3 GOOD HEALTH AND WELL-BEING

On the Relationship between Health Sectors' Digitalization and Sustainable Health Goals: A Cyber Security Perspective

Stefan Sütterlin, Benjamin J. Knox, Kaie Maennel, Matthew Canham and Ricardo G. Lugo

1. Towards Sustainable Digitalized Healthcare

Digitalization in the health sector is, as in all societal domains, motivated by a range of anticipated positive consequences, such as increased effectiveness of prevention, treatment and follow-up, a generally improved resource efficiency and improved health care availability. This chapter will discuss how the ambition of achieving sustainable health goals may be affected by measures of digitalization. This will be done by covering digitalization from a cyber security perspective and how new potential threats to privacy may influence the public's trust in their health care system, thereby affecting the envisaged goals of sustainable health care performance. It will also discuss further how digitalization in the healthcare sector unleashes an enormous potential in terms of cost-effectiveness, decentralization and the availability of specialist services and expertise, which risks and countermeasures these changes entail, and how they are currently dealt with and the role of cyber resilience in ensuring rapid digitalization does not come at the cost of essential trust mechanisms that are quid pro quo in the health sector.

Transformation to a digitalized healthcare system must be governed and framed by a range of measures in various societal domains. The World Health Organization's (WHO) report on the status of eHealth in the European region (WHO 2016) states that its member states "acknowledge and understand the role of e-Health in contributing to the achievement of universal health coverage and have a clear recognition of the need for national policies strategies and governance to ensure the progress and long-term sustainability of investments. However, leveraging eHealth as a national strategic asset demands a more coordinated approach [. . .]" (WHO 2016, p. xi). The WHO acknowledges the fact that a majority of its member states developed or are developing "national strategies or policies for eHealth, universal health coverage or national health information systems, and ensuring sustainable funding for their implementation." (WHO 2016, p. xi). The report requests the member states to develop an "inclusive and intersectorial approach to the development of national eHealth strategies" (p. xii). These international efforts to adapt to the consequences of technological development provide an example for the wide ranging consequences that the digitalization of health systems entails for legal security measures relating to a state's power over its citizens, institutional development, policy and practice, education, and cyber security. We argue that cyber security, in turn, is not just one of many subjects to consider, but instead it pertains to and penetrates all other affected domains, such as the aforementioned organizational structures, policymaking, and education of non-technical healthcare professionals, as well as legal structures.

The healthcare system's efficiency and effectiveness depends on policies and procedures such as the rapid and precise exchange of health-related information between its different acteurs. In recent years, more national healthcare systems approached sustainable health benefits for their populations by digitizing their services and administrative procedures, enabling new innovative models of health care delivery and efficient data sharing amongst stakeholders. Digitalization on a system level led to increasingly centralized databases offering synergies for new research possibilities, and the opportunity to improve individualised, time- and cost-efficient healthcare covering hitherto underserviced areas, such as disadvantaged parts of society or structurally weak geographical spheres. The manifold effects of digitalized healthcare result from a large variety of technological innovations on individual, institutional or system level.

The concept of e-Health combines aspects of areas such as healthcare business and administration, public health, and medical informatics. This broad term covers aspects of healthcare delivery, data administration and relies, to a large extent, on the availability of web-based patient care via communication platforms. e-Health is both a technical tool of practical healthcare delivery as well as a governance instrument. The term is also used as a more general description of a larger variety of digitalized healthcare. On the contrary, the term m-health ("mobile health") is a particular aspect of e-health describing medical and public health practice via mobile (wireless) electronic devices such as smartphones or specific monitoring devices such as EKG monitors or glucometers. Telehealth is a rather broad term referring to remote clinical services, as well as non-clinical activities such as training and medical education. The narrower term telemedicine is the aspect of telehealth dealing with remote clinical services. These various manifestations of digitalized healthcare contribute to the gradual achievement of sustainability goals in a number of ways. Within the last ten to fifteen years, electronic health records have become a universal feature of digitalized healthcare. This increased availability of digitalized information and the overall improved information management by healthcare professionals accelerated decision-making time, provided an information basis for better outcomes of clinical decisions, facilitated interdisciplinary cooperation, reduced the fragmentation of information between healthcare providers, and reduced duplicate tests and other treatment risks or side effects (Atasoy et al. 2019).

In developing countries, digitalization and thus this universally available information has increasingly been used not only to process patient-related information, but also to make medical services and the competence of rare and remote health care providers accessible to rural and secluded regions with lacking or insufficient medical infrastructure (Zhang and Zaman 2019) by means of eHealth. While eHealth has been mostly seen in terms of reducing inequality to access of healthcare, a discussion on unequal access to these benefits emerges. As mHealth contributes to an increased autonomy and strengthening of the patient role as administrator and gatekeeper over own health-related data, this increases the demands towards patients considerably. The access to "patient-facing" mHealth and a consequently more responsible and autonomous patient role are raising concerns related to digital inequality and cognitive skills. Unequal access to the benefits of digitalization for deprived societal groups could be particularly pronounced in countries with rather limited universal healthcare, such as the USA or developing countries.

2. Digitalization and Increased Vulnerability

Highly digitized healthcare systems relying on electronic health records are a vital part of a nation's critical infrastructure. Critical infrastructure describes the "physical and cyber systems and assets that are so vital [. . .] that their capacity or destruction would have a debilitating impact on [. . .] physical or economic security or public health or safety" (Department of Homeland Security 2019).

The model of an increasingly patient-centered healthcare emphasizing the individual's needs, rights, autonomy, preferences and values guiding all medical decisions is increasingly promoted and spread as a development unfolding parallel to digital change. Healthcare systems involve patients to an increased extent in ambulatory data collection, provide more insight into patient documentation, secure the patient's rights to own the data and become more inclusive when choosing amongst treatment options. As an effect of the increased cooperation between patient and numerous other acteurs in the healthcare system, the increased amount of patient-centered sensitive data is bundled, stored and processed in centralized or highly interconnected digital infrastructures.

The amount and availability of patient-related data are tempting high-value assets for criminal undertakings. The extent to which the healthcare sector has become a primary target of cyber crime is reflected in the number of cyber attacks on hospitals in recent years. More than 2000 breaches involving a total of 176 million patient records were reported between 2010 and 2017, with individual breaches ranging from 500 to nearly 79 million patient records. The total number of breaches increased from 199 in 2010 to 344 in 2017 (e.g., McCoy and Perlis 2018). One of the first occasions when the international general public became aware of cyber attacks on the health care sector was the 2017 WannaCry ransomware attack infecting an estimated 230,000 windows systems in 150 countries (Chen and Bridges 2017). The unprecedented scale of this cyber attack brought the relatively neglected field of cyber security in the healthcare sector onto the agenda of media, healthcare providers and policy makers.

The many years of negligence towards cyber security made many healthcare providers particularly easy targets, especially when compared to highly protected societal domains such as the military, law enforcement, and innovation-driven economy safeguarding their intellectual property or high-value tactical or strategic decisions. The Norwegian data breach of 2018 is a particular—but not exclusive—example of a targeted attack with the criminal intent to obtain sensitive patient data exploiting the lack of awareness and preparedness. The targeted attack resulted in the extraction of 2.9 million datasets, including patient records, resembling more than half of Norway's population (Hughes 2018; Johansson 2018). The attack is believed to have been carried out by highly sophisticated attackers explicitly targeting patient records stored by the health authorities in the South-East region of Norway. Following further investigations, it was assumed that the attackers were focused on the health service's relationship with Norway's armed forces and potential information regarding a major NATO exercise organized in Norway later in the year. The cyber attack seems to have benefitted from lax security standards and outdated operating systems no longer supported by security updates. According to the investigations of a national newspaper, as late as in 2017, about 1200 of the Health-South-East's computers were still running on Windows XP, about three years after Microsoft ceased supporting the popular operating system (Irwin 2018; VG 2017).

While these events demonstrate clearly the need for heightened cyber security awareness and preparedness, the viciousness of criminal hackers—be they rogue criminals with economic interests, financed by nation-states, competitors or others—data breaches do not necessarily presuppose criminal intent. Human failure is known to be the major vulnerability of all technical systems with which humans interact (“socio-technical systems”). Human failure provides numerous “attack vectors”, i.e., opportunities to exploit a person’s individual vulnerability in order to access a targeted network. However, while processes, people and technology need to be designed, trained, and maintained in a way that reduces the risk of human failure enabling third parties with malicious intent to get access to sensitive data, the loss of sensitive patient data does not necessarily require malicious intent. Amongst some of the most prominent—known—health data breaches made public in recent years include the breach of data on 150,000 patients by the UK’s National Health Service being shared without their permission in 2018. In fact, the patients whose data were made public actively opted out of any use of their data beyond own treatment. The breach was later explained as a “coding error”, i.e., an internal human failure without any criminal intent (Canham et al. 2020). The National Health Service (NHS) data breach of 2018 indicates how cyber security breaches and efforts to improve information security management routines are of crucial relevance for the patients’ trust in the healthcare system, even in the absence of any criminal attempt, as it undermines the public trust in the institutions’ very ability to maintain secure information processing as a part of their daily routines, and in the absence of acute threats. The case of the NHS data breach demonstrated impressively how a digitalized data administration potentiates the detrimental impact of singular human failure.

The motivation for targeting the health sector is comparable to other large societal sectors such as public authorities, governmental or non-governmental organizations or industry. With cybercrime dominating, hacktivism and cyber espionage are the major motivations behind cyber attacks in the healthcare sector (Passeri 2017). The often-reported observation that human factors seem to play a particular role in cyber breaches targeting the healthcare sector, has been associated with the particular lack of security awareness, training, and security-related attitudes (Kim 2017). As a result, health and hospital trusts are frequently considered “low hanging fruits” by cyber criminals aiming for financial profits on the black market for patient data. In addition, and in the comparably smaller but potentially more devastating case of nation-actors, the healthcare sector provides a relatively easy entrance for the acquisition of sensitive information required to paralyze a potential enemy’s critical healthcare infrastructure in a conflict situation.

Cyber security rests upon three pillars; confidentiality, availability, and integrity (Conrad et al. 2012; Canham et al. 2018). Cyber-attacks focused on the confidentiality pillar expose private information (such as credit card or health information) to unauthorized persons. The American Medical Collection Agency (AMCA) data breach in which 12 million patient records were exposed is an example of an attack using the confidentiality pillar. The integrity pillar represents the prevention of unauthorized modification of a system or data. Attacks against the integrity pillar modify data in such a way that it becomes untrustworthy, and the attack may not be discovered even after the damage has been done. In a healthcare context, cyber threat actors who attack the integrity pillar might change a patient's dosage instructions and create a potentially unsafe situation for that patient. The Stuxnet worm is often cited as an example of an attack on information integrity that caused a large number of Iranian uranium centrifuges to malfunction. This attack employed malware specifically designed to provide false performance readings to operators that left them unaware of an impending problem (Chien et al. 2012). Security researchers have conducted proof-of-concept attacks against the Integrity Pillar of neuro-prosthetic devices and were able to inject commands that disrupted the device's normal functionality (Canham and Sawyer 2019; Cusack et al. 2017). The availability pillar focuses on information assurance; in other words, ensuring that users are able to access the data that they are authorized to access. Examples of attacks against the availability pillar include the multitude of ransomware attacks against hospitals and healthcare facilities over the past few years.

The examples of major data breaches provided above are only a very small part of the overall picture and do by no means cover a substantial part of known cyber threats. Commercial cyber security providers publish regular lists of conducted cyber attacks that have become known. At the time point of detection, cyber attacks have usually already happened, and a considerable number of attacks and conducted data extractions may remain undetected or unreported. The majority of attacks directly target individual hospitals as key centers of gravity, with direct access to patients' sensitive data, while being known to be lagging far behind other institutions of comparable size in terms of their cyber security standards. Where a few hospitals with low resources for cyber security threaten the entire infrastructure due to their interconnectedness, the efforts to become a less attractive goal for cyber criminals needs to step up considerably. These efforts need to go beyond current regulations which largely focus on questions related to data privacy, but not data security (Jalali and Kaiser 2018). A surge in related analyses and systematic research on risk factors and potential countermeasures in recent years indicates an increasing awareness amongst the stakeholders, which may lead to increased future investment in technology, processes and personnel (Coventry and Branley 2018; Kruse et al. 2017; Martin et al. 2017).

3. Improving Sustainable Healthcare and Ensuring Cybersecurity: The Estonian Case

As digitalization as a means to improve national healthcare systems' effectiveness and efficiency comes with increased data exchange accompanied by an increased potential of vulnerabilities towards security threats, governments work towards finding a balance between technically feasible solutions maximizing the outcome benefits, whilst minimizing the threat potential with cyber security measures. Cyber resilient healthcare systems contribute to and maintain public acceptance for further transformation and sustainable development initiatives, and bolster public perception of information security. When discussing these future trends, the digitalization of the Estonian healthcare system may serve as a blueprint for future developments in other countries, too. The Baltic country with approximately 1.2 million inhabitants is considered a world leader in both e-government as well as cyber security. Estonia is regarded to be one of the most digitized countries of the world and has firsthand experience of being subject to hostile cyber attacks by a foreign state power. In 2007, a Russian cyber attack brought the Estonian public authorities, organizations, media and with it, the usual public life, to an abrupt hold. The attacks were interpreted as an expression of Russia's disagreement with the relocation of a Sovjet-era bronze soldier statue in the capital city Tallinn. In the aftermath of these attacks and reinforced by a continuously perceived threat by Russian interference, the country publicly and privately invested heavily in cyber security infrastructure, processes and competences. Both the level of digitalization of the country's healthcare services and the technological advancements in cyber security make Estonia an interesting case study and "laboratory" providing possible insights into future developments on an international scale. Trends and consequences in Estonia are likely to be—in similar or partial form—also introduced in other countries.

Estonia's healthcare system's patients and doctors, hospitals and the government, have to rely on e-services for health. Each person in Estonia that has visited a doctor at least once has an online e-Health record. The core of the Estonian e-Health System is the digital health record that functions as a centralized, national database and retrieves data as necessary from various providers, who may be using different systems, and presents it in a standard format via the e-Patient portal (e-estonia.com). These e-Health records are, among other purposes, used for prescriptions and in emergency situations. E-ambulances are available in emergency situations to detect and locate an emergency call within 30 seconds. On board the e-ambulance, a doctor can use a patient's ID code to read time-critical information, such as blood type, allergies, or recent treatments. To balance these obvious advantages in availability, efficiency and cost-effectiveness on the societal level, data privacy for the individual is secured by various means. Sensitive patient information is only accessible by authorised individuals identified via national electronic ID cards. Highly secure state-of-the art data transmission encryption techniques (Keyless Signature Infrastructure (KSI) Blockchain technology) are used for the system to ensure data integrity and mitigate internal threats to the data. Data transport and security layers are provided for by the government's data transmission software ("X-Road"), ensuring that only digitally signed and encrypted data are exchanged (Priisalu and Ottis 2017). The electronic databases are organised in a decentralized manner ensuring that cyber attacks or leaks cannot compromise the overall system. There are no so-called super-administrators with unrestricted access to patients' health records (Health and Welfare Information Systems Centre (TEHIK) (2019)). By default, medical specialists can access data using their unique individual identifier, but any patient can choose to deny access to any case-related data, to any, or all care providers; including one's own general practitioner (Priisalu and Ottis 2017). Every patient thus keeps full autonomic control over the stored data, provides permission and keeps the full overview over which individual person has accessed their personal information. Each data view leaves an identifiable trace and record.

The privacy and processing of personal data processed in the Estonian healthcare system and other public databases is regulated by the country's Personal Data Protection Act and the European Union's General Data Protection Regulation (GDPR). The governing principle is to provide an open and transparent attitude as a prerequisite for a robust trusted relationship between the citizens and the state. By investing in a person's confidence in the government's ability to keep their data secure and guarantee confidentiality, integrity and availability. While there are no direct survey data describing the public and individual trust into the Estonian eHealth services available, the high rate of access and usage since the system's introduction in December 2008, the constantly high ratings of perceived quality of healthcare in public surveys indicate a level of acceptance (Lai et al. 2013). The Estonian example combines state-of-the art e-government services with newest cyber security technology, maximizing the potential of "security by design", i.e., providing technology with least possible vulnerabilities and robustness towards human failure. To ensure public acceptance and trust, the patient is given full autonomy and transparency over the use of his/her personal information.

There are currently no known comprehensive data breaches following attacks on the Estonian healthcare system. While security-by-design solutions are a powerful and necessary means to provide cyber resilience, the human factor remains a considerable risk factor, particularly in less advanced partially digitalized systems and healthcare systems with lower degrees of centralization, as typical in larger countries. Human behaviour thus remains a constant threat of cyber security that is subject to intensifying research efforts by behavioural and interdisciplinary scientists.

4. The Human Factor in the Healthcare System's Cyber Security

Research on the human factor in cyber security acknowledges that technology does not exist in isolation, but that interpretations, conclusions and decisions are made by individuals or groups of humans with the "inbuilt guarantee" to commit a whole range of human failures if given the opportunity. Thus, even the best designed system for processing and storing sensitive data in a healthcare system faces human users and thus human failures, which potentially compromise data security at least on an individual, if not even systemic level, in unforeseen ways. These human failures—such as the coding error enabling the 2018 NHS data breach—occur on individual levels following erroneous conclusions and decision-making processes, insufficient or biased information as a decision-making foundation following inappropriate or inaccurate communication between individuals, teams, institutions or authorities. Given the relatively recent awakening concerning awareness of cyber vulnerabilities in the healthcare sectors, we argue that the human factor based on training, education and compliance, is of particular importance. In areas such as aviation, acute medical care, and many safety- and security-critical sectors, the devastating effects of human failure, for example by miscommunications, are well documented and acknowledged. In the area of cyber security, knowledge about the sources and underlying reasons of human failure and performance is still relatively scarce and "work in progress", but the amount of systematic research in this field is growing (Sütterlin et al. 2019).

Amongst the various ways in which human failure occurs and threatens cyber security, procedural compliance is one. A lack of procedural compliance when technology users do not adhere to existing security protocols can result from such protocols being too complicated, formulated in a, not understandable way, and highly technical. Other factors include the failure of organizational cultures, where enforced hierarchies and authoritarian leadership styles foster a culture of low tolerance to criticism and constructive feedback upwards along the vertical axis, making available competencies of lower ranking and technologically savvy younger experts unavailable for strategic decisions (Jøsok et al. 2016). Communicative challenges between individuals, teams, organisations and sectors particularly in interdisciplinary groups set up in an ad hoc manner and without established collaborative routines provide an environment that is particularly prone to misunderstandings, misinterpretations, and the loss of relevant information, resulting in discrepant mental models of a cyber threat situation. The reason why cyber security is particularly vulnerable to communicative challenges is the highly technical nature of the threat. A profound understanding and interpretation of a technical situation, its real-life consequences, options to act and their various anticipated consequences and associated risks in a cyber threat or cyber incident situation, with high stakes, that is potentially also characterized by time pressure and based on ambiguous information, creates an enormous cognitive individual and organizational workload prone to human errors. The creation of a shared situational awareness between technicians, decision-makers, and all other stakeholders requires a high degree of technical specialization in combination with efficient communication routines across disciplines, departments, organisations and societal sectors. The availability of understandable, yet accurate, technical information providing this shared situational awareness and decision-making ability gives technologically less informed decision-makers the ability to react and act with appropriate tactical and strategic decisions. The challenge is to provide an accurate yet simplified description of a given threat situation. The consequential options to act as well as the probabilities of anticipated consequences pose particular challenges in a context where not the shortage of information, but the overwhelming availability of it, adds to an enormous cognitive load for all stakeholders. In the communication of cyber threats, it is therefore not the situational status per se, but the outcome of its perception, interpretation, and communication by the cyber security technician that shapes the decision-makers' experienced reality. The decision-maker on the receiving end depends upon their understanding and thus upon the technician's simplification, selection, weighting, and interpretation. Knox et al. (2018) described the conditions that need to be put in place to facilitate information exchange on recognized cyber pictures between individuals and propose an orient-locate-bridge-model (OLB) describing how institutions can apply educational methods to enable both their cyber security personnel as well as their leaders in the effective communication of cyber security related situations (Knox et al. 2018).

Lacking procedural compliance and ineffective communication only represent examples of a number of ways in which human failures affect cyber security in and beyond the healthcare system. While there is a lack of research on human factor-related cyber security risks in the healthcare sector, the more extensive human-factor related knowledge from other domains can be transferred and applied in the healthcare sector as well. Human factor research can contribute to risk identification and the development of training approaches to facilitate cyber resilience. With 94% of malware distributed via email in 2018 (Verizon Communications Inc. 2019), phishing mails are the tool of choice to breach targeted networks. Empirical research has identified four categories of risk factors for susceptibility to phishing mails. These are situational factors, social engineering techniques, cultural factors, and individual differences (Canham et al. 2019). Employees who might not, under "normal" circumstances, be susceptible to a phishing attacks may be susceptible when distracted, or under significant cognitive load; in this way, situational factors play a major role in susceptibility. The social engineering techniques employed by threat actors can be very sophisticated and even appear to originate from known contacts. Some research suggests that cultural influences along the individualism–collectivism spectrum may significantly contribute to susceptibility (Butavicius et al. 2016). Finally, individual differences relating to personality and propensity to trust appear to account for some users being more susceptible than others. The most vulnerable users, sometimes referred to as "repeat clickers", represent a small minority of users who repeatedly fall prey to simulated phishing campaigns meant as training exercises. While these users usually only account for one to two percent of users within an organization, they can represent nearly 50% of the total simulated phishing failures (Canham et al. 2019).

Health care workers seem to fulfill some of these criteria, as they have shown a high propensity to click on phishing scams and have limited awareness of threats (Priestman et al. 2019). In a sector where women make up over 70% of workers in the health sector (WHO 2019) and usually rank higher on traits such as neuroticism, agreeableness (Parrish et al. 2009; Weisberg et al. 2011) and reward-based decision-making, known risk factors for maladaptive cyber behaviours cumulate. Getting targeted training to health care workers is essential in establishing and maintaining cyber resilience on an organisational level (Ghernaouti-Helie 2013). Other influencing factors determining susceptibility to fraudulent emails serving as an attack strategy to achieve entrance into sensitive IT systems are personality factors. IT users who are agreeable, emotionally less stable, and technically less knowledgeable, show higher risks of all unintended security violations in phishing attacks (Gratian et al. 2018; Halevi et al. 2013).

These vulnerabilities are usually addressed in cyber security education and training programmes. While these trainings are by far not sufficiently available and widespread in the healthcare sector, they are not even suitable to address all sources of errors. Even though general security training has shown to increase pro-security behaviors to some extent (Darwish et al. 2012), more targeted education is required to reach a significant improvement and lasting effects on behaviour.

In 2018, the United Kingdom's Information Commissioner (ICO) commissioned Kroll to conduct a study of all data breaches experienced by the UK government in 2017, 2124 incidents in total (Targett 2018). This study found that 88% of all data breaches involving UK government entities resulted from unintentional human error, without the direct involvement of a cyber threat actor. Examples of these errors included emailing unencrypted confidential patient information to the wrong recipient (21%), loss or theft of paperwork (20%) and data left in an insecure location (7%). Of the reported malicious cyber breaches, unauthorised access was the most common, accounting for 4% of the total, followed by malware (2.5%), phishing attacks (2.4%) and ransomware (1.5%). The healthcare sector accounted for the majority (57%) of these breaches, followed by general business (17%), education and childcare (16.7%), and local government (15.4%).

Knowledge workers in the information economy are often overworked, facing staffing shortages and constant deadlines. These workers commonly experience a tension between complying with security policy friction and accomplishing assigned tasks within deadlines (Posey and Canham 2018). Workers in the health care sector are no exception to this situation. One of the leading causes of (or contributing factors to) human error, is time pressure. Time pressure manifests in errors in two primary ways, deliberate policy violations and unintentional human errors (Reason 1990; Norman 2013).

The two categories of deliberate policy violations are routine violations and situational violations. Routine violations occur when policy non-compliance is so common that it is mostly ignored. A frequent example of this is the emergence of "shadow IT" systems. Shadow IT systems represent workarounds that users adopt in order to complete their work in an easier (but often less secure) manner. Examples include using unauthorized external cloud services or installing unauthorized wireless networks in secured spaces. Situational violations occur during exceptional circumstances. For example, in order to save a patient's life, emergency department medical staff might leave a proximity card on a monitoring cart in order to prevent the lock screen from activating. These violations are not routine, and usually occur when the cost of following proper security procedures is higher than abiding by them. Both routine and situational deliberate policy violations should give security staff pause, to reflect on the appropriateness of the policies causing these circumstances. If a policy is so cumbersome as to lead to it being deliberately ignored, this may be a good area to explore policy alternatives as a way to encourage secure behaviors. If existing IT infrastructure is so cumbersome to use that users are leveraging external resources, perhaps the existing infrastructure can be made more user friendly. Devices that utilize timeout lock screens might be modified to include an "emergency mode" so that they will not lock for the duration of the emergency.

Human errors, in contrast to deliberate violations, are unintentional and usually result from two distinctly different sources. The first type of human error is known as slips. Slips occur when an individual intends for one action to occur, but instead executes a different action. In this case, the person understands the correct action to take, but inadvertently takes the wrong action. An example of a slip might be pouring milk into coffee, but then placing the coffee cup in the refrigerator instead of replacing the milk (Norman 2013). In a cyber context, email address auto-complete is likely responsible for a great number of slip errors. Recall that the Kroll study found that emailing unencrypted confidential patient information to the wrong recipient was responsible for 21% of the 2017 data breaches (the largest number). In contrast to slips, mistakes are another type of human error that occur when an individual has the wrong goal (Norman 2013). Humans form mental models for how tools, artifacts, and environment operate and interact (Johnson-Laird 1983). These mental models encapsulate a simplified mental representation that allows the human mind to make predictions for actions taken with the things we interact with. Unfortunately, these mental representations are not always correct. When they are incorrect, this often leads to the wrong goal being formed, and an error then usually occurs. If a user believes that their employer has stronger security than what they have at home, they might forward a questionable email that they receive at their personal email account, to their work account, with the belief that the organization's security resources are better equipped to manage malicious software than their home system is. If this were the case, then this person would be taking the correct action, but of course this is false and based on an incorrect mental model.

This distinction between error types comes with consequence. In the cyber security industry, much emphasis is placed on user awareness training, with the implication being that if users were simply more aware of the inherent risks associated with their actions, they would be less vulnerable to attacks or committing errors leading to breaches (Carpenter 2019). While this may be true in some cases such as mistake type errors, it is untrue with regard to slip type errors. Slip errors result from highly learned behaviors that have become automatic and usually occur without conscious processing. In fact, slip errors tend to be more common in expert users, because they are so familiar with these actions. No amount of awareness training will fix slip errors; the best method to deal with these will likely be better design of interfaces and processes. Mistake errors result from incorrect goals, usually derived from incorrect mental models. Mental models can be updated through training and, therefore, these types of errors might be corrected through awareness training. Because these policy deviations can have radically different causes, they need to be addressed through different means (Canham et al. 2020). Security personnel in the health sector would be served well to track these errors in relation to data breaches and security violations and use these as a guide for developing corrective actions.

5. Cyber Resilience and Trust

In the previous sections, we laid out how digitalization transformed the way healthcare systems perform and the benefits these changes entail, as well as the vulnerabilities that come with large-scale health data administration. We also provided examples of how human behaviour can pose a large risk for breaches of sensitive data. Cyber resilience is more than the prevention of valuable data being stolen or the direct and collateral damages associated with a cyber attack. While data can in many cases be restored by backups, malware isolated and eliminated, and access to blocked data can be regained (ransomware)—there is a wider picture to it. Stolen data or access credentials and system vulnerabilities can spread in uncontrolled manners and be sold on illegal markets. The whereabouts of breached data remain usually unknown for long time periods, occasionally for years. The perpetrators can, in most cases, not be clearly identified, which adds an additional component of insecurity for the victims of cyber attacks, widely known as the "attribution problem". Cyber threats in the healthcare sector can have acute detrimental effects in times of national crisis (functionality of the healthcare system), hybrid warfare, or international conflicts above or below the threshold of war. In peacetime and in western democracies, however, breaches of data that were administered by private or public bodies (healthcare providers, insurances, etc.) can also undermine the public trust in these institutions. Public awareness and scepticism therefore influence policies around the digitalization of healthcare and consequently affects the development of institutions at the frontline of healthcare and achievement of sustainable development goals. The crucial role of people's trust in the protection of their privacy and thus in the integrity of the healthcare system as a whole has been recognized by state actors and lead to the development of relevant legal frameworks facilitating privacy, security and thus overall cyber resilience as a prerequisite of trust in a sustainable healthcare. According to the World Health Organization, trust in privacy legislation is key for the population's "confidence in their national eHealth programme" (WHO 2016, p. 77).

To reach a sufficient level of cyber resilience allowing for the further development, implementation and maintenance of digital solutions in healthcare, the vast majority of industrialized countries have established national legislation regulating the sharing, storing and use of personal data and/or personal health-related information as well as information exchange. While these legal frameworks have been put in place, the lack of cyber resilience on institutional levels makes healthcare institutions still an easy prey for malicious attacks or human failures due to mistakes and behavioural slips. One such cognitive barrier to prioritising cyber-resilience is the cost of investing in managing something that steals time from the primary and measurable role of the institution (Elgsaas and Heireng 2014). Investing time and resources into cyber secure systems and the people capable of ensuring persistent network resilience comes at considerable costs and is only rarely seen as a necessary and important investment in value generation (Coventry and Branley 2018). This is especially so when future funding for health institutions is very often performance related. Unfortunately, performance of cyber and information security is not the key criteria, meaning that in many countries, speed and efficiency of digital systems is prioritised ahead of security and resilience. For this reason, the introduction and implementation of digital systems in healthcare with the security by design principle at the forefront of development, and meet certain recognized classification frames, should be a step in adding cyber resilience from the start.

In Europe, national legal frameworks are directly affected by supernational legislation. The European Union Cyber Security Act of 2019 aims to increase EU resilience and response to cyber-attacks. The act established an EU framework for cybersecurity certification aimed at boosting the cybersecurity of digital products and services in Europe, including the various national healthcare sectors. In practice, the certification framework means improved cybersecurity across a wide spectrum of existing digital products and services, including the Internet of Things, as well as critical infrastructure such as, for example, hospitals. Even though these measures are not specifically aimed at cyber resilience in the healthcare sector, it contributes to the harmonization of cybersecurity standards, increasing the effectiveness in responding to cyberattacks as the system or device has a familiarity to it based on it meeting prescribed criteria. Manufacturers of healthcare technology are incentivised to invest in cyber security for their products, consequently giving them a potential competitive edge as customers see that certification is dependent upon a security-by-design approach to product development. When considering how the aforementioned potential of telemedicine and eHealth will rely heavily on the Internet of Things and the newest 5G data transmission standards, these new supernational legal frameworks can add a significant level of resilience; as it takes a stride in ensuring good cyber security as the foundation for trust in digital systems that should be able to guarantee information security.

Until legal frameworks such as the aforementioned legislation on harmonized certification have been implemented, security concerns remain a relevant factor influencing the users' trust in the healthcare system's ability to protect their sensitive data. The rise and investment in telemedicine to take advantage of the internet in support of ambulatory, more self-responsible monitoring and treatment in a "hospital-at-home" is heavily reliant upon security-by-design solutions minimizing or excluding the possibility of data breaches caused by unaware end-users. Such user-driven, self-monitoring of health care is ideal from a cost saving efficiency perspective as it is designed for people in certain risk-groups, people that might otherwise be re-hospitalized, and to assist people who are more likely to recover faster in their own home, whilst providing autonomy and enhanced quality of life. However, patients are required to place complete trust into their own network and the integrity of the data presented to them, or that they are required to share; as well as ensuring that the precise data that they need are available to them, their devices as well as to their healthcare professional, whenever it is needed and in real time. Lastly, the patient data must remain confidential in accordance with legal requirements. These demands are dependent upon a stable information and communication technology platform. Currently, many experts regard the Internet as simply not yet good enough for eHealth due to persisting reliability, availability and security issues. Each of which can undermine a patients' wellness due to the explicit risk related to telemedicine application and its dependency upon data management and data security.

Where even unintended individual human errors (slips) can cause massive data breaches, sensitive data of high value administered by poorly prepared and insufficiently aware healthcare professionals pose a huge incentive for malicious cyber attacks. The resulting limited trust in the system's integrity directly impairs the political incentives to facilitate digitalization further and increases the economic and organizational costs of further establishing robust cyber resilience. Precautions to ensure cyber resilience slow down or functionally impair the overall service performance by patients, due to delays, less user-friendly interfaces and identification requirements. As a result of diminished trust into both privacy and security, users may only reluctantly share highly personal data such as stigmatizing mental and sexual health conditions with a depersonalized and intransparent environment (Shenoy and Appel 2017). There is, to the best of our knowledge, currently no evidence-based knowledge on how far cyber security impairs the trust into the healthcare system and how reduced trust into cyber resilience impairs its performance or cost-effectiveness. Considering these likely side effects of hastily implemented digitalization without parallel implementation of a robust, transparent and technologically advanced cyber security strategy, we find the transparent, user-friendly and so far outstandingly successful cyber resiliency strategy provided by the Estonian example as a promising blueprint for future developments in other countries.

6. Conclusions

The digitalization of healthcare environments is changing the way healthcare systems operate and how they are organized, with significant changes for the patient's roles, responsibilities and opportunities. The benefits are manifold and relate to improved decision-making processes, availability of services, cost-effectiveness, and patient autonomy. The foundation of these changes is the constant and instant availability and exchange of patient- and service-related data that coordinate actors, communicate health-related patient data, provide the foundations for decision-making and facilitate the administrative processes at large. The comprehensive datasets occurring in this process provide the basis of the benefits of digitized healthcare, as well as the major challenge and vulnerability. A series of massive data breaches and enormous growth rates of cybercrime targeting valuable data processed in the healthcare systems, as well as a number of unintended breaches resulting from human failures, demonstrate an overproportional vulnerability of this societal sector, in which cyber security awareness is considered to lag behind other areas where security concerns appear more intuitively natural.

The health sectors' drive for digitalization to realize opportunities in, for example, eHealth and telemedicine will require far greater investment in cyber resilience if availability and security are to match the potential and ambitions of efficiency and effectiveness. Any progress towards ensuring the digitalization of the health sector needs to be measured against the current vulnerabilities to confidentiality, integrity and availability of before, between and after treatment data. Critical applications that are implemented to support achieving sustainable health goals may lack sufficient trust and reliability. Contact-tracing applications as they are introduced in the later phase of the COVID-19 pandemic have raised privacy and security concerns. While it is currently too early to thoroughly evaluate the outcomes of this particularly controversial symbol of accelerated digitalization in terms of public health benefits, the controversy around contact tracing apps provides an impressive example of the necessity of trust and its tight relationship with healthcare outcomes.

We argue that trust in healthcare systems affects its performance in a number of ways: (a) Patients hesitate to share sensitive data on their personal conditions if these are likely to be exchanged or administered in online databases and possible accessed by third parties. (b) The enormous additional investments in cyber security measures such as security-by-design or the engagement of qualified cyber security professionals as well as the related infrastructure increasing costs, planning and implementation time for digital innovations and thus slows down the transformation process. (c) Educational efforts by users including healthcare professionals, healthcare administrators, patients and third parties (for example, insurers) are necessary to develop cyber hygiene and reduce the risk of human failures, adding further to the time and financial costs of digitalized services.

Cyber security is fundamentally a human factor challenge and will require significant investment and research into achieving ways to develop a shared understanding across legal, institutional and national boundaries. The security aspect needs to be incorporated in the very early stages of designing and making it a central part of all digitalization processes.

While these measures to be taken may facilitate cyber resilience, increase the trust into a digitized healthcare with increased patient autonomy counteracting the simultaneous risk of privacy threats, parallel efforts have to be undertaken to ensure that all societal groups benefit from a more digitized healthcare. The empowerment and patient autonomy that comes with digitalization is of particular advantage for patients who know how to make use of their opportunities. Those with less technical affinity, but empowered, cannot take responsibility for their data security. This requires a balance of giving users full control and oversight over the use of their sensitive data, but without giving them the responsibility of making decisions that could unintentionally compromise their privacy.

In sum, the digitalization of healthcare is a potential major breakthrough in the development of sustainable healthcare worldwide. Sustainable healthcare system transformation, however, builds on the trust of its users and all measures taken to further improve the systems' effectiveness are subject to cost-benefit-analysis. Cyber resilience of healthcare systems plays an important role in building and ensuring ongoing trust as a central pillar of sustainability.

Author Contributions: All authors contributed substantially to all phases of the writing process, have approved the submitted version and agree to be personally accountable for the contribution as regards the accuracy and integrity of any part of the work.

Funding: This work was funded by the Research Council of Norway (Project nr. 302941).

Conflicts of Interest: The authors declare no conflict of interest.

References

Atasoy, Hilal, Brad N. Greenwood, and Jeffrey Scott McCullough. 2019. The digitization of patient care: A review of the effects of electronic health records on health care quality and utilization. *Annual Review of Public Health* 40: 487–500. [CrossRef] [PubMed]

Butavicius, Marcus, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. 2016. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv* arXiv:1606.00887.

Canham, Matthew, and Ben. D. Sawyer. 2019. Neurosecurity: Human Brain Electro-Optical Signals as MASINT. *American Intelligence Journal* 36: 40–47.

Canham, Matthew, S. Fiore, and B. Caulkins. 2018. Training Research to Improve Cyber Defense of Industrial Control Systems. In *Proceedings of the 62nd Annual Meeting of the Human Factors and Ergonomics Society*. Santa Monica: Human Factors and Ergonomics Society.

Canham, Matthew, M. Constantino, I. Hudson, S. M. Fiore, B. Caulkins, and L. Reinerman-Jones. 2019. The Enduring Mystery of Repeat Clickers. Paper presented at Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, August 11–13; San Jose: USENIX.

Canham, Matthew, P. Bockelman, and C. Posey. 2020. To Train, Or Not to Train: Exploring the Boundaries of Security Education and Training Awareness. In *Lecture Notes in Computer Science*. New York: Springer.

Carpenter, Perry. 2019. *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us about Driving Secure Behaviors*. Hoboken: Wiley.

Chen, Qian, and Robert A. Bridges. 2017. Automated behavioral analysis of malware: A case study of wannacry ransomware. Paper presented at 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, December 18–21; pp. 454–60.

Chien, Eric, Liam OMurchu, and Nicolas Falliere. 2012. W32. Duqu: The precursor to the next stuxnet. In *Presented as Part of the 5th {USENIX} Workshop on Large-Scale Exploits and Emergent Threats*. San Jose: USENIX Advanced Computing Systems Association.

Conrad, Eric, Seth Misenar, and Joshua Feldman. 2012. *CISSP Study Guide*. Rockland: Syngress.

Coventry, Lynne, and Dawn Branley. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* 113: 48–52. [CrossRef] [PubMed]

Cusack, Brian, Kaushik Sundararajan, and Reza Khaleghparast. 2017. Neurosecurity for brainware devices. Paper presented at 15th Australian Information Security Management Conference, Perth, Australia, December 5–6.

Darwish, Ali, Ahmed El Zarka, and Fadi Aloul. 2012. Towards understanding phishing victims' profile. Paper presented at 2012 International Conference on Computer Systems and Industrial Informatics, Sharjah, UAE, December 18–20; pp. 1–5.

Department of Homeland Security (DHS). 2019. Available online: https://www.dhs.gov/topic/critical-infrastructure-security (accessed on 16 May 2020).

Elgsaas, Ingvill M., and Hege S. Heireng. 2014. Norges Sikkerhetstilstand–en Årsaksanalyse av Mangelfull Forebyggende Sikkerhet. Available online: https://www.ffi.no/no/Rapporter/14-00948.pdf (accessed on 15 May 2020).

Ghernaouti-Helie, Solange. 2013. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Boca Raton: CRC Press.

Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security* 73: 345–58.

Halevi, T., J. Lewis, and N. Memon. 2013. A pilot study of cyber security and privacy related behavior and personality traits. Paper presented at ACM 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, May 13–17; pp. 737–44.

Health and Welfare Information Systems Centre (TEHIK). 2019. TEHIK—Data Security. Available online: https://www.tehik.ee/tervis/patsiendile/andmete-turvalisus/ (accessed on 30 November 2019).

Hughes, O. 2018. Norway Healthcare Cyber-Attack Could Be Biggest of Its Kind. *Digital Health*. Available online: https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/ (accessed on 21 February 2018).

Irwin, Luke. 2018. Breach at Norway's Largest Healthcare Authority Was a Disaster Waiting to Happen. *IT Governance Blog*. February 1. Available online: https://www.itgovernance.eu/blog/en/breach-at-norways-largest-healthcare-authority-was-a-disaster-waiting-to-happen (accessed on 15 May 2020).

Jalali, Mohammad S., and Jessica P. Kaiser. 2018. Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research* 20: e10059. [CrossRef] [PubMed]

Johansson, Grace. 2018. Half of Norway's Population Have Medical Data Leaked. *Cyber-Security News, Reviews and Opinion. SC Media UK*. January 19. Available online: https://www.scmagazineuk.com/half-norways-population-medical-data-leaked/article/1473442 (accessed on 15 May 2020).

Johnson-Laird, Philip Nicholas. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Cambridge, MA: Harvard University Press.

Jøsok, Øyvind, Benjamin J. Knox, Kirsi Helkala, Ricardo G. Lugo, Stefan Sütterlin, and Paul Ward. 2016. Exploring the hybrid space. In *Lecture Notes in Computer Science*. New York: Springer, vol. 9744, pp. 178–88.

Kim, Lee. 2017. Cybersecurity awareness: Protecting data and patients. *Nursing Management* 48: 16–19. [CrossRef] [PubMed]

Knox, Benjamin J., Øyvind Jøsok, Kirsi Helkala, Peter Khooshabeh, Terje Ødegaard, Ricardo G. Lugo, and Stefan Sütterlin. 2018. Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. *Military Psychology* 30: 350–59. [CrossRef]

Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 25: 1–10. [CrossRef] [PubMed]

Lai, Taavi, Triin Habicht, Kristiina Kahur, Marge Reinap, and Raul Kiivet. 2013. Estonia: Health system review. *Health Systems in Transition* 15: 1–196. [PubMed]

Martin, Guy, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. 2017. Cybersecurity and healthcare: How safe are we? *BMJ* 358: j3179. [CrossRef] [PubMed]

McCoy, Thomas H., and Roy H. Perlis. 2018. Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA* 320: 1282–84. [CrossRef] [PubMed]

Norman, Donald A. 2013. *Design of Everyday Things: Revised and Expanded*. New York: Hachette.

Parrish, James L., Jr., Janet L. Bailey, and James F. Courtney. 2009. *A Personality Based Model for Determining Susceptibility to Phishing Attacks*. Little Rock: University of Arkansas, pp. 285–96.

Passeri, Paolo. 2017. May 2017 Cyber Attacks Statistics. *Hackmageddon*. July 13. Available online: https://www.hackmageddon.com/2017/07/13/may-2017-cyber-attacks-statistics/ (accessed on 15 May 2020).

Posey, C., and M. Canham. 2018. A Computational Social Science Approach to Examine the Duality between Productivity and Cybersecurity Policy Compliance within Organizations. Paper presented at 2018 International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation (SBP-BRiMS 2018), Washington, DC, USA, July 10–13.

Priestman, W., T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire. 2019. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics* 26: e100031.

Priisalu, Jaan, and Rain Ottis. 2017. Personal control of privacy and data: Estonian experience. *Health and Technology* 7: 441–51. [CrossRef] [PubMed]

Reason, James. 1990. *Human Error*. Cambridge: Cambridge University Press.

Shenoy, Akhil, and J. M. Appel. 2017. Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics* 26: 337–41. [CrossRef]

Sütterlin, Stefan, Benjamin J. Knox, and Ricardo G. Lugo. 2019. TalTechi Küberkaitseteadlased: Ainult Tehnilistest Oskustest Ja Teadmistest Küberkaitses Ei Piisa. *Edasi.org*. October 30. Available online: https://edasi.org/48421/taltechi-kuberkaitseteadlased-ainult-tehnilistest-oskustest-ja-teadmistest-kuberkaitses-ei-piisa/ (accessed on 16 May 2020).

Targett, Ed. 2018. Revealed: Human Error, Not Hackers, to Blame for Vast Majority of Data Breaches. *Computer Business Review*. September 3. Available online: https://www.cbronline.com/news/kroll-foi-ico (accessed on 16 May 2020).

Verizon Communications Inc. 2019. *Verizon 2019 Data Breach Investigations Report*. New York: Verizon Communications Inc.

VG. 2017. 1200 Datamaskiner i Helse Sør-Øst Benytter Seg Av Utdatert Operativsystem. *Verdens Gang*. Available online: https://www.vg.no/nyheter/innenriks/i/BpbeQ/1200-datamaskiner-i-helse-soer-oest-benytter-seg-av-utdatert-operativsystem (accessed on 30 November 2019).

Weisberg, Yanna J., Colin G. DeYoung, and Jacob B. Hirsh. 2011. Gender differences in personality across the ten aspects of the Big Five. *Frontiers in Psychology* 2: 178. [CrossRef]

World Health Organization (WHO). 2016. From Innovation to Implementation—eHealth in the WHO European Region. Available online: http://www.euro.who.int/en/health-topics/Health-systems/e-health/publications/2016/from-innovation-to-implementation-ehealth-in-the-who-european-region-2016 (accessed on 16 May 2020).

World Health Organization (WHO). 2019. WHO Health Workforce—Data and Statistics. April 12. Available online: https://www.who.int/hrh/statistics/en/ (accessed on 12 April 2019).

Zhang, Xiang, and Badee uz Zaman. 2019. Adoption mechanism of telemedicine in underdeveloped country. *Health Informatics Journal* 26: 1088–1103. [CrossRef] [PubMed]