Protection of sensitive data in telemedicine services

DOI: 10.7365 / JHPOR.2016.1.3

Authors:

Joanna Śliwa[1], Marek Suchański[1], Bartosz Jasiul[1]

1- Military Communication Institute

Keywords:

telemedicine, BYOD, cyber security, protection of sensitive data, SIEM

Abstract

The article presents security risks related to the use of telemedicine services and technical guidelines for protection of the medical records in terms of their confidentiality, integrity and availability. It also mentions regulations related to protection of sensitive data that are required by the Polish government.

Introduction

The common and ubiquitous use of information technology impacts life of humans in all dimensions. One of them is health care, which changes the way both patients and health professionals cooperate. This materializes with the fast development of telemedicine and e-health applications, which have become standard medical practice and are in daily use across dozens of countries.

Telemedicine relates to the practice of health care professionals to evaluate, diagnose and treat patients in remote locations using telecommunications technology. This provides also the possibility for the patients in remote locations to access medical expertise quickly, efficiently and without travel. In developed and developing countries telemedicine offers a reduced cost solution to delivering remote care when and where it is needed without the building and staffing additional facilities. Local practitioners can also consult with their peers and with clinical experts when needed.

The advantages of telemedicine applications in daily medical practice has been valued highly by the medical practitioners. However realization of telemedicine applications relates strictly to the necessity of processing of patients sensitive personal data, usually stored in electronic medical records (EMR's), which now can be accessed from the Internet. Patients personal data, including health and diagnostic reports must be properly protected from unauthorized access. Information technology which is the enabler of telemedicine applications comes with all standard threats known from Internet that apply to the systems, hardware and software. Unfortunately, most healthcare providers treat application security and infrastructure security independently.

The article provides review of security risks related to sensitive data in telemedicine (chapter 2), Polish regulations in the area of medical records protection (chapter 3) and security measures that can be used to protect them (chapter 4). The last chapter provides summary of the guidelines for protection of telemedicine services.

Security risks related to sensitive data in telemedicine

Government regulations, electronic health records, and new Internet health services create numerous security challenges for healthcare compliance and information security teams.

According to Reuters (September 2014)[1] medical information is worth more to hackers than a credit card number on the black market. The data for sale includes names, birth dates, policy numbers, diagnosis codes and billing information. Fraudsters use this data to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers, according to experts who have investigated cyber attacks on healthcare organizations.

Medical identity theft is often not immediately identified by a patient or their provider, giving criminals years to use such credentials. That makes medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected.

According to an Annual Benchmark Study on Privacy & Security of Healthcare Data by the Ponemon Institute think tank from 2014[2], the percentage of healthcare organizations that have reported a criminal cyber attack has risen from 20 percent in 2009 to 40 percent in 2013. This trend continues. The latest annual report from 2016[3] emphasizes that data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. Based on the results of this study, there has been estimated that data breaches could be costing the healthcare industry $6.2 billion in 2016. Nearly 90 percent of healthcare organizations represented in this study had a data breach in 2014-2015, and nearly half, or 45 percent had more than five data breaches in the same time period. The majority of these breaches were small, containing fewer than 500 records. The report emphases that no healthcare organizations, regardless of size, are immune from data breach and are even more vulnerable than other industries. Despite this, about half of all organizations have little or no confidence that they can detect all patient data loss or theft.

For the second year in a row, in 2016 criminal attacks are the leading cause of data breaches in healthcare. In fact, 50 percent of healthcare organizations say the nature of the breach was a criminal attack and 13 percent say it was due to a malicious insider.

Indeed, cyber attacks remain a primary concern for healthcare organizations. In 2016, ransomware, malware, and denial of-service (DOS) attacks are the top cyber threats facing healthcare organizations. They were also significantly concerned about employee negligence, mobile device insecurity, use of public cloud services, and employee-owned mobile devices or BYOD (Bring Your Own Device) - all threats to sensitive and confidential information.

Polish regulations

Patient data confidentiality continues to grow as a leading concern for healthcare organizations. In Poland this has been regulated by the Personal Data Protection Act (from 29th August 1997 with subsequent changes) [4] in which health records fall into broad category of sensitive data the access to which in general is prohibited. One of the special situations when data processing is allowed is during realization of medical services (also telemedicine), however such data must be specially protected from unauthorized access. Processing of data is defined as all operations regarding personal data like gathering, saving, storing, modification, releasing, and deleting.

Regulation of the Minister of Health in terms of Electronic Health Records System (from 6thJune 2013)[5] indicate the necessity of implementation of the security management system that should meet requirements of the Public Entities Computerization Act and specifically – follow ISO/IEC *27002 Information technology – Security techniques – Code of practice for information security management standard*.

ISO/IEC 27002 provides best practice recommendations on information security management for people responsible for initiating, implementing or maintaining information security management systems. It covers 14 security controls describing their objectives and implementation guidance. In the remainder of this paper, 5 of them will be presented in more detail: access control, cryptography, protection from malware, technical vulnerability management and communications security.

Protection of sensitive data in telemedicine services

According to the Personal Data Protection Act, protection of sensitive electronic medical records must be performed during the whole cycle of data processing. Additionally Regulation of the Minister of Health in terms of Electronic Health Records System indicates that the control over this process must rely on the process of information security management, performed according to ISO/IEC 27002 standard. That is why the problem of protecting sensitive data has been described in two dimensions, taking as example 3 data processing steps: release of information, their storage and modification, as well as 5 suggested security controls: access control, cryptography, protection from malware, technical vulnerability management and communications security.

Information release

In general – all telemedicine services rely on information release. Patients' electronic records are made accessible remotely through the network to the patient himself or to his physician for monitoring purposes, additional diagnosis or statistics. Since the whole process involves several devices (i.e. end - user device; server – with telemedicine service running) and networks (usually – Internet, and possibly some internal inter-hospital network), the process of secure information release relates to two sub processes: access control and communications control.

Access Control

First of all, sensitive medical records can be released only to the authorised parties. In general this would be the patient himself and his physician, taking care of the patient. It is necessary therefore to provide identity management in the system that would allow to define user identity together with his role in the system. Based on this information it is possible to design and implement authentication service – for verification of WHO is trying to access particular electronic record. This mechanism can rely on a simple tuple: username and password used to log into the system. The simplicity of this solution is its big advantage (does not require much effort from the user), however this can also be a drawback:

- easy password can be guessed
- people tend to write passwords down where they can be easily accessible
- it is possible to perform brute force attack on the system to find out the password of the user.

That is why in the public domain it is more and more common practice to use qualified X.509 certificates to identify the user, confirmed by a trusted third party (certification authority – in Poland e.g. Certum, PWPW Sigillum).

Additionally, on the basis of the confirmed user identity and his role (e.g. patient, clinicist, researcher, manage-

ment) – authorization service is able to decide whether a user is actually allowed to access particular record. This mechanism must be tailored to the logic of the service taking into account necessity of data anonymization when it is to be used for the purpose of statistics (usually also for researches).

Communications control

Information, while transferred over the network can be subject to e.g. eavesdropping and modification. Information release imposes therefore the necessity to provide:

- Integrity of released information – making sure the information released has not been changed on its way to the requestor, and
- Confidentiality – making sure the information has not been available to any other parties than the authorised during its transfer to the requestor.

Integrity can be realised with the use of digital signature based on the aforementioned qualified X.509 certificates. The digital signature is attached to the requested information. It is calculated with the use of asymmetric cryptography and the keys generated from the X.509 certificate (so called public key – available publicly, and private key – that must be stored securely by the owner – usually on a smart card protected with a secret PIN number). The algorithm allows the sender X to create a hash from the message, and then encrypt it with its private key (known only to the sender). Then if the remote site is able to decrypt the signature, it believes that it is a valid digital signature from sender X. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

The information, while being sent through the network, can be eavesdropped. This is especially important when the devices are using wireless connections with shared wireless medium (often unprotected Hot Spot WiFi) and when the traffic can be easily captured and read.

Confidentiality of information can be provided with encrypting the information itself or encrypting the communications channel. This also can be done with the use of digital certificates. Public key of the requestor can be used to encrypt the information. After that only the requestor will be able to decrypt the message (with its private key). X.509 certificates can be also used to encrypt the communications channel (using e.g. TLS or SSL connections with one side or mutual authentication).

Another important subject that must be emphasised when discussing information release is non-repudiation. All actions on sensitive information data stores (who accessed which information, with timestamp) must be properly logged for further audit.

Information storage

Sensitive health records are usually stored in databases the protection of which is crucial. It is highly recommended to enforce encryption of data at storage which provides both confidentiality and integrity as well as makes the attempts to read stolen database unsuccessful. Of course sensitive data, after being received from the service, are also stored at user devices. These can be both office computers that are used in hospitals and other medical facilities, but also smartphones, more and more often – private devices used also for official matters. This attitude is usually called "Bring Your Own Device" (BYOD) and is perceived by security specialists as particularly risky due to a very fast growth of threats targeting mobile devices and very careless use of smartphones, which should be treated as personal computers. Each mobile device must have at least antivirus software running. It is also highly recommended to apply for using telemedicine services so called protected profile which allows to encrypt data processed while it is activated.

Information protection

Protecting the confidentiality, integrity, and availability of patient information is a complex task. A foolproof solution must secure both the clinical applications and the underlying IT infrastructure. Dozens of healthcare personnel—registration, accounting, nursing, physicians, technicians, and associates—have access to clinical applications. To safeguard patient privacy, healthcare providers must monitor access to applications and protect against inappropriate data disclosure without impeding legitimate use or obstructing patient care.

The security specialists[6,7] emphasize that implementation of access control, encryption, audit mechanisms are not enough. The overwhelming inflow of security threats, new attack paths and malware types cause that application-layer surveillance alone is not sufficient. Providers must also monitor underlying IT systems (implementing security management system) , employee communications, and endpoints for policy violations. A rogue administrator can avoid an application-centric privacy monitoring solution by accessing raw patient records from databases or network storage devices. However sensitive data can also be leaked via email, chat, removable media, or something as simple as printing patient records in a public area.

	Privacy Monitoring	Security Information and Event Management
Purpose	• Patient privacy	• Network and system security
Focus	• Internal threats • Clinical applications	• Internal and external threats • IT infrastructure
Examples	• Medical record snooping • Internal identity theft	• Malicious attacks (viruses, worms, Trojan horses) • External identity theft • Eavesdropping
Audience	• Privacy and compliance personnel • Business-oriented	• Information security personnel • Technology-oriented
Audit Sources	• Clinical applications	• IDS, IPS, firewalls, AAA, switches, routers
Managed Attributes	• Patient, user, and department function codes	• IP addresses, MAC addresses, TCP/UDP ports

Figure 1. SIEM vs Privacy Monitoring by MacAfee[6]

Many healthcare providers treat protection of sensitive data in compliance with government regulations and infrastructure security independently. The functions are performed by separate teams using separate tools. However in order to safeguard the data in the whole cycle of processing these two approaches must be combined. Both privacy officers and security officers need to meet the same regulations and both have a stake in ensuring patient privacy and the integrity of the healthcare systems. Yet what has been lacking is a common set of tools to identify and isolate threats and a way to correlate clinical application events with IT infrastructure events. Such tools are called security information and event management (SIEM) solutions. They identify, collect and analyze important events observed in the network and systems itself and protect against both internal and external threats.

According to MacAfee[7] (see Figure 1.) collective defence based on SIEM is able to identify eavesdropping, external identity thefts and hidden activity of different malicious attacks (caused by viruses, worms or Trojan horses) whereas privacy monitoring alone can only recognize e.g. medical record snooping or internal identity thefts.

Summary

Protection of sensitive data in telemedicine services must follow the best practice of IT security based on standards. Increasing value of patients records on the black market and growing number of threats to computer systems make it necessary to use advanced solutions known from IT systems for cyber defence. It is necessary to implement security management system following ISO/IEC 27002 standard targeting all security dimensions. One of them is also a security culture of the personnel that should be aware of the risks that are related to their behaviour and use of computer devices. There is no single technology solution or best practices guideline that will achieve success without a security culture apparent to all medical practitioners in the organization. It is necessary to carry out periodic trainings presenting both security threats as well as required behaviour of personnel in relation to medical records.

References

1. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card, Reuters. Sep 24, 2014
2. Fourth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute LLC. March 2014
3. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute LLC. May 2016
4. Personal Data Protection Act (from 29th August 1997 with subsequent changes)
5. Regulation of the Minister of Health in terms of Electronic Health Records System (from 6th June 2013)
6. Roberts TL, Electronic Medical Records: Success Requires an Information Security Culture. SANS Institute InfoSec Reading Room; 12/2012
7. Security and Privacy of Electronic Medical Records, MacAfee white paper. 2011