Slovenian Medical Journal

Personal data security in telemedicine services

Varovanje osebnih podatkov v telemedicinskih storitvah

Rok Bernik,[1] Marija Petek Šter[2]

[1] Faculty of Medicine, University of Ljubljana, Ljubljana, Slovenia
[2] Department of Family Medicine, Faculty of Medicine, University of Ljubljana, Ljubljana, Slovenia

Correspondence/ Korespondenca:
Rok Bernik, e: rokbernik5@gmail.com

Key words:
data compromising; videoconferencing; electronic mail; remote monitoring; security measures

Ključne besede:
informacijske nevarnosti; videokonferenca; elektronska pošta; spremljanje na daljavo; varnostni ukrepi

Received: 13. 7. 2020
Accepted: 28. 9. 2020

Abstract

Telemedicine is a rapidly evolving field that presents an effective way of providing healthcare services. As its use, likewise everyday clinical practice, involves handling of sensitive personal data, it is necessary to be aware of the dangers posed by cybercrime and ways of protection against such attacks. The field of personal data protection is well defined in the Slovenian and European legislation, but there are some unresolved issues in the telemedicine field. Telemedicine services are divided into synchronous (real-time, e.g. videoconferencing), asynchronous (with a delay in communication, e.g. e-mail) and remote monitoring of patient health parameters (arterial pressure, blood sugar, etc.). Each of these areas has its own security features and peculiarities. The protection of personal data in telemedicine services must be ensured at the systemic and individual levels. Every healthcare employee who uses telemedicine services must ensure data security at their work. It is especially important to conduct regular training on the topic of information security. A relatively large number of telemedicine projects have already been implemented in Slovenia, some of which have been put into regular use. One of the most extensive healthcare projects in Slovenia is the eHealth project, which also includes some telemedicine services (*TeleKap, Teleradiologija, ePosvet*).

Izvleček

Telemedicina je hitro razvijajoče se področje, ki na učinkovit način zagotavlja zdravstvene storitve. Ker se pri telemedicini, tako kot v vsakdanji običajni klinični praksi, rokuje z občutljivimi osebnimi podatki, se je treba zavedati nevarnosti spletnega kriminala ter spoznati načine za zaščito pred takimi napadi. Področje varovanja osebnih podatkov je slovenski in evropski pravni prostor dobro opredelil, obstajajo pa odprta še nekatera nerazrešena vprašanja na področju telemedicine. Telemedicinske storitve delimo na sinhrone (v realnem času, npr. videokonference) in asinhrone (z zaostankom v komunikaciji, npr. spletna pošta) ter na spremljanje parametrov zdravja na daljavo (spremljanje arterijskega tlaka, krvnega sladkorja ipd.). Vsako od teh področij ima svoje varnostne značilnosti in posebnosti. Varovanje osebnih podatkov je pri telemedicinskih storitvah potrebno zagotoviti na sistemski in individualni ravni. Vsak zaposleni v zdravstvu, ki izvaja storitve na področju telemedicine, mora pri svojem delu skrbeti za varnost podatkov. Posebej pomembno se je redno izobraževati na temo informacijske varnosti. Tudi v Sloveniji se izvaja že sorazmerno veliko telemedicinskih projektov, med katerimi jih je nekaj tudi prešlo v redno uporabo. Eden najobsežnejših zdravstvenih projektov pri nas je projekt *eZdravje*, ki med drugim vključuje tudi nekatere telemedicinske storitve (*TeleKap, Teleradiologija, ePosvet*).

Cite as/Citirajte kot: Bernik R, Petek Šter M. Personal data security in telemedicine services. Zdrav Vestn. 2021;90(3–4):159–72.

DOI: https://doi.org/10.6016/ZdravVestn.3131

1 Introduction

Information and communication technology is becoming an increasingly prevalent part of our lives. Its positive aspects, such as time efficiency, are used both in personal and professional life. With a slight delay, it is now becoming increasingly more important in healthcare, with some of the activities now referred to as telemedicine.

Telemedicine means using electronic communication methods and information technology for performing clinical services remotely. The first concepts of telemedicine cropped up in mid 19th century, when the invention of telegraph and later also the telephone made long-distance communications possible. In 1924, the US magazine Radio News published an illustration depicting a family communicating with their physician over a video screen. What we call telemedicine today was mostly developed based on military technology in the mid-20th century. At first, it was prohibitively expensive and available only in a very limited scope. Its use was expanded only towards the end of the century after the invention of the Internet, and with the accelerated development of information technology (1,2).

Because clinical work requires access to and processing of sensitive data, information security is an essential part of telemedicine. With expanding digitalization, the danger of the abuse and theft of personal data is also growing. According to some surveys, more than 80% of healthcare institutions have admitted to being victims of cyber attacks in the past. There was a famous case in April 2004, when stolen medical data from hundreds of US citizens was discovered on a server in Malaysia, or when a few years ago, an anonymous poster published a list of over 4,000 HIV-positive inhabitants of Florida. One of the biggest attacks so far took place in 2016. Attackers hacked the servers of *Anthem*, the second biggest US healthcare insurance company, gaining access to the medical data of over 80 million insured persons. The stolen data included names and addresses and the data on their conditions and treatments. Many similar attacks and a few cases of medical data theft have also been reported in Slovenia (3,4,5).

There is a significant risk related to personal data security, because healthcare workers also violate regulations related to personal data protection. In its annual report, the Information Commissioner emphasized the following violations in particular (6):

- sending medical data over unsecured (unencrypted) connections (general email, unencrypted online connections);
- lending means of authentication for data access (passwords, cards) and securing them inappropriately;
- data leaks and selling data from healthcare institutions for direct marketing purposes;

- limited oversight and control over data processing performed by external contractors;
- lack of awareness that spreading information on patients is inappropriate;
- lack of security in facilities where patients' medical records are kept.

2 Legal regulation of telemedicine services and personal data protection

2.1 Legal regulation of telemedicine services in the European Union

At the European Union level, telemedicine is defined as a healthcare service and information society service. As such, it falls under the Treaty establishing the European Community, and the field of valid secondary legislation (European directive) (7,8):

- Directive 2000/31/EC (Directive on electronic commerce) details providing information society services in member states and among them, and includes telemedicine.
- Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector sets up different requirements for electronic communications providers that ensure communication confidentiality and network security.
- The Directive on the application of patients' rights in cross-border healthcare (Directive 2011/24/EU) details the field of cross-border patient mobility and their options for accessing cross-border services. Based on this directive, the Commission must adopt measures that will support the interoperability of the means for providing e-healthcare services, including telemedicine.
- Directive 2015/1535 defines the procedure that obliges a Member State to provide the Commission and other Member States with every draft technical regulation on information society services, including telemedicine, before adopting it at the national level.

The Court of the European Union has through different rulings (case no. C-385/99, Müller and Van Riet, Recueil 2003; case no. C-157/99, Smits and Peerbooms, Recueil 2001; and in case no. C-372/04, Watts, Zodl. 2006) confirmed that there are no special aspects to the method of organization or financing of healthcare services that would exclude them from the scope of the basic principle of free movement. Users of healthcare services can, therefore, seek and receive medical assistance in another Member State, regardless of how this service is performed, i.e., also including telemedicine (7).

2.2 Legal regulation of telemedicine services in the Republic of Slovenia

In 2017, the National Assembly of the Republic of Slovenia adopted the Act Amending the Health Services Act which transposed Directive 2011/24/EU into the legal order of the Republic of Slovenia. This brought a change to the wording of Article 3 of the Health Services Act and defined the meaning of telemedicine (9): "Healthcare services in respect of which a patient and one or more healthcare service providers can be spatially separated considering the rules of medical doctrine may be performed by means of information and telecommunications technologies (hereinafter: telemedicine). In this case, health records shall be sent in accordance with the regulations governing the

protection of personal data which concern the transfer of sensitive personal data over telecommunications networks. If healthcare activities are provided in the form of telemedicine, healthcare shall be provided in the Member State where the healthcare service provider applying telemedicine is established."

When transferring and processing medical data for the provision of telemedicine services, the existing national legislation relevant for this issue must be considered, especially (10,11):

- Health Services Act (ZZDej),
- Medical Services Act (ZZdrS),
- Patients' Rights Act (ZPacP),
- Health Care and Health Insurance Act (ZZVZZ),
- Healthcare Databases Act (ZZPPZ),
- Personal Data Protection Act (ZVOP-1),
- Information Security Act (ZInFV),
- Electronic Communications Act (ZEKom-1)
- Electronic Commerce Market Act (ZEPT),
- Electronic Business and Electronic Signature Act (ZEPEP).

2.3. Personal data and their protection

The Personal Data Protection Act that applies on the territory of the Republic of Slovenia defines personal data as any piece of data relating to an individual, regardless of its format. Sensitive personal data include all the data on national, racial, or ethnic background, political, religious, or philosophical convictions, union membership, health, sex life, entry or removal into or from criminal records or records for minor offences. These include biometric characteristics, if their application can determine the individual in relation to any of the above characteristics (12).

Personal data protection is detailed in numerous EU decisions already provided for in primary legislation. It is mentioned in Article 16 of the Treaty on the Functioning of the European Union. It is further detailed in the Charter of Fundamental Rights of the European Union, in Articles 7 and 8. In May 2018, Directive 95/47/EC on personal data protection, which had until recently been the most relevant one for this area, was replaced by the General Data Protection Regulation (GDPR), which details among other requirements that public sector organizations, and in some cases also those in the private sector, must appoint a person responsible for data protection to advise the data manager on personal data protection related issues. It also prohibits the processing of special types of personal data (including health-related data), other than the exceptions listed in Article 9 of the GDPR. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union defines the measures for raising the information security level and establishing mechanisms for responding to cyber threats. It imposes on Member States the requirement to establish a national framework for network and information security that includes the national strategy, at least one response centre, and the applicable national body with the charter to coordinate activities at the national level. Personal data protection is also part of numerous strategies and guidelines, e.g., the Digital Agenda for Europe 2020, European Strategy for Data, etc. (3,10,13).

At the national level, personal data protection is already included in the Constitution of the Republic of Slovenia, in which Article 35 defines privacy protection, while Article 38 ensures the protection of personal data, and the use of

personal data is prohibited except for the specific purpose of its collection (3). In accordance with the Slovenian legislation, the owner of personal data is a patient to whom individual data pertains. The owner of the data carrier is the organization that stores the documentation. It must ensure personal data protection, while its employees must adhere to all the ethical principles and regulation on personal data protection, including the Personal Data Protection Act. A physician who stores their patient's medical records is directly responsible for adhering to the provisions of the Act (14). The Patients' Rights Act, especially Articles 43 and 44, which define privacy and the patient's right to personal data confidentiality, and the Information Security Act, which details information security and the measures for achieving a high-level network and information system security in the Republic of Slovenia, are also important. There are also several guidelines that assist in implementing legal documents (e.g., Guidelines for providers of healthcare services, Guidelines for protecting personal data in hospital information systems, etc.) (3,15).

3 Aspects of protecting personal data in telemedicine services

Telemedicine services must satisfy general information security requirements in order to be performed securely. These include confidentiality, authenticity, access control, integrity, availability, and non-repudiation (4,16,17):

- *Confidentiality* is the most basic function of security. It ensures that data can only be accessed by authorized persons whose identity has been verified beforehand, and only in the scope that permits them to effectively perform their work.
- *Authentication* is the service of verifying the identity of the person or data source. For this purpose, we use passwords, PIN codes, digital signatures, ID cards, fingerprints, etc.
- *Authorization* means verifying whether a person or a computer has the right to perform a specific activity.
- *Integrity* means the accuracy and intactness of data. In order to ensure integrity, a system for monitoring and logging every data change must be established.
- *Availability* means constant access to the data, including during power outages and software or hardware failures, etc. Various preventive measures must be taken to ensure availability.
- *Non-repudiation* is important for proving a performed activity, especially when the person denies it.

Threats or attacks are divided by their impact on information flow across the network into interruption, interception, modification, and fabrication. More detailed explanations of different types of attacks are available in the article by Zain J, et al. (18).

Every organization must recognize its own security needs and prepare a plan for realizing security requirements. They can utilize various existing recommendations or standards (ITIL, COBIT, ISO, CALDICOTT etc.). The most established ones in this area are the international standards ISO/IEC 27001 (Information technology – Security techniques – Information security management system – Requirements) and ISO/IEC 27002 (Information technology – Security techniques – Code of practice for information security controls), which, among other things, also defines how to establish an information security management system (19).

Telemedicine services are divided into (20):

- asynchronous (store-and-forward);
- synchronous (real time);
- remote patient monitoring (telemonitoring).

Every area has its particularities from the information security perspective.

3.1 Asynchronous telemedicine services (store-and-forward)

Asynchronous telemedicine services include sending medical data (e.g., images, videos) over electronic networks for review and assessment to be performed later. The method is often used in dermatology, radiology, and pathology (20). Data can be either sent by email or uploaded onto an online server which the recipient may access when they choose to (21). The newer method is to send data using cloud computing (22).

3.1.1 Email security

Even in healthcare, email is one of the most broadly used and convenient communication methods. It is especially widespread among family medicine specialists for communicating with patients and other healthcare workers. This communication method can be high-risk from the perspective of personal data security. In the US, for example, attackers obtained access to personal medical data of more than 100 organizations that used inappropriately protected electronic communications in the period between 2009 and 2015. It is important that users understand the danger of such communication and can protect themselves from it (23,24).

In order to understand why sending data over email can be dangerous, we must first know how email works. Unlike with regular mail, an email message is not carried from point A to point B but is copied to every link in the transfer chain. The message is created on the sender's device (computer) from where it travels to the sender's email server. From there, it is transferred to the recipient's email servers, and finally to the receiver's device (Figure 1). Attackers can obtain access to medical data during the transmission of the message, or by accessing individual links in the communication chain. All the above must be protected (24,25).

Data security can be increased using several methods. Using cryptography is the most important one. The message can be encrypted using various algorithms (e.g., 3DES, AES) and the recipient can only decrypt it using a special key. This way, personal data can be theoretically protected during the whole transfer, although they are still vulnerable if the sender's or receiver's computer is under threat. If data is sent in an attachment to the message, this part is also encrypted. As a rule, freely available internet emailing solutions (Gmail, Hotmail, AOL) are not encrypted, meaning they are not secure enough for transferring medical data. It is equally important to use sufficiently complex passwords in order to protect our accounts. A password must generally consist of at least eight characters and must include upper- and lower-case letters, numbers, and special characters. Words that can be found in a dictionary should not be used as a password. It is recommended to change the password at least every 90 days. It is reasonable to always include the warning about data security in the email, as it alerts the patient or recipient that their email includes medical data, and that the person reading this should make sure that the data is secure (24,26).

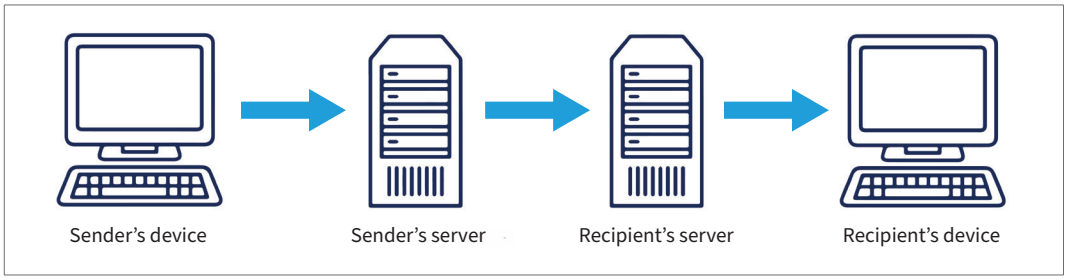

Figure 1: Diagram of message transfer by email (24).

3.2 Synchronous telemedicine services (real time)

In most cases, this means using videoconferencing apps for communication between two or more users, who may be patients and/or medical workers (27). This type of communication has gained particular traction during the Covid-19 pandemic, becoming more frequently used in outpatient clinics as an alternative to attending in person.

Because telemedicine videoconference conversations include sensitive personal data, they are frequently targeted by cyber criminals, who exploit weaknesses in videoconferencing apps. An example of this are security flaws in the Webex and Zoom videoconferencing apps, which were discovered in early 2020. These allowed unauthorized persons to join private meetings and publish unsolicited and even prohibited content (so-called zoom-bombing). Attackers also stole and sold thousands of usernames and passwords over the dark web (in April, this number exceeded 500,000). There are many more cases of abuse (28,29,30).

In April 2020, the US National Security Agency (NSA) published an analysis of the most frequently used commercially available videoconferencing apps, along with recommendations for using them (Table 1). They applied the following criteria (31,32):

- Does the service implement end-to-end encryption (E2E)?
- Are strong, well-known, testable encryption standards used?
- Is multi-factor authentication (MFA) used to validate users' identities?
- Can users see and control who connects to collaboration sessions?
- Does the service privacy policy allow the vendor to share data with third parties or affiliates?
- Do users have the ability to securely delete data from the service and its repositories as needed?
- Has the collaboration service's source code been shared publicly (e.g., open source) so that it is possible to verify what security mechanisms it uses and whether they are appropriate?
- Has the service and/or app been reviewed or certified for use by a security-focused nationally recognized or government body?

The table shows that among the apps used more frequently in Slovenia, the most secure one according to this report is Cisco Webex.

We are largely responsible ourselves for making sure that our videoconference calls are secure. We can improve security by adhering to the following recommendations (28):

- Always ensure that meetings are password-protected.

Table 1: Assessment of videoconferencing apps (31).

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex®	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™	a, b, c ,d	N	Y	Y[1]	Y[1]	Y	Client – Y Server –Y[2]	N	FedRAMP
GoToMeeting®	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™	a, b, c,e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server –N[3]	N	None
Slack®	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®	a, b, c, e	Y[1,4]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Legend: Y = yes, N = no; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing; MFA – multi-factor authentication; [1] configurable; [2] Free version - N; [3] No Published Details; [4] Partial.

- Do not share meeting information on public platforms.
- It is recommended to use host controls to lock meeting rooms once all those invited have joined the conversation and to remove any unwanted guests.
- Disable file transfer features in the videoconference.
- We can also activate a so-called waiting room, which allows the host to selectively approve guests before they join.
- Always update to the latest version and apply all the patches for videoconferencing apps.

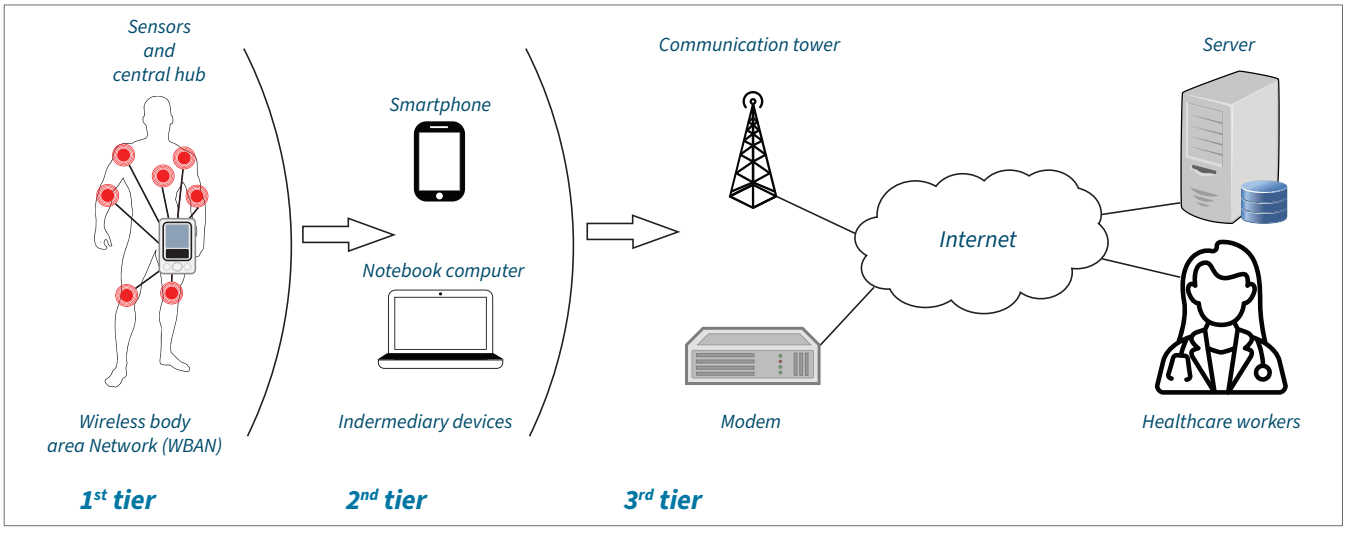

Figure 2: Three-tier architecture for remotely monitoring health parameters. Summarized from Partala J, et al (33).

3.3 Remote patient monitoring

This applies to utilizing various technological devices to monitor the patient's health parameters. Globally, remote monitoring is mostly used for the medical treatment of chronic patients with cardiovascular diseases (blood pressure measurements), diabetes (blood glucose measurements) or asthma. This type of monitoring is reasonable as it is cost-efficient and allows for more frequent checkups (20). The system used consists of several components and is complex from the security perspective (Figure 2). The first part has one or several sensors or devices for taking measurements, which are organized together with a central hub into a so-called wireless body area network (WBAN). Sensors communicate with the central hub, and the data is then transferred to the server over an intermediary device (e.g., mobile phone, notebook computer). Communication is organized across three tiers. The first includes communication in the WBAN, between the sensors or measurement devices and the central hub, the second between the central hub and the intermediary device, and the third from the intermediary device over the public network (i.e., the Internet) to the server where the data is collected and processed. From a security perspective, each of them has its own characteristics and peculiarities (33).

The wireless body area network operates at a very short distance (a few metres). This means that in order to intercept radio signals, the hacker would have to get physically very close to the patient, which is not very likely. Such attacks could become a bigger issue in the future if the use of systems for monitoring health parameters were to become widespread. In such a case, attacks would most likely occur predominantly in public places. From the security perspective, the most important standard on the first tier is the new IEEE 802.15.6 standard, which ensures data confidentiality, authentication, and privacy (33).

The second tier (between WBAN and the intermediary device) operates over greater distances than the first and is, therefore, also exposed to interception, tracking and redirection of data. An additional vulnerability is presented by the intermediary device itself. This can allow

the attacker to gain access to the network through a mobile device or a notebook computer that has been infected with malware. On this tier, the type of communication technology used is also important from the security perspective. Bluetooth brings quite a few security weaknesses, including specific types of attacks, such as so-called Bluejacking. Zigbee is more secure, and defines a group of high-level security protocols. The introduction of the IEEE 802.15.4 standard is also important on this tier, as it ensures confidentiality of data and improves their security (33).

On the third tier (between the intermediary device and the server), communication takes place over public networks, which makes it exposed to interception, modification, access prevention, assuming control, etc. Data is stored on the server, which must utilize appropriate mechanism for access limitation, including firewalls. The end server software and operating system must be promptly upgraded with the latest patches. It is also reasonable to use a virtual private network (VPN), which can create a virtual isolated connection with other parts of the system for remote monitoring. On this tier, the most dangerous attacks are those utilizing so-called social engineering (e.g., phishing attacks through email that provide the attacker with control over the system (33).

An overview of the available literature shows that researchers seldom focus on the issue of personal data protection when using technology for monitoring health parameters remotely. The main problem is the lack of awareness of information security. There is also only scarce evidence of effective implementation of security mechanisms in systems for remote monitoring. Most studies assume that personal data protection is the responsibility of the medical or communication technology vendor (34).

4 Measures for ensuring personal data security in telemedicine services

The security of transferring and processing personal data in the provision of telemedicine services can be improved utilizing the following measures. These include (11,17):

- data mirroring (additional backups);
- defining specifically defined access categories (physician, nurse, network administrator, etc.);
- installing the latest antivirus protection;
- utilizing firewalls;
- utilizing security keys, certificates, unique passwords;
- utilizing complex passwords;
- utilizing encryption for encrypting data traffic;
- establishing network intrusion systems;
- establishing data infrastructure monitoring systems;
- regularly installing patches of software and operating systems;
- using only verified software;
- decentralized data storage;
- employee training on the best security practices;
- nurturing a security culture among employees;
- preventing physical access to equipment.

Much like other networks, the security of the telemedicine network depends on its weakest link. Therefore, it is important to constantly check the security and discover any potential weaknesses of the system and promptly fix them (4).

A frequent problem with healthcare workers is illegal access to databases of personal data, either because of curiosity or because they are trying to obtain personal data for their own purposes. Access to a patient's personal data is only permitted if

the employee is participating in the process of the patient's medical treatment or for other legitimate reasons (e.g., notifying the police on the case, issuing an invoice). Where possible, access to personal data should be limited by defining access categories. In accordance with Article 24 of ZVOP-1, a system for internal traceability of personal data processing must also be established (5).

Another important aspect is protecting the data with the users themselves—the patients. They need to be informed of potential data security risks that are present when using telemedicine services. This is especially important for services of monitoring health parameters remotely, where we utilize the latest technological solutions; however, patients (especially seniors) are often not skilled in using them. If unsecured information and communication solutions are used for communication with healthcare workers, they need to be alerted to the fact, with alternative, i.e., more secure communication methods recommended (35,36).

5 Best practices of personal data security in the *eZdravje* (*eHealth*) project

In Slovenia, there have been numerous telemedicine projects, including a few that have been adopted into regular use. A few of the best security practices of the *eZdravje* project, which includes some telemedicine solutions (e.g., *TeleKap* (TeleStroke), *Teleradiologija* (TeleRadiology), *ePosvet* (eConsultation)), are described below.

From the information security perspective, the most important parts of the *eZdravje* project are the information security management system (ISMS) and the zNet secure medical network. ISMS is a system defined according to the ISO/IEC 27001 standard. This is a range of organizational procedures, decisions and technical measures performed by *eZdravje* in order to ensure data and information security. An important part of ISMS are security policies that focus on numerous areas of data protection (e.g., physical protection, malware protection, backups, audit trails, etc.), and are available at http://www.ezdrav.si/category/projekti/suvi/ (37). zNET is a private medical computer network managed by the National Institute of Public Health. It provides secure and reliable connections between the network entry point, other certified points, and key actors in healthcare. It provides access to *eZdravje* services (38,39). Security is ensured with firewalls, antivirus protection, data encryption, an intrusion detection system/intrusion prevention system (IDS/IPS), the use of virtual private network (VPN) services, and infrastructure for user authentication and authorization. Physical protection of critical facilities (offices, data centre, etc.) is also ensured, as well as the provision and appropriate storage of archival backups. For accessing *eZdravje* services, users must utilize complex passwords and qualified certificates stored on a smart card. Uninterrupted operation is ensured with redundancy in equipment and connections to all endpoints. Security measures that all users must meet before connecting to zNET are defined in the Rules on conditions, deadlines, and method of connecting to and using *eZdravje* services for mandatory users (39,40,41).

6 Conclusion

Telemedicine services are in a growth spurt, and according to many, are the future of healthcare. In spite of their many advantages, we must not neglect maintenance of the standards for personal data protection. This has also proven to

be critical during the Covid-19 pandemic, when the number of cyberattacks on healthcare institutions has risen sharply. Some organizations have reported a fourfold increase in attacks, with most of them being phishing, i.e., sending emails with links to fake websites, and ransomware, i.e., preventing data access by encryption with malware (5,42,43). Measures need to be implemented at the system and the individual level immediately in order to ensure security in accordance with the valid legislation. One of the most important measures is to ensure regular training for all healthcare employees who encounter personal data in their work. They must be informed of the dangers and the measures for prevention and mitigation. Only by motivating and developing a good security culture will it be possible to ensure an environment for the successful application of telemedicine.

References

1. Russell D, Boisvert S, Borg DJ, Burke ME, McCord D, Heathcote S, et al. Telemedicine Risk Management Considerations. Chicago (IL): American Society for Health Care Risk Management; 2018 [cited 2020 Jun 3]. Available from: https://www.ashrm.org/sites/default/files/ashrm/TELEMEDICINE-WHITE-PAPER.pdf.
2. American Telemedicine Association. Telemedicine, Telehealth, and Health Information Technology. Geneva: World health organization; 2006 [cited 2020 Jun 8]. Available from: https://www.who.int/goe/policies/countries/usa_support_tele.pdf?ua=1.
3. Baloh T. Veliko podatkovje in zasebnost v medicini: (magistrsko diplomsko delo). Ljubljana: Pravna fakulteta; 2018.
4. Das S, Mukhopadhyay A. Security and Privacy Challenges in Telemedicine. CSI Commun. 2011;35:20-2.
5. Prelesnik M. Letno poročilo informacijskega pooblaščenca za leto 2019. Ljubljana: Informacijski pooblaščenec Republike Slovenije; 2019 [cited 2020 Aug 26]. Available from: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/LetnoPorocilo2019.pdf/.
6. Prelesnik M. Letno poročilo informacijskega pooblaščenca za leto 2016. Ljubljana: Informacijski pooblaščenec Republike Slovenije; 2016 [cited 2020 Aug 26]. Available from: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2016_web.pdf.
7. Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o koristih telemedicine za paciente, zdravstvene sisteme in družbo. Ljubljana: EUR-Lex; 2008 [cited 2020 May 15]. Available from: https://eur-lex.europa.eu/legal-content/sl/ALL/?uri=CELEX:52008DC0689.
8. Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe. Ljubljana: EUR-Lex; 2008 [cited 2020 May 15]. Available from: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32015L1535.
9. Zakon o spremembah in dopolnitvah Zakona o zdravstveni dejavnosti. UL RS. 2017(64).
10. Nacionalni odzivni center za kibernetsko varnost. Ljubljana: Si-cert; 2017 [cited 2020 May 15]. Available from: https://www.cert.si/.
11. Lihtenvalner J, Flerin U, Dinevski D. Varnost osebnih podatkov v (tele)medicini. Infor Med Slov. 2014;19(1-2):29-43.
12. Zakon o varstvu osebnih podatkov. UL RS. 2004(94).
13. Ilovar E. Vpliv razvoja tehnologije na zdravstveni sistem v Sloveniji. (Magistrsko delo). Ljubljana: Pravna fakulteta; 2018.
14. Kersnik J, Tušek-Bunc K. Zdravnik kot lastnik in posrednik zdravstvene dokumentacije. Med Razgl. 2007;47(1):155-62.
15. Zakon o informacijski varnosti. UL RS. 2018(30).
16. Pesante L. Introduction to Information Security. Pittsburgh: Carnegie Mellon University; 2008. Available from: https://us-cert.cisa.gov/sites/default/files/publications/infosecuritybasics.pdf.
17. Hudomalj E. Varnost informacij. Lecture presented at: Uvod v medicino - informatika. Ljubljana: Medicinska fakulteta; 2019 [cited 2020 May 15]. Available from: https://pouk.mf.uni-lj.si/mod/resource/view.php?id=19.

18. Zain J, Clarke M. Security in Telemedicine: Issues in Watermarking Medical Images. In: SETIT 2005: 3rd international conference: Sciences of Electronics, Technologies of Information and Telecommunications; 2005 March 27-31; Susa, Tunisia. New Jersey: IEEE; 2005 [cited 2020 May 21]. Available from: https://www.researchgate.net/publication/228576599_Security_in_Telemedicine_Issues_in_Watermarking_Medical_Images.
19. Potokar M. Telemedicina z vidika varstva osebnih podatkov. In: Štrancar Fatur K, Golob P, eds. Telemedicina – Izzivi v urgenci in na čezmejnem območju; 2014 Jun 20. Portorož, Slovenija. Izola: Splošna bolnišnica Izola, projekt InergAid; 2014. pp. 44-52.
20. Smith Y. Types of Telemedicine. S.l.: News Medical Life Sciences; 2005 [cited 2020 May 26]. Available from: https://www.news-medical.net/health/Types-of-Telemedicine.aspx.
21. Schlachta-Fairchild L, Rocca M, Elfrink Cordi V, Haught A, Castelli D, MacMahon K, et al. Telehealth and Applications for Delivering Care at a Distance. In: Nelson R, Staggers N, eds. Health Informatics - E-Book: An Interprofessional Approach. St. Louis: Elsevier Health Sciences; 2014. pp. 125-46.
22. Wainstein L. Cloud-Based Telehealth Defined: Advantages, Applications, and Security. Arizona: University of Arizona Health Sciences; 2018 [cited 2020 May 27]. Available from: https://telemedicine.arizona.edu/blog/cloud-based-telehealth-defined-advantages-applications-and-security.
23. Royal Australian College of General Practitioners. Using email in general pracice. Melbourn: RACGP; 2020 [cited 2020 May 27]. Available from: https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Using-email-in-general-practice-fact-sheet.pdf.
24. Security Metrics Inc. Sending HIPAA Compliant Emails 101. Orem (UT): SM Inc; 2019 [cited 2020 Jun 3]. Available from: https://www.securitymetrics.com/static/resources/orange/HIPAA_Compliant_Emails_White_Paper.pdf.
25. Kreindler DM. Email security in clinical practice: ensuring patient confidentiality. Open Med. 2008;2(2):e54-9. PMID: 21602943
26. Li Y. Thinking of Emailing Medical Records? Think Again. Electronic health reporter. 2014 Dec 2 [cited 2020 Jun 3]. Available from: https://electronichealthreporter.com/thinking-of-emailing-medical-records-think-again/.
27. Hadeed GJ, Holcomb M, Latifi R. Communication Technologies: An Overview of Telemedicine Connectivity. In: Latifi R, ed. Telemedicine for Trauma, Emergencies, and Disaster Management. Norwood (MA): Artech House; 2011. pp. 37-50.
28. Trend Micro Incorporated. How to Secure Video Conferencing Apps. Irving: TMI; 2020 [cited 2020 May 24]. Available from: https://www.trendmicro.com/vinfo/us/security/news/security-technology/how-to-secure-video-conferencing-apps.
29. Winder D. Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords. Jersey City (NY): Forbes; 2020 [cited 2020 May 24]. Available from: https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/#7938b2165cdc.
30. Bode K. Zoom Is Full of Security Flaws — But You Can Protect Yourself. San Francisco (CA): Medium; 2020 [cited 2020 May 26]. Available from: https://onezero.medium.com/zoom-is-full-of-security-flaws-but-you-can-protect-yourself-f153f078ecbf.
31. National Security Agency (US). Selecting and Safely Using Collaboration Services for Telework. Fort Meade (MD): NSA (US); 2020 [cited 2020 May 26]. Available from: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2163484/working-from-home-select-and-use-collaboration-services-more-securely/.
32. Cimpanu C. NSA security guide: How to choose safe conferencing and collaboration tools. San Francisco (CA): CBS Interactive; 2020 [cited 2020 May 26]. Available from: https://www.zdnet.com/article/heres-the-nsas-guide-for-choosing-a-safe-text-chat-and-video-conferencing-service/.
33. Partala J, Keranen N, Sarestoniemi M, Hamalainen M, Iinatti J, Jamsa T, et al. Security threats against the transmission chain of a medical health monitoring system. In: 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services; 2013 Oct 9-12. Lisbon, Portugal. New Jersey: Institute of Electrical and Electronics Engineers; 2013 [cited 2020 May 26]. Available from: https://ieeexplore.ieee.org/document/6720675?arnumber=6720675&tag=1. DOI: 10.1109/HealthCom.2013.6720675.
34. Ondiege B, Clarke M, Mapp G. Exploring a New Security Framework for Remote Patient Monitoring Devices. Computers. 2017;6(1):11. DOI: 10.3390/computers6010011
35. Evropski ekonomsko-socialni odbor. Mnenje Evropskega ekonomsko-socialnega odbora o Sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o koristih telemedicine za paciente, zdravstvene sisteme in družbo (COM(2008) 689 konč.). Brussels: EUR-Lex; 2020 [cited 2020 May 22]. Available from: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52009AE1197.

36. Miliard M. Telehealth privacy and security: Investment and education are key, attorney says. Portland (OR): Healthcare IT News; 2020 [cited 2020 May 25]. Available from: https://www.healthcareitnews.com/news/telehealth-privacy-and-security-investment-and-education-are-key-attorney-say.
37. SUVI. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 28]. Available from: http://www.ezdrav.si/category/projekti/suvi/.
38. zNET. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 28]. Available from: http://www.ezdrav.si/category/projekti/znet/.
39. Pravilnik o pogojih, rokih, načinu vključitve in uporabe eZdravja za obvezne uporabnike. UL RS. 2015(69).
40. Drnovšek S, Bucaj Ž, Šinkovec M, Ladinik J, Černe M, Breznik K, et al. Študija izvedljivosti projekta eZdravje – predinvesticijska zasnova in investicijski program s študijo izvedbe: Definicije podprojektov. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 29]. Available from: http://mz.arhiv-spletisc.gov.si/fileadmin/mz.gov.si/pageuploads/eZdravje/predstavitev/studija/definicija_projektov.pdf.
41. Žele M. Predstavitev varnostnih politik [PowerPoint slides]. Lecture presented at: Informativni dan informacijske varnosti; Jun 2010. Ljubljana: Medicinska fakulteta; 2010 [cited 2020 Aug 29]. Available from: http://mz.arhiv-spletisc.gov.si/fileadmin/mz.gov.si/pageuploads/eZdravje/predstavitev/Predstavitev_politik.pdf.
42. Keown A. Cyberattacks on Health Care Groups Increase During COVID-19 Pandemic. Urbandale: Biospace; c1985-2020 [cited 2020 Jun 22]. Available from: https://www.biospace.com/article/pandemic-creates-opportunities-for-cyberattacks-on-healthcare-groups-report-shows/.
43. European Union Agency for Cybersecurity. Cybersecurity in the healthcare sector during COVID-19 pandemic. Athens: The Agency; c2005-2020 [cited 2020 Jun 22]. Available from: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.