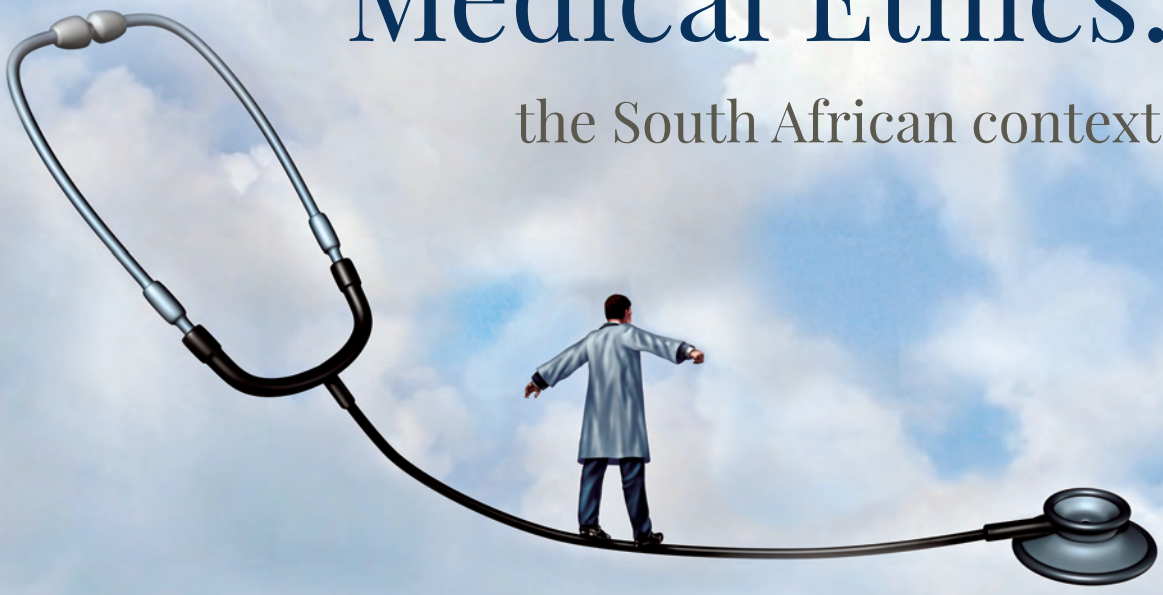
C. Jones, M. Kruger, J. van den Heever & A. van Niekerk (eds.). Challenges in Medical Ethics: the South African context. Stellenbosch: African Sun Media

Challenges in Medical Ethics:

the South African context



Editors:
Chris Jones, Mariana Kruger, Juri van den Heever & Anton van Niekerk

https://doi.org/10.52779/9781991201959/13

C. Jones, M. Kruger, J. van den Heever & A. van Niekerk (eds.). Challenges in Medical Ethics: the South African context. Stellenbosch: African Sun Media

13

Cyberspace-related Risk Aspects in the Medical Ecosystem

Basie von Solms

Keywords: cybersecurity; cybersecurity governance; cybersecurity risks; cyberspace; internet of medical things (IoMT); medical ecosystems; medical ethics

13.1 INTRODUCTION

New developments in technology have, over the ages, always been core drivers in the dramatic improvement in all areas of health care. Such developments include the availability of newer and more effective drugs, the possibility to implant a stent and a pacemaker in the body to address a problem which, only a few years earlier, may have needed a massive invasive operation. Technological developments, operating in what we today experience as 'cyberspace', have already become massive new drivers in improving health care, and will continue to do so at a dizzying pace in coming years. However, as has always been the case with any new technology, there are always risks which must be managed as comprehensively as possible to prevent the new technology from causing negative consequences.

In this chapter, we will try to give an overview of how cyberspace has already impacted the medical ecosystem, and what are some of the important risks which must be identified and managed.

The chapter is structured as follows:

- Some technical background
- Risks in cyberspace and attack methods
- Examples of cyberattacks on hospitals and medical devices

https://doi.org/10.52779/9781991201959/13

- Cybersecurity measures to mediate the risks of a cyberattack
- The internet of medical things (IoMT)
- Online operations and surgical robots
- Medical ethics and cybersecurity
- A cyber-incident response plan (CIRP) in the medical ecosystem
- Cybersecurity governance in the medical ecosystem
- Conclusion

We start off by giving some technical background used in this chapter.

13.2 SOME TECHNICAL BACKGROUND

13.2.1 Defining a few concepts

As background to sections in this chapter, some concepts must be defined. While many definitions do exist, and many different definitions can be provided from existing literature, the definitions which are provided below are mostly based on the author's personal experience of the relevant concept over many years and may therefore be criticised by the 'purists'. Nevertheless, the purpose is to make concepts as understandable as possible and is specifically directed at the non-technologists.

- The internet: In its simplest form, the internet can be visualised as millions of computers and computing devices connected via millions of computer networks. Such computers include big enterprise type computers, desk top computers, laptops, tablets, smart phones, and many more. The internet can therefore be seen as purely an interconnected technical infrastructure on which more advanced applications can be built.
- The World Wide Web (WWW): On every one of the computers and devices making up the internet, there may reside databases containing data, information, and software. In its simplest form, the WWW can be seen as all these databases, and therefore the data, information, and software in these databases, connected via the internet infrastructure. The WWW is therefore built on the underlying internet infrastructure.
- Cyberspace: Again, with the risk of oversimplifying, cyberspace can be seen as the internet and the WWW together. This means that cyberspace can be seen as everywhere where there is some computing device connected to other computing devices. This *interconnectedness* is maybe the main characteristic of cyberspace. In this chapter, we will specifically investigate risks which arise because of this *interconnectivity*.

https://doi.org/10.52779/9781991201959/13

- Cybercrimes: Cybercrimes are crimes performed in and through cyberspace.
- Cyberattacks: Cyberattacks are the methods and actions used by cybercriminals to break into (hack) computer and data systems to perform cybercrimes.
- Ransomware attack: This is an attack method used by cybercriminals in which the computer system of a company is penetrated, and all the data stored and managed by the computer system is encrypted. This makes such data inaccessible and unavailable to the authorised users. In most cases, a ransom amount is then demanded by the criminals to restore the data to useable format.
- Malicious software (Malware): Malware is unauthorised software which can be loaded onto compromised computers, phones, and intelligent devices to perform unauthorised actions.
- Cybersecurity: Cybersecurity is an encompassing term referring to all actions and measures implemented to protect computer and data systems against cyberattacks.
- The Internet of Things (IoT): Because of the interconnectivity of cyberspace, more and more (small) devices like sensors are connected to it, making it possible to monitor and manage such devices remotely. Such devices may be simple sensors measuring for example rainfall, temperature, and more. This 'extended' cyberspace is called 'the internet of things' where these 'things' refer to the connected devices and sensors.
- The Internet of Medical Things (IoMT): The IoMT can be seen as a subset of the IoT covering the collection of medical devices and applications that connect to health care IT systems through cyberspace. In this case, the 'Things' are medically related sensors, equipment, and more.
- Cyberspace-based Medical or Health Care Ecosystem: The cyberspace-based medical ecosystem can be seen as an infrastructure (people, enterprises, devices, computer systems, and more) that use cyberspace and the Yom to deliver, monitor, and manage health care services.
- The Cloud: The cloud refers to servers and databases that are used to store data, but are not on the same site where the data is provided or captured from. These servers and databases are accessible via cyberspace. This means that you store your data somewhere in cyberspace without actually knowing where the server of database is situated. Cloud service providers provide and manage such services.

As this chapter is all about the cyber risk aspects related to the medical ecosystem, including the attack methods used by cybercriminals, it is good to first understand the general risk aspects in cyberspace we are exposed to every day and

https://doi.org/10.52779/9781991201959/13

the attack methods used. This will help as many of such risks and attack methods are exactly the same as those experienced in the medical ecosystem. In the next paragraph, we will investigate cyber risks and attack methods. There are many such risks and attack methods, but we will concentrate on just a few.

13.3 RISKS IN CYBERSPACE AND ATTACK METHODS

Because of its interconnectedness, cyberspace provides a good platform to cybercriminals to launch cyberattacks through. They may launch an attack on a system on the other side of the world from where they are physically located, as the specific targeted system can be reached through cyberspace. As an example, image a hospital in country X having a website. The website allows anybody in the world to access the website and get information about the specific hospital. For this reason, a cybercriminal in country Y, thousands of kilometres away from country X, can access this hospital's website, and try to penetrate the rest of the hospital's medical ecosystem to perform unauthorised actions.

Cybercriminals have different reasons why they attack and hack computer systems, and we will concentrate on two such reasons – getting access to personal and other types of data and getting access to some electronic device to use as a springboard for further unauthorised actions. We will now briefly discuss these two reasons.

13.3.1 Getting access to personal and other types of data

Data has become extremely valuable, and criminals want to get access to different types of data which they then sell or use in ways to force the owners of the data to react to their demands. They can get access to such data by different means, including directly hacking into the central database or trying to get (steal) the login data from a user of the company. They then use this login data to perform an (unauthorised) login to the system, masquerading as the user.

In particular, personal health data is very high on their list, and therefore attacks on medical databases are common. Such stolen medical data can be used to blackmail a patient whose data was stolen, or even to blackmail a whole hospital through a ransomware attack. In other cases, they use personal medical data to try to get login parameters to the patients' financial systems, and even to misuse stolen electronic scripts to get illegal drugs.

As explained above, the interconnectivity of the medical ecosystem just increases this risk as personal patient data can be collected from different places, sent between different systems, shared between different doctors and medical staff, and stored in different places.

https://doi.org/10.52779/9781991201959/13

Furthermore, the Yom will have many more devices and sensors connected to the care of a patient, and all the data captured by such devices is being sent along networks and even cyberspace. There are national initiatives by countries to force health care providers to upload all patient data to a central data base managed by some central body. Such a database will be a treasure trove for cybercriminals and needs excellent security and protection.

Interconnectivity in cyberspace has massive benefits for the medical ecosystem, but also carries massive risks in terms of patient and related medical data (Green, 2018; Khalik, 2018).

We will expand on these aspects later in the chapter.

13.3.2 Getting access to electronic devices, sensors, and other components of the IoMT

With more and more people doing banking via cyberspace and online systems, cybercriminals are committed to getting access to a client's smart phone to steal the client's login details. This is done by infecting the smart phone with malicious software. This software now waits until the client logs into an online bank account, captures the login information, and sends it back to the cybercriminal. Apart from using the stolen login information in an unauthorised way, or planting malware on the user's phone, the criminals can try to intercept the communication between the phone and the bank, for example changing the bank account number the client intended to transfer money to.

Any device, sensor, or 'thing' connected to cyberspace can potentially be misused in the way described above, and many other ways too. In the Yom, many such devices already exist and will just increase in number in the future.

Pacemakers are intelligent devices that are implanted in a person's body to help control their heart's rhythm. In many cases, such pacemakers have built-in communication facilities that can communicate back to the physician via cyberspace and provide data in real time. The physician, which may be hundreds of kilometres away, can now monitor the person's heartbeat, and in emergencies, even send a message to the device to perform a specified emergency action like increasing the rhythm.

Just like the smart phone above, such a pacemaker or the communication between the pacemaker and the doctor can be hacked. Malicious software can be loaded on the pacemaker, or the doctor's commands to the pacemaker can be changed, causing potential deadly consequences. In 2013, former US Vice President Dick Cheney's doctors disabled his pacemaker's wireless capabilities to thwart terrorists and possible assassination attempts (Vaas, 2013).

https://doi.org/10.52779/9781991201959/13

More and more people today use different forms of health and fitness monitoring devices. The main benefit of such devices is that they can be interconnected into the medical ecosystems and are therefore all components of the IoMT.

> Wearable medical devices and home health monitoring devices are becoming more prevalent among patients of all ages. These devices allow vital data to be transmitted from a patient's home directly to hospital and other health care staff, resulting in real-time monitoring of a patient's health. (Ronte, Taylor & Haughey, 2018)

Such sharing of often very sensitive medical data creates motivation and reason for cybercriminals to try to compromise such systems to get their hands on the sensitive data.

Within the IoMT, such risks will grow as more and more devices are used to monitor, control, and manage patient health care in the medical ecosystem. Cyberattacks against such Yom components will grow and become more sophisticated.

> […] cybersecurity issues are pervasive across medtech (medical technology), as the increasing numbers and capability of connected medical devices present additional risks for data security. (Ronte et al., 2018)

We will expand on these aspects again later in this chapter but will in the next section firstly investigate a few examples of how these risks were exploited in real life.

13.4 EXAMPLES OF CYBERATTACKS ON HOSPITALS AND MEDICAL DEVICES

In subsection 13.3.1 above, we considered the cyberattacks to steal data and, in our context, medical data. In this section, we will first look at the theft of personal medical data, and then at the compromise of medical equipment. It is claimed that medical data is up to 10 times more valuable than a credit card number (Alpine Security, 2021).

Attacks to steal personal medical data can happen on an individual level, where a specific person's sensitive medical data is compromised, and the person is blackmailed. Such an event occurred in Finland where a database of a clinic was compromised, and the data used to blackmail individual patients (Sipilä, 2020).

The attacks can, however, also be made directly on a health institution, where the medical database of the institution is hacked, and the whole database is encrypted through a ransomware attack. This makes all the data unavailable to all concerned. A ransom amount is then demanded, and if paid, the data may

https://doi.org/10.52779/9781991201959/13

be decrypted to be used again, but in many cases paying the ransom does not solve the problem. Such an attack can of course have a devastating effect on the institution's medical infrastructure and the relevant patients.

> Cybercriminals have begun to target the healthcare industry with ransomware – malware that encrypts an infected device and any attached devices or network drives. After encryption, cybercriminals demand a ransom before releasing the devices from encoding. Without adequate disaster recovery and backup plans, many businesses are forced to pay the ransom. (Aver, 2021; Spence et al., 2018)

Several cases have been reported where such a ransomware attack caused the death of patients.

> German authorities are investigating the unknown perpetrators on suspicion of negligent manslaughter, the Associated Press, German news outlet NTV, and others reported. The event under investigation occurred last Friday when the unidentified woman was turned away from Düsseldorf University Hospital because a ransomware attack hampered its ability to operate normally. The woman was rushed to a hospital about 20 miles away, resulting in about a one-hour delay in treatment. She died. (Goodin, 2020)

In subsection 13.3.2 above, we considered cyberattacks on devices. Cyberattacks will of course make medical data unavailable, as discussed above, but can also compromise medical devices and equipment. Such devices and equipment are mostly intelligent devices, meaning they are computers themselves, and if their software is compromised, they cannot operate. As part of the IoMT, many devices are connected to a hospital's computer system. This interconnectivity creates risks as a cyberattack on a specific device can potentially spread to the rest of the equipment in the hospital, and make them unavailable (Miliard, 2021; Rothschild, 2020).

Many more examples of compromised medical systems have been reported, and the question now is of course how to protect oneself against such attacks. We will expand on this in the next section.

13.5 CYBERSECURITY MEASURES TO MEDIATE THE RISKS OF A CYBERATTACK

Cybersecurity is a very big and important field as cyberattacks are growing daily. A report from McAfee estimated that global losses from cybercrime topped $1 trillion in 2020, and they are expected to skyrocket to more than $6 trillion in 2021, according to a report produced by Cybersecurity Ventures, which was sponsored by Intrusion (Morgan, 2017).

https://doi.org/10.52779/9781991201959/13

Furthermore, as mentioned above, hospitals and medical institutions are becoming a growing target for cyberattacks (Weiner, 2021). "Healthcare has become the most targeted industry for cybercriminals" (Steger, 2020). Hospitals should therefore be specifically wary and ensure that their cybersecurity and cyber protection are based on internationally accepted best practices such as the ISO 27000 series of documents (Irwin, 2020).

It is not the purpose of this chapter to extend too deeply into cybersecurity practices, but institutions must understand a number of important aspects related to cybersecurity attacks. Firstly, there is no such thing as 100% cybersecurity. No enterprise, or hospital, can totally prevent cyberattacks – the best that can be done is to lower your cyber risks as much as possible, and manage the cyber risk environment constantly and as comprehensively as possible.

Secondly, no cybersecurity plan can be based on technology only. Products such as firewalls, anti-virus software, and more are essential, but is not sufficient. The human part of cybersecurity is just as important. Reports claim that more than 90% of successful hacks against a company has a human origin. Creating a cybersecurity culture in the company where every employee is cyber aware and knowledgeable on how to recognise and prevent a cyberattack is maybe the core of a good cybersecurity plan. "A holistic approach designed with people at the heart – Did you know that people are the single biggest risk factor to cyber-attacks? Many organisations overlook the human side of cybersecurity" (Deloitte, 2020).

Thirdly, it is essential to understand that cybersecurity is a corporate governance responsibility. This means that the accountability for cybersecurity resides with the board of directors of the company – the buck stops right at the top! We will expand on this aspect in section 13.10 below on cybersecurity governance in the medical ecosystem.

In the next section, we expand the concept of the internet of medical things.

13.6 THE INTERNET OF MEDICAL THINGS (IoMT)

As the concept of the IoMT is crucial to modern integrated health care, and as components of the IoMT are open to cyberattacks, we have to discuss the concept in more detail.

As briefly defined in subsection 13.2.1 above, the IoMT can be seen as a collection of medical devices, interconnected via networks (and cyberspace). These devices may be individual sensors connected to a patient. For a specific hospital,

https://doi.org/10.52779/9781991201959/13

it may be medical devices on site, but also remote medical devices, all connected to a central computer and database within the hospital. These devices can collect data directly, and then send that to some central processing computer and data store. The data may also be stored in the cloud, which can cause further risks.

Examples of such medical devices may be a range of sensors connected to the patient, including devices to monitor parameters such as heart rate, respiration, blood oxygen saturation, skin temperature, blood glucose, blood chemistry, and body weight. Furthermore, parameters like behavioural parameters (e.g., motion, acceleration, mood) linked to health and well-being can also be collected (Mittelstadt, 2017).

Many of these devices may be in the physical hospital environment itself, but many may also be remotely located, for example fitness devices which patients can wear at any place and any time. Such collected data are then transmitted via cyberspace, and other network technologies, to some central computer.

Figure 13.1 below gives some idea of the IoMT (Dilawar, Rizwan, Ahmad & Akram, 2019).

It is widely reported that medical devices and components of the IoMT often do not have very good cybersecurity protection and are hackable.

> More than 60 percent of all medical devices are exposed to some degree of risk, according to a recent report from healthcare cybersecurity company CyberMDX. It's crucial, then, for healthcare systems to understand the vulnerabilities of Yom tools and how to protect them – both today and in the future. (Kawamoto, 2017; Steger, 2020)

According to Critical Insight (n.d.), the top six hackable medical IoT devices are:

- Infusion and insulin pumps
- Smart pens
- Implantable cardiac devices
- Wireless vital monitors
- Thermometers and temperature sensors
- Security cameras

The IoMT is an essential component of comprehensive health care in the future, but does have significant risks, including cyber risks attached, which will have to be managed and regulated very well.

https://doi.org/10.52779/9781991201959/13

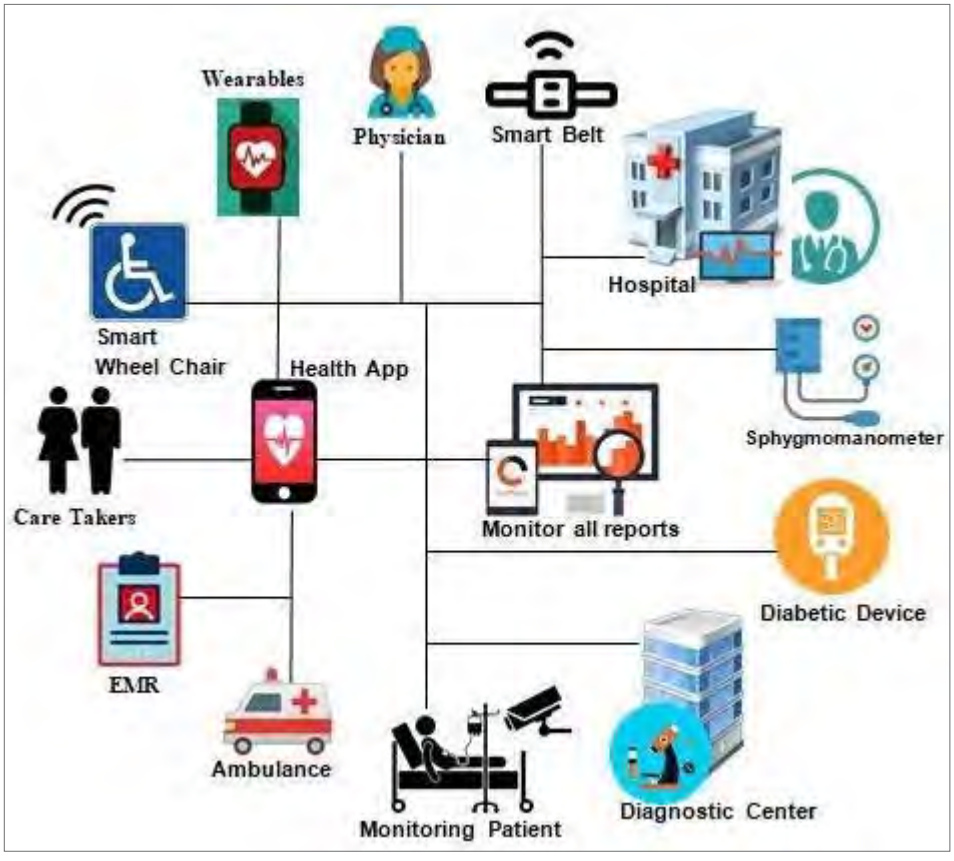


FIGURE 13.1: The internet of medical things (IoMT)

13.7 ONLINE SURGICAL OPERATIONS AND SURGICAL ROBOTS

In this day and age, robotic surgery is performed regularly. The patient is surrounded by different robots, controlled from an onsite surgeon, using controls and screens connected to the robots. This connection is via dedicated data transmission cables directly connecting the robots to the surgeon's control centre. The surgeon's instructions reach the robots nearly immediately and the surgeon always has full and direct control. The surgeon can now manipulate the robots through the controls to perform the delicate activities required for the operation. Prostate operations have been performed very successfully in this way (Intuitive, n.d.).

When the surgeon and the patient are in different locations, maybe in different cities, this approach becomes much more difficult, complex, and risky. Although the setup is identical as described above, direct dedicated transmission lines are

https://doi.org/10.52779/9781991201959/13

not always possible. The surgeon's instructions are sent to the robots via cyberspace. A core requirement for this approach is of course the speed of the communication network, as any delay can cause disaster and even death. With the advancement in 5G communication systems, the required speed is theoretically possible – this makes online surgical operations possible where the surgeon and patient are in different locations.

The potential benefits of such interventions should be clear – the expertise of skilled surgeons can now be used more widely, and surgical operations can now be performed in rural hospitals where surgeons with the specific necessary skills may not be available (Madder, 2020). This approach has the promise to provide experts with specialised surgical interventions in remote areas, which would otherwise not be possible. The technologies of the 4th Industrial Revolution make such approaches viable, "delivering top-tier surgical expertise anywhere in the world" (Amerding, 2015).

Although such approaches sound exciting, using cyberspace confronts it with all the inherent risks associated with cyberspace discussed in this chapter. In many cases such online operations using surgical robots will be cases where interruptions can be life threatening, and even fatal. Multiple risks exist, of which availability and speed of the network connection between the surgeon and the hospital are crucial. The network connection can be lost at a crucial stage during the operation, or the connection may suddenly slow down – both with potentially fatal consequences (Madder, 2020).

Cybercriminals are of course aware of all these risks and implications and can launch a cyberattack on the communication network between the surgeon and the hospital and take it off the air or deliberately slow it down. Furthermore, if the communication network is not properly secured through advanced encryption, the integrity of the data flowing over the network can be compromised. The cybercriminal can hack into the network and change the instructions sent by the surgeon to the robot, causing the robot to perform incorrect and potentially dangerous actions. Reports do exist of cybersecurity researchers which successfully hacked into and hijacked a surgical robot. This stopped the robot and made it impossible for the surgeon to continue (Storm, 2015).

Therefore, although such online operations using surgical robots have immense potential, severe cybersecurity-related risks must still be addressed and resolved. In the last instance, it must also be accepted that no systems operating in cyberspace can be 100% secured – there will always be the potential that cyberattacks can be successful. There may be some ethical aspects related to this approach of online operations and surgical robots, and that will be addressed in the next section.

https://doi.org/10.52779/9781991201959/13

13.8 MEDICAL ETHICS AND CYBERSECURITY

13.8.1 Background

The normal definition of cybersecurity is that it is the people, processes, and technology needed to ensure the confidentiality, integrity, and availability of data in cyberspace. In a financial environment that may mean that a bank must ensure that clients' financial data is protected against unauthorised persons viewing it (confidentiality), their financial data must be protected against unauthorised changes (integrity), and their financial data must be available when they need it (availability) – the CIA principle. In this scenario, the bank does not really have to worry about the client's personal safety and that cyberattacks on the bank will have a direct effect and impact on the client's life and safety. The cybersecurity officer of a bank can, with little risk, decide to take the bank's whole computer system offline if a cyberattack is noticed, or to contain such an attack. Furthermore, financial institutions have developed very strong cybersecurity protection measures for lowering the risk of unauthorised access to client's data, and also have a more 'closed' environment of employees who may have access to the bank's computer systems – therefore, although the risk is never eliminated, it can be lowered significantly in such a financial environment.

However, this totally changes when we look at medical and health care data in the IoMT. Cybersecurity in medical ecosystems has potentially a much more direct impact on patients' safety and even their lives. ICU ventilators are very good examples of a type of equipment which can be seen as life supporting (Kacmarek, 2011). Many more hospital employees have access to the devices and sensors connected to the hospital's computer systems, and many of them may not be very aware of the risks and possibilities of compromising sensitive private patient data. In section 13.4 above, we gave brief examples of what such consequences can be.

The ethical dilemma when the medical ecosystem is involved, is much more complex. Three aspects will now briefly be investigated:

- the security and privacy of patient data
- the cybersecurity management of the IoMT
- the security of medical sensors.

https://doi.org/10.52779/9781991201959/13

13.8.2 Ethical decisions related to the security and privacy of patient data

As indicated in section 13.2 above, medical personal data is extremely valuable, and is a growing target for cybercriminals. Very often, personal medical data is collected from many locations, and not only in a hospital. It is therefore much more difficult to secure all this data during transmission and storage. In many cases, for example in an emergency, such data can be collected, transmitted, stored, and processed without the knowledge and approval of the patient. This can result in ethical questions and even legal consequences.

The amount of data captured through all such sensors and devices is immense and will just keep growing. New ways of storage are needed for these masses of data and using the cloud has become a very obvious choice. Cloud storage creates its own security and protection problems, many of which are not yet properly solved. This stored patient data can also be accessed by a much wider group of medical staff, increasing the risk of unauthorised access and misuse.

Some ethical questions, which do arise in such a case, include:

- Is all the data collected about a patient really necessary?
- How are patients involved in decisions to collect, store, and process their data?
- How can the patient be assured that such collected data is not misused?
- How can the number of people having access to a patient's data be limited to enforce better access control?

Surely, such questions have a strong technical implication, but in this case, ethical aspects also play a major role. As discussed in section 13.10 below, these ethical aspects must be part of the governance in the medical ecosystem and must therefore be addressed at board level.

13.8.3 Ethical decisions related to cybersecurity management of the IoMT

The cybersecurity officer of a major hospital must make much more difficult and sensitive decisions. Suppose the officer notices a cyberattack on a life-supporting system used by patients and connected to the hospital's computer system network. Suppose further this life-supporting system is at that moment supporting some patients in real time. The officer must now make some serious decisions and take action to contain the attack.

On the one hand, the officer can take the life-supporting system offline to contain the attack and prevent it from spreading to other connected systems. This may, however, risk the lives of the patients connected to the specific life-supporting

https://doi.org/10.52779/9781991201959/13

system. On the other hand, the officer can leave the life-support system online but risk infecting the hospital's wider networks and computer systems. This decision is eventually not just a cybersecurity decision (as the bank's cybersecurity officer could decide), but also has serious ethical consequences. The hospital's cybersecurity officer, who is basically a technical person, must now make a decision which may have life and death implications. There is no way this officer can do that alone. The whole medical ecosystem of the hospital, interconnected to the hospital computer systems, the IoMT, and staff are now all involved in a basically technical cyberattack and cybersecurity decision. Medical ethics and cybersecurity have now become integrated as far as management and decisions are concerned.

13.8.4 The ethical decisions related to the security of medical sensors

Very often medical sensor devices themselves do not have built-in cybersecurity protection, and then they are nevertheless implemented without proper security protection, endangering the privacy and lives of patients. "Medical IoT devices have great benefits to patient care but can leave medical centers and hospitals wide open to cyber-attacks" (Archon, n.d.).

The question now should be: is it ethical to install medical sensors if it is known beforehand that they may have serious security flaws, which can impact on patients' privacy and security? To address this aspect, before implementation, it must be ensured that all such devices are robustly designed, reliable, and secured cybersecurity-wise. This is not only a technical issue but also an ethical one, which demands input and consent from top management. This is an important aspect, discussed in section 13.10 below on cybersecurity governance in the medical ecosystem (Mittelstadt, 2017).

13.8.5 Summary

Medical ethical aspects within the IoMT are growing and will keep growing as new devices are developed and implemented. The relationship between cybersecurity and ethics in the IoMT must get more attention and must be accepted as a core component of the medical ecosystem. "Medical ethics can no longer be separated from cybersecurity in healthcare" (Frenz, 2021).

Taking all these risks and concerns into account, it is very important in the medical ecosystem to have a cyber-incident response plan. Quick and well-planned actions in the case of a cyberattack are essential for the safety and well-being of everyone, especially the patients. This matter is discussed in more detail in the next section.

https://doi.org/10.52779/9781991201959/13

13.9 A CYBER-INCIDENT RESPONSE PLAN IN THE MEDICAL ECOSYSTEM

As mentioned in the previous paragraph, a cyberattack on the medical ecosystem and the IoMT can potentially result in death. It is therefore irresponsible not to be properly prepared for such an eventuality, and to act with the greatest speed.

It is important for any company exposed to cyberattacks to have a cyber-incident response plan (CIRP). Such a plan provides clear guidance on what must happen if a cyber-incident occurs. For the medical ecosystem, such a CIRP is even more important. The example discussed above about decisions to be taken if a cyber-attack happens is an example of why a CIRP is essential. Of course, it is important to take preventative action to prevent any cyberattack as far as possible, but more is needed. A CIRP must clearly spell out what must be done if such an attack does happen – at that point in time, everybody should know immediately how to react. Such plans are a normal plan demanded by security good practices but is often lacking in the medical ecosystem (ECRI, 2020). This aspect is again mentioned in the following section.

13.10 CYBERSECURITY GOVERNANCE IN THE MEDICAL ECOSYSTEM

13.10.1 Background

Cybersecurity governance is a component of corporate governance, meaning the responsibility and accountability of cybersecurity governance lies squarely on the shoulder of the board of a company (Fortium, 2017; Price, 2018a; Scholtz, 2021).

The main objective of corporate governance is to provide direction and guidance in a company, including:

- Determining the strategic direction and objectives of the company;
- Ensuring that the necessary policies, procedures, and resources are in place to achieve the strategic objectives;
- Overseeing and ensuring that the strategic objectives are accomplished (WHO, 2014); and
- Understanding the relevant ethical aspects and be prepared to act properly.

International good practices for corporate governance emphasises that cybersecurity governance is a core component of corporate governance. If the company operates in cyberspace in any way, the implication is therefore that the accountability and responsibility to ensure that all data, transactions, and operations are cyber-secured, resides with the board. In cyberspace, the board must understand

https://doi.org/10.52779/9781991201959/13

and accept that cybersecurity governance is not (only) a technical issue, but a business risk management issue where the buck stops in the boardroom.

Cybersecurity governance in the medical ecosystem involves all of the above but includes more – this makes it even more essential that the board of a health care institute making use of the IoMT must take on this responsibility and accountability. As already noted in section 13.8 above on medical ethics and cybersecurity, the involvement of the IoMT can cause certain situations where life and death are at stake, and where the final decisions are actually that of the board. This aspect is emphasised by stating that operating in the IoMT requires the extensions of existing governance mechanisms to ensure safety and security (Skierka, 2018).

> Cybersecurity is an essential part of maintaining the safety, privacy and trust of patients. More money and effort must be invested into ensuring the security of healthcare technologies and patient information. Security must be designed into the product from conception and not be an afterthought. Cybersecurity must become part of the patient care culture. (Coventry & Branley, 2018)

This is basically what cybersecurity governance in the medical ecosystem is all about. It, however, seems that there is "lack of appreciation among health care executives (about) the business risks of cyber breaches" (He, 2021).

Subsection 13.10.2 will provide a few steps which should be part of every medical institution's cybersecurity strategy plan.

13.10.2 A few guidelines to the board for cybersecurity governance (CSG) in the medical ecosystem

In this section, we will provide a number of guidelines for the board of a health care enterprise to ensure that the very important and strategic matter of cybersecurity governance in the medical ecosystem is properly implemented. The board must take these guidelines seriously to ensure strong oversight of the whole cybersecurity area.

The board must:

1. ensure that they understand and accept that cybersecurity governance is a corporate governance accountability, and they have an important oversight role regarding cybersecurity;
2. accept that the cybersecurity buck stops with them;
3. ensure that cybersecurity is a standing item on the board agenda;

https://doi.org/10.52779/9781991201959/13

4. ensure that regular feedback is provided to the board about the status of cybersecurity in the enterprise to be able to perform their oversight role;
5. ensure that there is at least one cybersecurity expert on the board (even an outside expert);
6. ensure that a culture of cybersecurity awareness is established and enforced;
7. create a cybersecurity risk policy, approved and signed by the board. This must include the cyber-incident response plan (CIRP), discussed in section 13.9 above, and must have representation from the legal department;
8. ensure that international good practices in cybersecurity, like encrypting data, are implemented in the enterprise;
9. create a cyber-risk governance committee as a subcommittee of the board, reporting directly to the board;
10. understand that operating the medical ecosystem has potentially very serious business risks;
11. understand that the accountability for cybersecurity governance cannot be delegated to executive management or the chief security officer – some responsibility can be delegated, but the board stays accountable; and
12. understand the ethical risks in operating in the medical ecosystem.

Price (2018b) provides more background on this matter.

13.11 CONCLUSION

The medical ecosystem will see massive growth in the coming years, primarily driven by the IoMT. This will again create a greater dependence on cyberspace, which will again provide a larger attack service for cybercriminals. To counter these cyberattacks, cybersecurity must be at the core of the medical ecosystem. This reality must be accepted by the board of an enterprise, exercising their corporate governance oversight role to ensure that the enterprise is prepared against cyberattacks as far as possible.

https://doi.org/10.52779/9781991201959/13

Bibliography

Alpine Security. 2021. *Comprehensive guide to Yom cybersecurity: risks, safeguards, and what we protect.* https://bit.ly/3GHu27G [Accessed 25 February 2022].

Archon. n.d. *Medical IoT device security risks and solutions.* https://bit.ly/3GJv7fm [Accessed 25 February 2022].

Armerding, T. 2015. *Surgical robots: smart but insecure*. https://bit.ly/3V6QSKq [Accessed 25 February 2022].

Aver, H. 2021. *Ransomware attacks on healthcare.* https://bit.ly/3VnCgWx [Accessed 25 February 2022].

Coventry, L. & Branley, D. 2018. *Cybersecurity in healthcare: a narrative review of trends, threats and ways forward.* https://doi.org/10.1016/j.maturitas.2018.04.008

Critical Insight. n.d. *Top 6 hackable medical IoT devices.* https://bit.ly/3Xnzank [Accessed 25 February 2022].

Deloitte. 2020. *Cyber transformation.* https://bit.ly/3tZ4JGy [Accessed 25 February 2022].

Dilawar, N., Rizwan, M., Ahmad, F. & Akram, S. 2019. Blockchain: securing internet of medical things (Yom). *International Journal of Advanced Computer Science and Applications*, 10(1). January. https://doi.org/10.14569/IJACSA.2019.0100110

ECRI. 2020. *Getting started with a cybersecurity incident response plan for your medical devices.* https://bit.ly/3ugzION [Accessed 25 February 2022].

Fortium. 2017. *Cyber security: the buck stops in the boardroom.* https://bit.ly/3tYxGlX [Accessed 25 February 2022].

Frenz, C. 2021. *Importance of medical ethics in cybersecurity.* https://bit.ly/3F0gFOQ [Accessed 25 February 2022].

Goodin, D. 2020. *A patient dies after a ransomware attack hits a hospital.* https://bit.ly/3ECCK4A [Accessed 25 February 2022].

Green, J. 2018. *Centralised medical records database: convenient or risky?* https://bit.ly/3V6Mvif [Accessed 25 February 2022].

He, Y. 2021. *Health care cybersecurity challenges and solutions under the climate of Covid-19: scoping review, 2021*. https://doi.org/10.2196/29877

Intuitive. n.d. *Prostate surgery.* https://bit.ly/3F1BwkS [Accessed 25 February 2022].

Irwin, L. 2020. *What is the ISO 27000 series of standards?* https://bit.ly/2JHfB4f [Accessed 25 February 2022].

Kacmarek, R. 2011. *The mechanical ventilator: past, present, and future.* https://doi.org/10.4187/respcare.01420

Kawamoto, D. 2017. *Hacked IV pumps and digital smart pens can lead to data breaches.* https://bit.ly/3VqCMDu [Accessed 25 February 2022].

Khalik, S. 2018. *Greater protection of patient data when national electronic medical records become mandatory.* https://bit.ly/3UalcSR [Accessed 25 February 2022].

Madder, R. 2020. *Robot surgery could be the future of health care in remote areas.* https://bit.ly/3OwuDeo [Accessed 25 February 2022].

Miliard, M. 2021. *Hospital ransomware attack led to infant's death, lawsuit alleges.* https://bit.ly/3VtRk5j [Accessed 25 February 2022].

Mittelstadt, B. 2017. *Ethics of the health-related internet of things: a narrative review.* https://doi.org/10.1007/s10676-017-9426-4

Morgan, S. 2017. *Cybercrime damages $6 trillion by 2021.* https://bit.ly/2K6QZnp [Accessed 25 February 2022].

Price, N. 2018a. *The relationship between cybersecurity and corporate governance.* https://bit.ly/3tVb0Dl [Accessed 25 February 2022].

Price, N. 2018b. *How to transform corporate governance for your hospital board.* https://bit.ly/3AIf6lP [Accessed 26 February 2022].

Ronte, H., Taylor, K. & Haughey, J. 2018. *Medtech and the internet of medical things.* https://bit.ly/2OafRdy [Accessed 25 February 2022].

https://doi.org/10.52779/9781991201959/13

Rothschild, F. 2020. *Medical devices are double-edged swords for hospitals: vital for patient care but vulnerable to cyberattacks.* https://bit.ly/3V5HfeW [Accessed 25 February 2022].

Scholtz, T. 2021. *Security & risk strategy.* https://bit.ly/3EYVMmT [Accessed 25 February 2022].

Sipilä, J. 2020. *Patients in Finland blackmailed after therapy records were stolen by hackers.* https://cnn.it/3U3b26M [Accessed 25 February 2022].

Skierka, I. 2018. *The governance of safety and security risks in connected healthcare.* The Institution of Engineering and Technology. https://doi.org/10.1049/cp.2018.0002

Spence, N., Bhardwaj, N., Paul, D. & Coustasse, A. 2018. *Ransomware in healthcare facilities: a harbinger of the future?* https://bit.ly/3Ukxb0B [Accessed 25 February 2022].

Steger, A. 2020. *What makes Yom devices so difficult to secure?* https://bit.ly/3V1eYGi [Accessed 26 February 2022].

Storm, D. 2015. *Researchers hijack tele operated surgical robot.* https://bit.ly/3OxavsC [Accessed 25 February 2022].

Vaas, L. 2013. *Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking.* https://bit.ly/3AHXiHy [Accessed 26 February 2022].

Weiner, S. 2021. *The growing threat of ransomware attacks on hospitals.* https://bit.ly/3U6fce6 [Accessed 25 February 2022].

WHO. 2014. *Health systems governance for universal health coverage.* https://bit.ly/3TYVukk [Accessed 25 February 2022].

https://doi.org/10.52779/9781991201959/13