HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 6 • € 22

ISSN = 1377-7629

Cybersecurity: Preventing the Worst-Case Scenario

THE JOURNAL 2022

Is it Safe to Exchange Data?

The Need for Integrated Hospital/ Healthcare Organisation Interoperability and Cyber- and Information Security Plans

Henrique Martins | Associate Professor | ISCTE Business School | ISCTE-IUL, Lisbon | Faculty of Health Sciences | Universidade da Beira Interior | Covilhã, Portugal

One of the biggest health organisation challenges is to protect patient data within but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for effective, efficient, safe, sustainable and high-quality healthcare.

Key Points

- Patients can be at risk of harm due to breach in the safety of clinical procedures as well as when data and information systems security is breached.
- Different roles and multiple leadership is needed for a balanced approach to data usage and data security and protection.
- HL7® FHIR® does not increase risks for cyber- and information security.
- HoF (Hospitals/Healthcare Organisations on FHIR) can serve as a community of practice to stimulate further learning and cross-EU sharing and trust building.

Patients can be at risk of harm due to breach in the safety of clinical procedures as well as when data and information systems security is breached. They are equally at risk when information about them is not shared across the continuum of care, or research and new discoveries are delayed, new treatment solutions/approaches are not fund because of barriers to data sharing. Barriers to data exchange can cause the loss of lives or less optimal care.

One of the biggest health organisation challenges is to protect adequately patient data inside them but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for an effective, efficient, safe, sustainable and high-quality healthcare.

Different leadership roles are necessary for dealing with the interplay between digital transformation interoperability security and data protection as there is a constant need to balance four (only apparently) conflicting demands regarding healthcare organisational health data usage: 1) the needs of the Clinical Information Leads, 2) the needs of researchers who need to access data for secondary use; 3) the responsibilities of personal data protection; 4) the cyber- and information security needs.

An integrated approach to interoperability at the organisational level with cyber- and Information security is needed to pave the way to the design and adoption of a truly effective Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security (HICIS) Plan. Such document(s) should be the ongoing and live record and output of a joint collection of efforts.

Even though it doesn't impose any security model, the HL7 FHIR standard provides considerations on time keeping; communications security; authentication; authorisation/access control, audit, digital signatures, security labels; data management policies, and security/privacy event. The expectation of HL7 FHIR is in fact that the application of those security models does not impact the actual goal of HL7 FHIR that is enabling data sharing through an agreed health data model. Moreover, the Hospitals-on-FHIR (HoF) community of practice can be a forum for sharing not only best practices in interoperability but also on how it links to cyber- and information security as well as data protection.

and networks". It helps us as it places the cybersecurity realm into that of policy, leadership, managerial and even academic,

Different leadership roles are necessary for dealing with the interplay between digital transformation, interoperability, security, and data protection

Introduction

In most countries in the world, the population is growing old (OECD 2018), which, associated with unhealthy lifestyles and increased healthcare needs, is leading to healthcare systems sustainability challenges (OECD 2019). Health 4.0 (Bause et al. 2019) means a possibility for organisational change through the implementation of new digitalisation strategies and advanced information technologies. These, however, come with a new ever-increasing risk of "damage" to information. Cyber-attacks that impact or are directed to health units are ever more frequent due to the critical and intrinsic value of the information about humans which they harbour. There are multiple examples, often hitting public opinion and trust as they are mediatised. The Ransomware WannaCry, in 2017, led to British National Health Service disruption of service with over 20,000 appointments cancelled and estimated costs of 90M£. Recently, a cyberattack hit the second-biggest hospital in Czech Republic amid the coronavirus outbreak (Bîzg 2020). As a result of the attack on SingHealth, over 1.5 million patient personal data and medical records of over 160.000 appointments, including the prime minister's data, were exfiltrated in Singapore, a country known for its advanced cybersecurity policy, strategy and practices. These illustrate that healthcare can suffer in large cyberattack events even in countries with renowned national cross-sectorial cybersecurity capabilities and strategies, as it poses specific challenges. This can justify that special attention is needed within national defence strategies.

The increased digitalisation and datafication of health and care cannot be stopped, slowed down or even put into question due to fears of clinical harm in the face of raising concerns about the cybersecurity of health organisations and health systems. The way forward is to push for more, better efforts in both patient safety as well as cybersecurity, understanding that digital health indeed brings new risks as well as opportunities for patient safety, but inversely, patient safety methodologies and principles can inspire new ways of thinking in cybersecurity for health.

The European Commission talks about cybersecurity as a "set of concerns and actions taken to protect cyberspace, both in the civil and military domains, against threats resulting from the interdependency of its information infrastructures concerns and not just actions. Sharing concerns about the topic is already a way to foster cyber resilience.

Digital Health is a priority worldwide, reiterated by the World Health Organization (WHO) and put into evidence by the COVID-19 pandemic response in all countries. Recently the WHO Europe announced its Regional Action Plan, which reinforced the idea that digitalisation and digital transformation of health and care is expected to increase the quality of care and clinical safety. Such safety is ever more univocally dependent on information systems security. A larger use of these technologies brings more efficiency and effectiveness to health and care, but the increasing dependency of productive processes on digital platforms expands risk surface and risk exposure. As healthcare digitalisation progresses, tampered information systems will lead to increasing problems in health and care services and with higher potential and real impacts on individual human health. It is, therefore, paramount to break this negative cycle, thus enabling healthcare professionals and patients to take full advantage of the digitalisation of the health industry. This explains why there is a more declared interest of governments and health organisations in cybersecurity. There is, however, a severe lack of strategising, implementation of concrete actions and broad awareness of the severity of the matter. There is also a need to understand cybersecurity in the context of cyber- and information security interplay with interoperability needs and the concreteness of where these issues raise more preeminently – that is, in large healthcare organisations.

There should be no trade-off between minimum cybersecurity and patient safety. This is particularly relevant for telemedicine services. If a service requires privacy and security standards to be lowered, this service should not be performed as the risks associated with privacy and security breaches are high, and two types of consequences can be problematic: reputational and liability issues may arise to the hospital or other healthcare provider, and, more importantly, patient safety can be at risk. Security breaches can pose risks not just to patients and healthcare providers but, more generally, to the development of digital health as trust and goodwill may be eroded.

However, there is a need to move quickly to digital healthcare systems in all countries. Cybersecurity concerns should not stop this but rather increase its urgency. Developing and deploying eHealth services that fit and optimise existing healthcare systems is crucial to improve their performance, access, comfort and efficiency.

> **An integrated approach to interoperability at the organisational level with cyber- and information security needs to exist**

One of the biggest health organisation challenges is to adequately protect patient data within but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for effective, efficient, safe, sustainable and high-quality healthcare:

a) Healthcare cannot continue to be provided in stove pipes and isolated levels of care but rather in an integrated, holistic manner;

b) For a) to be enabled by coherent patient data, information systems have to be interoperable, allowing data exchange between all types of health institutions and the citizen's home;

c) For b) to be realised without service disruption, data modification, exfiltration or loss, the highest possible levels of cybersecurity must be in place. This, however, without limiting what was outlined in a) and without making interoperability described in b) a technical and economically unsustainable effort.

As interoperability and interconnections increase at a global scale, additional threats to data integrity will result from networks of health information between organisations and countries with different maturity levels, different attack surfaces and distinct technical and political vulnerabilities. Adequate security strategies, which include a solid data-sharing policy and inherent information exchange requirement, and a cybersecurity architecture, are needed for health organisations to be able to ensure confidential data is properly protected while shared when needed.

Leadership and Information Management in Hospitals/Healthcare Organisations

While roles like that of the Chief Information Officer (CIO) or similar posts often under names like Director for IT (Information Technology) or IS (Information Systems), or Data Protection Officer (DPO) are well established, in governance frameworks like COBIT® or even through legislation (the General Data Protection Regulation, in the EU), others may be less well-known or even under-recognised as crucial in the proper management of information in large complex healthcare organisations. These include roles like a dedicated officer to cyber and information security – the so-called CISO, as well as Clinical Information Leads.

The CISO - Chief Information Security Officer – who does not necessarily need to be a staff member of the IS directorate, nor a technical person, as cyber- and information security includes but does not limit itself to digitally supported information and practices, is the person who ultimately is responsible for ensuring information integrity of the hospital or other healthcare organisation.

The clinical leads include, as a minimum (even if operating at a part-time capability), three important roles, the CMIO, CNIO and CPIO. The Chief Medical Information Officer (CMIO) is a medical doctor operating as an organisational boundary spanner between clinical and information systems directorates, to promote medical information representation needs and all clinical aspects related to the use of IS. The Chief Nursing Information Officer (CNIO) equally acts to bridge between nursing and remaining non-medical informational needs, in articulation with the CMIO, to align the organisational multidisciplinary usage of information systems. Finally, the Chief Pharmacist Information Officer (CPIO) is a key player in ensuring closed-loop medication, appropriate drug and electronic prescription strategies, as well as several roles in digital approaches to patient safety.

Need for a Balanced Approach to Primary and Secondary Use of Health Data in Hospitals or Other Healthcare Organisations

There is a constant need to balance four (only apparently) conflicting demands regarding healthcare organisational health data usage:

1. The needs of the Clinical Information Leads, who represent genuine functional and business interests of clients (often patients) and healthcare professionals, encompass the highest possible Quality-of-Care demand for data exchange and interoperability to ensure better and more integrated care, including between organisations nationally and cross-border – primary use of health data.
2. The needs of researchers who need to access data for secondary use to promote internal but ever more increasingly interoperable research both inside the country in research networks but more importantly, EU-funded research and cross-border research efforts, paving the way to contributions to European Health Data Space related projects – secondary use of health data.

3. The responsibilities of personal data protection, incarnated by the DPO figure, are often more strongly empowered than the previous due to a clear legal basis for their role, and whose roles and responsibilities are relatively well established across the EU, although we see a wide range of more liberal or too conservative interpretations of similar situations rendering a too high degree of uncertainty to inter-organisational projects that may involve data sharing.
4. The cyber- and information security needs, seeking to secure information and critical information security systems, too often to the expense of practicality and health professionals' work effort and comfort or inducive of disproportional blockage to data sharing.

Finally, in most organisations the figure of a sort of Chief Interoperability Officer is completely absent. They could be the missing link between the four afore-mentioned demands. For now, and in most organisations, this role is to be played by a well-educated and well-prepared CIO. Interoperability, understood in its broadest sense and not limited to the technical layer but to include the legal, organisational and semantic (following the LOST model underneath the Refined eHealth European Interoperability Framework) needs to be seen as a cultural and procedural effort that is transversal to the organisation preparing it to cross-country and cross-border data sharing and care integration.

The HICIS Plan: Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security Plan

Having a LOST-inspired plan to tackle the interplay between interoperability and cyber- and information security helps to align different dimensions, such as and not exclusively:

1. Technical alignment – If the technologies that are set up, in particular, the standards used and how they interrelate, are not promoting both data exchange and data security, professionals will find a (not so secure) way to exchange data if that is critically needed for patient care and do some not so good use of health data for research if the need is pressing.
2. Procurement alignment – If different parts of the organisation buy technologies or consult on processes which are not acting synergically, once the commitment to buy is firmly established it is followed by an implementation tension that leads to conflicts.
3. Education alignment - Education of internal and subcontracted IT staff as well as IT providers on the matters of interoperability, cyber- and information security, and data protection needs to be planned and considered holistically so that messages are consistent and coherent and not conducive to further tension raising. Clinical staff should also be included in such educational initiatives to help bridge the gaps between subcultures but also different needs.

When such an integrated approach to interoperability at the organisational level with cyber- and information security exist, we can talk about a truly effective HICIS Plan: Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security Plan. Such document(s) should be the ongoing and live record and output of the joint efforts of two teams and focus of attention within the directorates for information systems: the interoperability team and the cyber- and information security team, both operating under the Chief Information Officer (CIO) or similar post but with dynamic and intense interrelations with Clinical Information Leads and the Data Protection Officer (DPO).

HL7® FHIR® and Cyber- and Information Security and the HoF Community

As explicitly indicated in the standard (http://hl7.org/fhir), HL7 Fast Healthcare Interoperability Resources (FHIR) is "not a security protocol, nor does it define any security-related functionality". This, at first glance, may seem a shortage, but is, on the contrary, a point of strength, allowing the adoption of various security protocols and models based on the interoperability paradigm chosen (e.g. document, REST, messages, services) and the context requirements (e.g., enterprise vs patient vs cross-enterprise centric model).

The expectation of HL7 FHIR is, in fact, that the application of those security models does not impact the actual goal of HL7 FHIR, that is, that of enabling the sharing of data through an agreed health data model.

Even though it doesn't impose any security model, the HL7 FHIR standard provides considerations on timekeeping, communications security, authentication, authorisation/access control, audit, digital signatures, security labels, data management policies, security/privacy event reporting and other related topics; documenting them in the HL7 FHIR standard security page.

Moreover, the standard defines specific FHIR resources as Provenance, Consent and AuditEvent, and metadata elements (e.g. security labels) for better supporting the adopted models. Additional and more detailed reflections on cybersecurity aspects associated with the HL7 FHIR standard can be found on their blog.

A community-of-practice approach to interoperability, cyber- and information security and data protection is perhaps the best way to help leaders deal with and learn from each other in such complex interconnected matters. The HoF (Hospitals/Healthcare Organisations on FHIR) constitute a growing community of practice promoting the use of interoperability standards and the exchange of experiences in how best to use the HL7® FHIR® standard and ultimately also the experiences around data sharing and, in the EU, the promotion of the generalised use of the European Electronic Health Record Exchange format (EEHRxF). Members of HoF have progressively asked to see a more intense discussion of the interplay between interoperability, in particular the use of FHIR and cyber- and information security, as well as data protection issues. This will be sought in the coming annual work plan of the HoF for 2023 as part of regular online sessions starting in January 2023.

Acknowledgment

The author would like to acknowledge the kind contribution of Giorgio Cangioli to the part of the article about HL7®FHIR® and information security, as well as Catherine Cronaki's and Valentina Tageo's continuous efforts to build and enlarge the HoF Community (www.hospitalsonfhir.eu).

Conflict of Interest

None. ■

REFERENCES

Bause M, Khayamian Esfahani B, Forbes H, Schaefer D (2019) Design for Health 4.0: Exploration of a New Area. Proceedings of the Design Society: International Conference on Engineering Design. 1(1):887–96.

Bîzgă A (2020) Mysterious cyberattack cripples Czech hospital amid COVID-19 outbreak. Available at https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak

OECD (2018) OECD Regions and Cities at a Glance. p. 160.

OECD (2019) Health at a Glance 2019.

HealthManagement.org

Promoting Management and Leadership