Regulating Cybersecurity in the Health Care Sector

During the COVID-19 pandemic, awareness about vulnerabilities in the health care sector increased. Experts from governments, civil society, and industry called for more cybersecurity regulation that clarifies responsibilities and expectations. Regulation is one answer, but some issues require other policy solutions, such as further international cooperation.

By Nele Achten

In October 2021, 290,000 medical records were leaked in Israel, including information about patient's medical test results, procedures, treatments, and appointments. Similar cyber incidents around the world have involved the theft of personal data, and in some cases health related data, such as records of medicine dispenses. Since the beginning of the pandemic, cyber incidents have also disrupted hospitals and medical facilities. As a result, surgery appointments were cancelled and patients had to be directed to nearby facilities.

Medical personnel attend a patient at the emergency room in a clinic in Germany in May 2021.
Kai Pfaffenbach / Reuters

While it is difficult to determine whether cyber incidents in the health care sector have increased over the past years, public awareness about cyber threats in this field has grown since the beginning of the COVID-19 pandemic. The need to improve the protection of health data, facilities, and devices is particularly urgent for two reasons. First, a leak of health care data concerns the most sensitive area of patients' privacy. Second, the disruption of medical facilities and interference with medical devices can endanger lives.

Governments and public agencies around the world want to play a more active role in protecting victims of cyber incidents in the health care sector. States can use a combination of regulatory instruments and policy tools. EU cybersecurity regulations are arguably the most comprehensive and developed in the world. Within the EU, cybersecurity aspects are regulated in three different fields: data protection, security practices of essential service operators, and security of digital products. An assessment of these regulatory fields can help other states identify different policy areas and develop their own approaches to address cyber threats. Understanding how regulatory frameworks intersect with international norms, ethical considerations, and international policy debates provides a broader perspective in the search for adequate solutions relating to cybersecurity in the health care sector.

Data Breaches

Data protection is a well-established regulatory field that gained renewed importance in the framework of the EU General Data Protection Regulation (GDPR). The

GDPR defines obligations for any entity that either determines why and how personal data is processed (data controller) or that itself processes the data on the controller's behalf (data processor). Data concerning health is considered personal data and companies controlling or processing health data therefore have to comply with the GDPR. Data protection authorities control compliance with the GDPR and may issue fines.

Data breaches may occur for many reasons, including loss or theft of unencrypted devices. However, US healthcare data breach statistics show that unauthorized access and disclosures have become the main cause for breaches. Healthcare data has become a new target for criminal groups due to its particularly sensitive nature, which can be more lucrative than the extortion of other forms of personal data. Data breaches due to unauthorized access often follow the same pattern. A malicious actor first gains access to a system, network, or database. Frequently, victims are not aware that a malicious actor was able to gain such unauthorized access. The malicious actor then extracts data and encrypts the victim's database. Finally, they threaten to publish sensitive information unless they receive a ransom. In the case of the Israeli medical records leak, the company operating a database for nearly 30 medical clinics refused to pay a ransom and, as a result, the hacker group leaked the medical records.

Healthcare data has become a new target for criminal groups due to its particularly sensitive nature.

In order to avoid unauthorized access of personal data, Article 32 of the GDPR determines that any data controller or processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This risk-based approach leaves a certain degree of flexibility regarding the implementation of different security practices depending on the type of data that needs to be protected. However, two crucial questions emerge: who will define the appropriate technical and organizational measures, and on which best practice policies will they be based? If data protection officers and judges only look at security practices of globally operating companies, there is a risk that smaller companies may be unable to compete and that existing market powers will be reinforced. It is still too early to identify trends in this regard. Data protection authorities only started to issue fines for insufficient security measures in 2019 and specifically for data breaches in the health care sector in 2020.

Finally, it should be noted that the GDPR also had a significant impact on companies located outside the EU since it equally applies to non-EU data controllers and processors located who offer goods or services to EU residents or monitor their behavior. This extraterritorial application has created a significant compliance burden for companies dealing with EU residents. Some companies simply refuse to deal with EU residents and adopted measures such as geo-blocking websites to EU-based visitors. This has an impact on potential future regulation in the cybersecurity context and raises the urgency in coordinating approaches among jurisdictions rather than adopting domestic rules with broad scopes of application.

Essential Service Operators

The second regulatory field concerns security practices of essential service operators. Adopted in 2016, the directive on security of Network and Information Systems (NIS directive) is the main regulatory instrument, commonly framed as the first EU-wide cybersecurity regulation. The NIS directive aims to strengthen the level of cybersecurity in all EU member states, to facilitate cooperation among them, and to ensure a security culture among essential service operators.

Under the NIS directive, healthcare providers, including hospitals and private clinics, are operators of essential services. However, each member state individually identifies the entities considered essential for society and the economy when implementing the directive into domestic legislation. Each entity determined to be an essential service operator then has the obligation to adopt appropriate security measures and to notify public authorities about significant incidents. The main idea behind the NIS directive is that a disruption of these essential service operators would pose a national security threat. This justifies a closer cooperation of state agencies with essential service operators and increased information sharing.

The European Commission, however, has already identified deficiencies and proposed a revised NIS directive 2.0 in December 2020. A major critique has been that the determination of essential service operators varied widely among member states and that the directive thus did not bring the desired harmonization. The Commission's proposal adds new sectors to the list of essential services and introduces a clear size cap in selected sectors, thereby including all medium and large companies within the directive's scope. At the same time, the revised directive allows member states to identify smaller entities with high-risk profiles as essential service operators.

The main question, however, is whether it is still appropriate to adopt regulatory mechanisms that distinguish essential service operators from other businesses. Recent cyber incidents have shown that the functioning of smaller entities can be equally significant, even if they have not been designated as essential in the first place. A small hospital, for example, might not fall under the definition of essential service operator but a cyber incident disrupting its services can be just as critical for the individuals concerned.

Digital Products Security

Finally, a new regulatory and policy field relating to digital products has recently become more prominent. This field of regulation is generally concerned with cyber incidents that occur due to product vulnerabilities. Standards, certificates, and regulations aim to strengthen security practices during the design and life cycle of digital products, as opposed to policies and regulation of essential service providers that focus on the security practices of organizations. One advantage of this new field of regulation and policy is that increased product security helps to protect all types of businesses and society as a whole, not only specifically defined essential services.

Due to its life-threatening potential, the interest to develop medical devices that are as secure as possible is higher than for other products. While there has not yet been a reported life-threatening cyber incident related to a medical device, security researchers have warned about their vulnerabilities for more than a decade. In one case, a vulnerability was discovered in connected pacemakers that could have allowed hackers to administer cardiac shocks. As a result, the US Food and Drug Administration had to recall nearly 500,000 devices, some of which were already implanted.

Within the EU, the Medical Devices Regulation became fully applicable in May 2021. The regulation aims to ensure a high level of protection for patients and users of medical devices. It requires a pre-market conformity assessment by an accredited institution. After releasing a medical product on the market, public authorities continuously monitor conformity with safety and security requirements, for example, through unannounced inspections. This is known as post-market surveillance. While most of the provisions determine safety requirements – ensuring that a product is safe for its intended use, the regulation also contains security requirements that deal with external threats, risk management, and mitigation.

The effectiveness and consequences of the regulatory approach on digital products security remain to be seen. There has been some skepticism by public policymakers and technical experts as to whether regulation can lead to improved security practices in any way. The fear is that regulation leads to a compliance-based security culture and does not promote the best possible practices. Moreover, it will be interesting to see the impact of these regulations on international trade. On the one hand, a high European security standard could be an advantage as it may make EU-certified products more competitive abroad. On the other hand, some manufacturers outside the EU might significantly delay the sale of innovative products on the EU market due to the burden of getting their products certified. EU citizens would have access to particularly secure products but not always the most innovative solutions.

International Norms

The EU regulations outlined above focus on prevention and resilience. Cyber threats to the health care sector, however, do not stop at the EU's borders. International cooperation, information sharing, and diplomacy are necessary to reduce threats. While the outlined regulatory approaches in the EU addressed security practices related to personal data, organizations, and products, international rules and norms primarily define responsible state behavior. Frequently, these rules and norms determine negative obligations, meaning that they establish what kind of attacks are prohibited.

States have widely acknowledged a norm that prohibits them to attack critical infrastructure. This norm was first determined within the final report of the UN Group of Governmental Experts in 2015, which was consequently adopted by consensus by a UN General Assembly resolution. The UN resolution reflects the opinion of states and can help create customary international law over time. In addition, some states have also affirmed the prohibition to attack critical infrastructure in their individual statements on the application of international law to cyberspace. While there is no comprehensive international definition of critical infrastructure, there is a broad consensus that medical facilities constitute critical infrastructure. In March 2021, states confirmed in the report of the UN Open-ended Working Group that "healthcare infrastructure including medical services and facilities" are critical infrastructure and therefore should not be attacked.

Beyond the Law

While legal provisions play an increasingly important role for security practices, the protection against cyber threats is also shaped by ethical considerations and non-regulatory public policies. Ethical values recognized in international rules may arguably play an important role in the context of cyber threats for health care providers. Any potentially life-threatening cyber attack, for example, could be considered in contradiction to the right to life protected under the Universal Declaration of Human Rights.

States have widely acknowledged a norm that prohibits them to attack critical infrastructure.

During the early stages of the COVID-19 pandemic, some experts argued that hacker groups would not intentionally target hospitals because they may adhere to self-imposed ethical norms protecting the universally recognized right to life. There were indeed cases where the victim of a ransomware attack reached out to the hacker stating that they are an urgently needed health care provider and where the criminal group subsequently delivered a decryption code without demanding a ransom. The majority of hacker groups, however, do not seem to adhere to this self-imposed ethical norm, as proven by threats specifically claiming to target health facilities.

The value of human life is also frequently used in immediate reactions after cyber incidents that try to hold someone accountable for the incurred harm. Politicians, journalists, and scholars like to coin incidents with the label of "first cyber death". Using such a term creates fear when, in reality, facts are insufficient to determine a legal responsibility for causing the death of another person in a direct or indirect manner. It is mostly difficult to establish a chain of causation between the incident and the death. Moreover, the label of "cyber death" focuses on the attacker and does not sufficiently acknowledge the responsibility of the hospital or other medical facility for not having adequate fallback mechanisms in case of an incident.

Beyond these ethical considerations, there are also relevant public policy initiatives complementing cybersecurity regulations within the EU. For example, member states are involved in public-private information sharing groups and international policy initiatives. In October 2021, the US government for example launched the Counter Ransomware Initiative. The initiative, which was signed by over 30 countries, calls for closer cooperation with the private sector and builds on existing international instruments. The initiative is promising because it proposes concrete areas for action related to resilience, countering of illicit finance, disruption of ransomware activities and their subsequent investigation by law enforcement, as well as diplomatic efforts to promote international rules. This makes it one of the most substantive international policy documents so far. The initiative also signals further international cooperation between a number of different ministries, public agencies, and the private sector.

Outlook

Since aspects of cybersecurity are addressed through a variety of different EU legal regimes, lawyers and public policymakers often operate in silos. This is no different

Further Reading

Emily Skahill / Darrell M. West, "Why Hospitals and Healthcare Organizations Need to Take Cybersecurity More Seriously," *Brookings* 09.08.2021.

Neta Alexander, "My Pacemaker Is Tracking Me From Inside My Body," *The Atlantic*, 27.01.2018.

The CyberPeace Institute, *Playing with Lives: Cyberattacks on Healthcare are Attacks on People*, March 2021.

when it comes to cybersecurity aspects of one specific sector, such as health care. As the scope of security regulations within these legal regimes increases, so does the risk of having overlapping regulations and unnecessary legal burdens. Encouraging regular exchanges between experts from these different fields on legal developments and industry best practices would help to mitigate this risk.

Policymakers and lawyers will need to ensure that similar requirements are interpreted coherently across different legal instruments.

States that are in the process of developing their own policy approaches to cybersecurity threats might want to consider the risk of overlapping regulations and the need to coordinate. However, cybersecurity provisions will most likely always be part of many different legal instruments. Even in jurisdictions that are only now starting to determine mandatory security requirements, these might be included as part of different existing legal instruments. This is not a problem *per se*, but policymakers and lawyers will need to ensure that similar requirements are interpreted coherently across different legal instruments. It will require close coordination between administrative agencies, judicial authorities, and industry associations.

For more on Cybersecurity Politics, see CSS core theme page.

Nele Achten is Senior Researcher for Cybersecurity Policy in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editors: Névine Schepers, Benno Zogg
Language Editing: Henrik B. Larsen
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000515084