx cybersecurity requirements, but they are limited to setting out such requirements for medical devices in general.

In addition, the perspectives of both documents are necessarily of an indicative nature, so that they can be exhaustively applied to different possible types of medical devices. However, if the approach to data security has to be contextualized in greater detail by applying its principles to DTx, the discussion has to be less abstract, and a more detailed approach has to be developed. The specificities of DTx need to be examined in detail and, in a certain sense, raise different issues from other medical devices. This becomes clear if one thinks of the difference between a classic medical device, such as an infusion pump for chemotherapy, and a DTx service available as used on a patient's smartphone. Without taking into account the possible complexity of the software in the two types of device, the DTx manufacturer does not have the simple option of being able to use a trusted hardware support, because the patient's personal smartphone is inevitably exposed to further threats: this means that the attack surface is far greater than in the case of the classic medical device. The extent of this vulnerability to threats in the case of DTx must be considered during the research phase, and also in risk analysis and management.

For a full understanding of this difference from other medical devices, we will now examine the architecture of a generic DTx application (or SaMD - Software as a Medical Device), before analysing insider threats and outsider threats. This will facilitate the description, based on an example, of useful concepts and practices to ensure cybersecurity in the context of DTx.

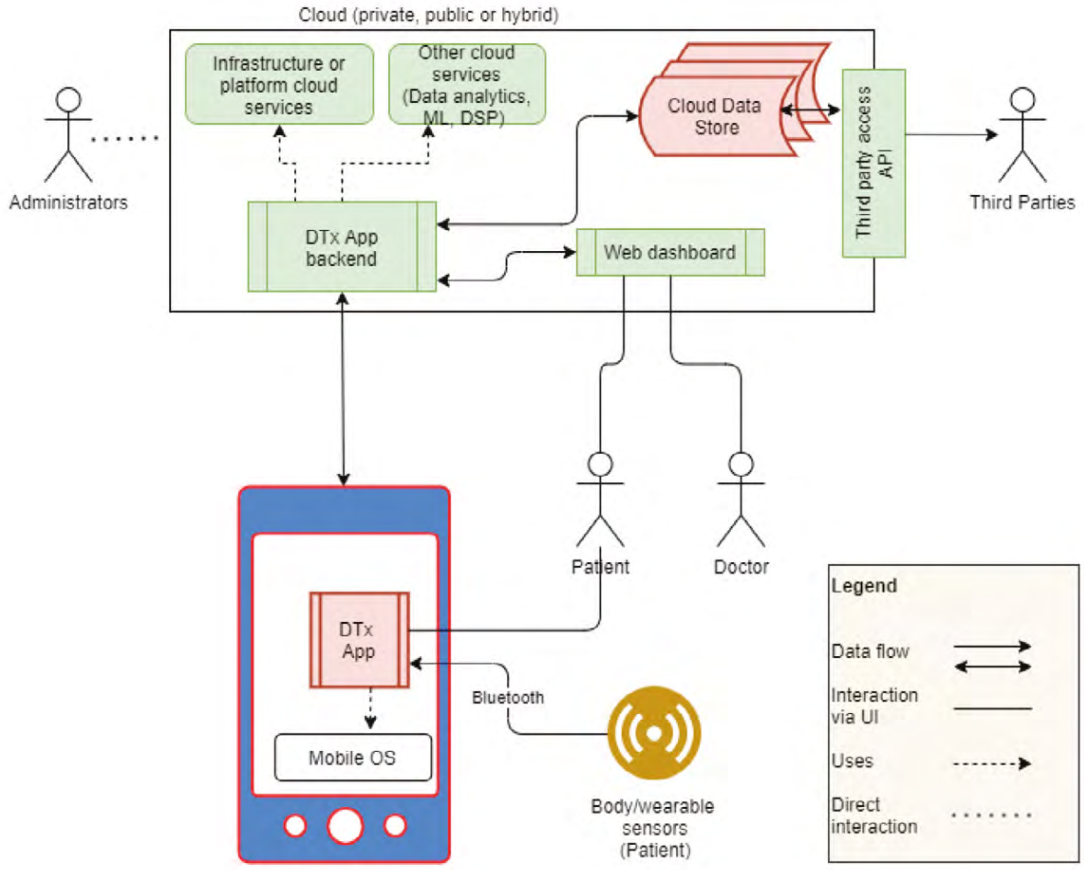
2.1 Reference architecture

The general reference architecture for a system delivering a DTX service (DTx[3] or SaMD) can be outlined as in *Figure 1*.

The DTxApp, the chief means of access to DTx, is made up of two main macro-components:

- The first, the DTxApp, is hosted and run on the patient's mobile device. Below, we will assume that the DTxApp has been developed using a Cross-platform or Hybrid web pattern[4].
- The second component, the DTxApp backend, is hosted and run on a cloud platform and can perform several functions, such as access to data memorized in the Cloud Data Store (CDS), writing of data in the CDS, analysis or processing of data, execution of DTx algorithms, and execution of engagement algorithms. The DTxApp backend offers a series of Application Programming Interfaces (API), to be used by the DTxApp and the Web dashboard.

Figure 1 - Reference architecture of a delivery system for a DTx service



The Web dashboard is a web portal that typically enables access to a subset (or an overset, according to the role of the person accessing it - e.g., patient, caregiver or doctor) of functions offered by the DTxApp.

The cloud, which can be public, private or hybrid according to needs, can host and run other support services - e.g., authentication, user profile and therapy profile management, access/memorization of dynamic data, data analytics, voice recognition and image recognition, monitoring, data stream processing (DSP) and many others. It is important to bear in mind that the CDS, storing patient treatment data, should be managed by a cloud provider with specific features for health data management, or certified for this purpose (e.g., HIPAA, HITRUST CSF, ISO/IEC 27018).

Finally, the DTx/SaMD could offer third-party access API, as in the figure, thus allowing third party systems to access the data collected (e.g., Ministry of Health, pharmacies, pharmaceutical companies manufacturing and distributing traditional drugs to be combined with DTx systems).

Below is a list of the actors interacting with the system:

- The patient is the subject who accesses the DTxApp, using the personal mobile device on which the app is hosted. The app provides the patient with a user interface (UI). Typically, it also enables monitoring of certain vital parameters, by means of implantable/wearable body sensors. In addition, the patient can interact with the DTxApp through the web dashboard - e.g., via a PC.
- The caregiver is the contact person who normally provides day-to-day support for the patient. This is the person who answers calls, reminds the patient of therapies, accompanies him/her throughout the diagnostic-therapeutic and clinical pathway, and takes charge of daily care. The caregiver too accesses the DTx/SaMD system by means of a DTxApp or web dashboard.
- The doctor accesses the system via the web dashboard, to check the patient's state of health and the progress of treatment.
- The healthcare professional (nurse, speech therapist or other healthcare operator), on the basis of a doctor's prescription, takes care of any needs and/or actions identified by reading the data transferred. The healthcare professional accesses the DTx/SaMD system via the web dashboard.
- Third parties are subjects (e.g., pharmacy, manufacturer of drugs used in combination with DTx, Ministry of Health) who can access data, typically in aggregate form and anonymized by means of a dedicated API.
- Administrators, not examined here, are the subjects tasked with management of the DTx/SaMD cloud platform.

In order to understand possible cyber threats, it is also important to

provide a brief explanation of how the various DTxApp system components interact. Again using the architecture in *Figure 1* for illustrative purposes, from bottom to top:

- The body/wearable sensors provide data to the DTxApp via Bluetooth or another wireless protocol;
- The DTxApp, installed and run on the patient's mobile device, uses the operating system functions (Android or iOS) for access to resources (e.g., local memory) and I/O operations (e.g.,, use of the internet, display, audio or camera);
- The DTxApp communicates with the DTxApp backend to carry out such procedures as authentication, access to the user profile and therapy, access to dynamic data, sending of data generated by sensors or by the DTxApp, etc. Interaction between the DTxApp and DTxApp backend takes place via the internet, usually by means of web services (API REST);
- The DTxApp backend uses cloud platform services to guarantee performance, reliability and security - e.g., load balancing, scaling of resources, geographical distribution, redundancy, VPN, firewall, etc.
- The DTxApp backend, in turn, can also use cloud services such as authentication, user profile management, data encryption and scalable platforms for data analysis (e.g., Hadoop) or for data stream processing (e.g., Spark);
- The DTxApp backend reads and writes data from one or more CDS;
- The web dashboard uses the API provided by the DTxApp backend for web access to DTxApp functions.

2.2 Threat analysis

The cyber threats to the DTx system mentioned above will now be analysed.

Many of the DTx/SaMD system components in *Figure 1* (the ones indicated in green) can be made secure by using good practices and standard technologies, as illustrated in the MDCG and IMDRF documents. In particular, technological solutions and security checks are available for communication networks and protocols (ISO/IEC 27033 Parts 1-6 inclusive), cloud services (ISO/IEC 27017) and applications carried out on the cloud as an integral part or supporting element of DTx. On the other hand, the DTxApp (run on the user's mobile device) and the CDS (in red in *Figure 1*) are the weak links in the system and merit closer analysis.

2.2.1 Main threats to the Cloud Data Store component

The Cloud Data Store (CDS) is certainly one of the most enticing resources for anyone wishing to attack the system[5]. As shown by Tang *et al.*[6],

a CDS can be subject to various types of threat - e.g., data theft or disclosure, illegal access, corruption or loss of data, and violation of data protection. The culprits can be hackers, curious cloud service providers (who can readily view users' data and access profiles), or vulnerable cloud service providers who can lose or compromise data. Recently, the scientific community has proposed a number of techniques to make CDS secure, but such solutions are still immature. In addition, the techniques to be used are closely dependent on the specific use of the CDS and the security requirements.

For example, if research must be carried out on the data without affecting their confidentiality, encryption techniques are recommended. These make it possible to search for information inside an encrypted database (searchable encryption)[7]: only the final result will be decrypted. On the other hand, if the intention is to guarantee the confidentiality of data during their processing by means of an application (e.g., DTxApp backend, or third party applications), homomorphic encryption techniques should be used[8]. These make it possible to perform calculations on encrypted data without having to decrypt them. If the DTx provider is interested in sharing data with third parties, doctors and patients, data access and data integrity must be at all times controllable. This means that controlled access must be ensured, by means of innovative protocols such as the following:

- selective encryption[9], enabling selective access to encrypted data by advanced encryption key management techniques;
- attribute-based encryption[10], meaning a technique to manage access policy for encrypted data on the basis of users' privilege levels (e.g., doctors, patients, third parties, administrators);
- provable data possession[11], enabling the provider of the DTx/SaMD service to verify that the data memorized in a CDS are correct (useful when the CDS it not under the control of the DTx/SaMD provider, but entrusted to third parties);
- proof of retrievability[12], making it possible to verify that a file is intact and always available to legitimate users.

Finally, it is important to consider the problem of data protection and privacy for users requiring access to data memorized in the CDS and to cloud services (DTx/SaMD). Examples of innovative techniques for this purpose include the following:

- access pattern protection[13], to mask the externally observable behaviour of users accessing a cloud service (observation of their behaviour could enable system hackers to garner sensitive user information);

• query privacy protection[14], to mask associations between indexes and keywords used for research and the corresponding data;

• user identity protection[15], ensuring that the identity of the user accessing data remains secret (following authentication).

2.2.2 Main threats to the DTxApp component

Security practices included in the MDCG and IMDRF documents, though generally recognized as effective, can find their full application in infrastructure that delivers a DTx service, as long as there is complete control of every single component shown in *Figure 1*. The main differences between a medical device (MD) and SaMD are the characteristics of the underlying IT infrastructure, and the control that can be kept over it. For a classic MD such as a pacemaker, the manufacturer has the possibility of controlling and certifying every aspect of development - from firmware to communication protocols, the update system and so on; on the other hand, in the case of generic SaMD, security control depends mostly on external factors, related to the operating system (Android or iOS) of the patient's mobile device, thus remaining outside the control of the DTx/SaMD manufacturer.

Specifically, as stated by MDCG in "Practice 4 - Secure implementation", each externally supplied system component must comply with the practices defined in "Practice 1 - Security management", though these seem not enough to maintain a high standard of security for DTx/ SaMD, at least insofar as the security of the patient's mobile device is concerned.

Given the constant increase in malware on mobile platforms, there is an undeniable risk of the patient's smartphone already being compromised before the SaMD is installed. A study by Kaspersky on data collected in the year 2019, for example, identified 3,503,952 malicious installation packages, 69,777 new mobile banking Trojans and 68,362 new mobile ransomware Trojans on clients' mobile devices (16).

This possibility, not covered by the MDCG and IMDRF documents, deserves particular attention because the level of risk involved is not negligible. A possible objection is that a similar level of risk is present even with equally sensitive applications such as those used by banks for personal finance, but it is readily apparent that the two situations are rather differently managed. Where a smartphone hosting a banking app is compromised, a would-be hacker will in any case always have to interface with the bank's systems, since all financial information is stored and managed sole-

ly by them; the application is merely an interface for the user. For this reason, the bank can always notice any unusual activity, blocking it where appropriate and reporting it to the user and the authorities concerned: bank operations must in all cases be approved by the bank server. By contrast, in SaMD, the patient follows the treatment and provides inputs (if required) to the DTx application, generally with no need for the DTxApp backend's constant validation: the patient's mobile device enables direct interaction with the DTxApp. This first example serves to illustrate the difference between SaMD and any other medical device, as well as any other App used today, in terms of cyber risk management.

It is useful at this point to consider two cases. In the first, malware has already been installed and taken complete control of the patient mobile device, with the result that the therapy administered to the patient is not as intended. Since the malware has complete control over the patient's mobile device, it can also show the cloud control system that everything is normal and the patient is improving. As many SaMD systems currently use mechanisms similar to cognitive-behavioural psychotherapy, a deliberate change of these therapies in the treatment of serious conditions such as drug addiction could aggravate the problem.

In the second case, instead of modifying the content of the medical treatment administered, the malware alters the patient's inputs and responses to the DTxApp. This means passive alteration (in other words, without modifying the DTx software) of the patient's treatment pathway. Some SaMD systems adapt the medical treatment according to progress made, changing its objectives if - and when - certain results are achieved. Inducing this type of system to think that certain aims of the medical treatment have been achieved could thus, for example, bring about a premature change in the treatment given to the patient, compromising its efficacy or even worsening the patient's condition.

These examples show how, in the case of SaMD, normal security practices as described in the MDCG and IMDRF documents are not enough, meaning that specific further actions are needed to mitigate the peculiar threats and risks described above. Among possible solutions could be device attestation of the patient's mobile device or the DTxApp[17], and integration of encryption systems for the cloud control system to validate the SaMD's delivery of treatment. DTx/SaMD should also be fitted with anomaly detection mechanisms, for automatic or semi-automatic detection of anomalies in administration of the treatment and in the individual's re-

sponse to it, as previously mentioned. If the patient's data are compromised from the very outset of treatment, however, it is important to recognize that this could make it impossible to identify the anomalies, given the lack of correct data on which to base decisions. Hence the need, in suspect cases, for an independent, trusted, direct and frequent channel of communication with the patient, to confirm the state of progress in treatment and the real extent of the resulting improvement or worsening. This channel could be set up by extending functions of the control room in which healthcare professionals work, enabling a response to patients' and caregivers' doubts about any change in the treatment schedule. In this case, operators answering telephone calls must be able to speak the necessary languages correctly and understand what the patient/caregiver is reporting.

2.3 Concluding remarks

In conclusion, DTx are associated with risks in relation to cyber threats that have to be specifically assessed and limited, paying particular attention to the specificity of DTx/SaMD as a mixture between a medical device and software distributed across a complex architecture. Despite the availability of many technological solutions enabling adequate mitigation of cyber risks, both for medical devices and for software products, it is the very specificity of DTx/SaMD that requires targeted further integration of the practices and principles set out in the MDCG and IMDRF documents. For example, the template of the ISO/IEC 27000 family of standards could be taken as a basis for practices enabling creation of an information security management system: to enable practical application of the general guidelines and requirements for information security management, which are necessarily very broad since they are devised for adaptation to organizations of any type and size, the standards provide guidelines specific to various settings/sectors (e.g., financial services, cloud services, inter-sectoral and inter-organizational communication, etc.). In addition, to make their application more concrete and readily practicable, the standards also include annexes detailing specific controls and adequate information security management mechanisms. For the DTx/SaMD field, what seems essential is to ensure that the specificities of such systems are methodically addressed in relation to cyber risks, and that there is coordinated development of a specific document setting out security management guidelines for the information processed, together with a series of dedicated controls to be applied throughout the system's life-cycle.

What is known:

- DTx operates by processing data on the patient's state of health, which fall under the heading "particular categories of data" (Article 4.15, Regulation (EU) 2016/679). It will thus be necessary to analyse the legal profiles involved in this type of data processing, in the light of Regulation (EU) 2016/679 (the so-called GDPR). The data controller must guarantee that data are processed in compliance with the principles set out in Article 5 of the GDPR: lawfulness, purpose limitation, transparency, accuracy, data minimization, data accuracy, and limitation of data storage
- Where a DTx/SaMD system is set up, technological solutions and security controls are available for protection of data networks and communication protocols (ISO 27033, Parts 1-6 inclusive), cloud services (ISO/IEC 27017) and applications run on the cloud, as an integral or supporting part of DTx
- Use of DTx depends on a bring-your-own-device policy, meaning that the patient, to access the treatment, must have a device such as a smartphone and the necessary data connection.

What is uncertain:

- The CDS is certainly one of the most enticing resources for a hacker. Among the threats to which a CDS is exposed are data theft or disclosure, illegal access, corruption or loss of data, and violation of data protection. The scientific community has proposed various solutions that are still immature, to guarantee confidentiality, integrity, availability, and protection of data memorized in CDS. This has to be carefully taken into account during design and implementation of a DTx/SaMD system
- The fact that a DTxApp is installed on a mobile device belonging to the user means that the setting is, by definition, not trusted. The implications of this can compromise the efficacy of the treatment or lead to severe undesired effects. Given their intrinsically general nature, the MDCG and IMDRF guidelines do not develop this important aspect.

What we recommend:

- Use of high-level governance guidelines like MDCG and IMDRF must be complemented by specific and detailed technical analysis of the new cyber risk, resulting from a complex mobile device app software in combination with the traditional concept of a medical device. This will enable implementation of specific security controls for DTx/SaMD -

e.g., taking as a template the ISO/IEC 27000 family of standards
- The patient's and caregiver's digital literacy has to be ascertained before prescribing DTx, and tutorials or training courses on the key role played by the patient must be organized.

Acknowledgments

The contribution of E. Casalicchio, L.V. Mancini, A. Mei and A. Spognardi is financed by Sapienza Università di Roma, as part of the "PRISMA - PRIvacy-preserving, Security, and MAchine-learning techniques for healthcare applications" project, and by the Italian Ministry of Universities and Research-MIUR, as part of the funding to the Informatics Department, Sapienza Università di Roma under the "Dipartimenti di eccellenza 2018-2022" scheme.

Bibliography

1. Medical Device Coordination Group MDCG 2019-16 - Guidance on Cybersecurity for medical device - December 2019 https://ec.europa.eu/docsroom/documents/41863.

2. International Medical Device Regulators Forum - March 2020 - Principle and practice for medical device Cybersecurity - March 2020 http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

3. https://dtxalliance.org/

4. What is Mobile App Development? https://aws.amazon.com/mobile/mobile-application-development/

5. Akil M, Mancini LV, Venturi D. Multi-covert channel attack in the cloud. Sixth IEEE International Conference on Software Defined Systems 2019: 160-165.

6. Tang J, Cui Y, Li Q, et al. Ensuring security and privacy preservation for Cloud Data Services. ACM Computing Surveys 2016; 49 (1), Article 13. https://doi.org/10.1145/2906153.

7. Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data. In Proceedings of IEEE 30th International Conference on Distributed Computing Systems (ICDCS'10) 2010: 253-62.

8. Craig Gentry C. A Fully Homomorphic Encryption Scheme. Ph.D. Dissertation. Stanford University, 2009.

9. De Capitani Di Vimercati S, Foresti S, Jajodia S, Paraboschi S, et al. Encryption policies for regulating access to outsourced data. ACM Transactions on Database Systems (TODS) 2010; 35: 12.

10. Sahai A, Waters B. Fuzzy identity-based encryption. In Advances in Cryptology (EUROCRYPT'05) 2005, Springer: 457-73.

11. Ateniese G, Di Pietro R, Mancini LV, Tsudik G. Scalable and efficient provable data possession. Proceedings 4th Intl. Conf. on Security and Privacy in Communication Networks (SecureComm 2008), September 2008.

12. Juels A, Kaliski BS Jr. PORs: Proofs of retrievability for large files. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07). ACM 2007: 584-97.

13. Yang K, Zhang J, Zhang W, Qiao D. A light-weight solution to preservation of access pattern privacy in untrusted clouds. In Computer Security (ESORICS'11) 2011, Springer: 528-47.

14. Cao N, Wang C, Li M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems (TPDS) 2014; 25 (1): 222-33.

15. Wang B, Li B, Li H. Knox: Privacy-preserving auditing for shared data with large groups in the cloud. In Applied Cryptography and Network Security. 2012, Springer: 507-25.

16. Chebyshev V. Mobile malware evolution 2019. Kaspersky https://securelist.com/mobile-malware-evolution-2019/96280/

17. Dushku E, Rabbani M, Conti M, et al. SARA: Secure Asynchronous Remote Attestation for IoT systems. IEEE Trans. Inf. Forensics and Security 2020; 15: 3123-36.