Where There is No CISO

Johan Ivar Sæbø, Andre Büttner, Nils Gruschka, Bob Jolliffe, Austin Mcgee

Where there is no CISO

Johan Ivar Sæbø
University of Oslo, Oslo, Norway
johansa@ifi.uio.no
ORCID 0000-0001-9873-4544

Andre Büttner
University of Oslo, Oslo, Norway
andrbut@ifi.uio.no
ORCID 0000-0002-0138-366X

Nils Gruschka
University of Oslo, Oslo, Norway
nilsgrus@ifi.uio.no
ORCID 0000-0001-7360-8314

Bob Jolliffe
HISP Centre, University of Oslo, Oslo, Norway
bob@dhis2.org

Austin McGee
HISP Centre, University of Oslo, Oslo, Norway
austin@dhis2.org

Abstract: Globally, health information security and associated topics have received considerable attention from both professionals and the academic community. The literature on the threats and mitigations when it comes to developing countries is scarce, and tends to focus on issues such as cryptographic techniques for secure safe data transmission or patients' perceptions of data confidentiality. However, investigation of health information threats in relation to the local context has received less attention. In this paper we reflect on a long-term and global action research project that presents different perspectives on information security. Operating in environments of absent or obsolete relevant jurisdiction, poor institutional capacity for adherence and oversight, and limited awareness of appropriate security and confidentiality issues, we note unique security and confidentiality threats "where there is no CISO". We reflect on mitigations adopted over the years to counter rising threats, and provide recommendations for practice and further research in this regard.

Keywords: information security, digital platforms, data privacy, data confidentiality

1. Introduction

Information security is usually defined by the so-called CIA triad, i.e. the properties confidentiality, integrity, and availability, or more precisely the safeguarding of these properties. Examples of security-critical situations in the context of health information systems (HIS) are: medical diagnoses shall only be accessible to authorized health personnel and shall be kept confidential otherwise; an electronic medical prescription shall not be changed, i.e. the integrity of the data set must be ensured; in case of an emergency immediate access to medical data (e.g., possible drug allergies) is important, therefore, uninterrupted availability of the health service is required. Violation of the security goals in the aforementioned examples can have different consequences from blackmailing with the threat of publishing medical conditions (or reputation loss due to actual publication) to illness or death due to taking the wrong drug or dose. The reasons for violation of information security are diverse. It can be caused by natural disasters, accidental misbehavior, malicious actions or other causes. The goal of information security is the development and implementation of protective measures against these violations. Typical examples are redundancies of services, backup of critical data, control mechanisms to restrict access to data, cryptographic measures like encryption or digital signatures to ensure confidentiality and integrity, and network monitoring to detect and prevent remote attacks.

This paper reports from a large international effort to strengthen national health information systems in developing countries. It centers around the development and implementation of the open source platform DHIS2. Development of DHIS2 is coordinated by the University of Oslo, Norway, and implemented in a range of countries around the world [1]. As a web-based system, DHIS2 is typically set up on local servers in the respective countries, or deployed using commercially available cloud services [2]. As a digital platform in the public sphere, DHIS2 also potentially has a "dark side" [3]. While issues of confidentiality and adverse effects of user data have seen some exploration, for instance related to behaviorall data [4], we in this paper look at aspects of information security as such platforms are developed and implemented globally, also where the context offers challenges considerably different than what has been hitherto examined.

Systems using DHIS2 contain various types of health data, from aggregate statistics to registries containing personal health data. Security issues can thus be broadly categorized in three groups; those relating to the data itself, such as correct handling of confidential data; those relating to hosting the system, including server monitoring and back-up plans; and those related to the software platform and its development, such as community contributions through apps, ensuring secure code, and routines for handling threats. Building on the authors' own involvement for the past two decades, we reflect on the special nature of the project, events and threats experienced, and the measures employed to counter them.

Our title is a nod to David Werner's classic book "Where there is no doctor: A Village Health Care Handbook" [5], which has been a strong influence and motivation for the HISP project in it's aims to strengthen primary health care in communities around the world. It is also an acknowledgment that in many of the settings where we are involved, there is in fact no CISO (Chief Information Security Officer). While we do not aim to provide here a "handbook" for resource-constrained settings, we are intrigued by the apparent lack of focus on contextual health information security issues in the literature.

Our research questions are; What is the nature of information security threats in public health information systems in the Global South, and how can they be mitigated?

2. Methods

This research builds on two main methods. First, we as authors are involved in the HISP project, which coordinates the development of DHIS2 and its implementation in several countries. Working with implementing agencies, typically ministries of health, we have nearly 2 decades of action research from which to reflect on the topic of this study. Second, some of the authors are conducting a comprehensive scoping review of information security and confidentiality issues in health in developing countries. While the scoping review is not completed at the time of writing, it forms the basis for the included review of relevant literature here. We start by describing the process of the review.

2.1. Scoping review

We have been conducting a scoping review [6] to get an overview of the research that has been done regarding security and privacy of health information systems with particular focus on developing countries. The review was split into four different stages: (1) collecting articles, (2) reviewing titles and abstracts, (3) reviewing full-texts and (4) summary of results.

In the first stage, a search query was defined that was used against relevant databases to collect a list of potential articles. The query was constructed as a combination of various IT-security and privacy terms, different health terms and terms describing the developing context and a list of low- and middle-income countries. The general structure of the query used was as follows: (<security-terms> OR <privacy-terms>) AND <health-terms> AND <developing-countries-terms>. After applying the query to the Web of Science, Scopus, IEEE and ACM digital libraries, putting the results into one list and removing duplicates we had a list of 3486 articles. All titles and abstracts were then read by at least two reviewers each for inclusion or not. When there was a conflict between the decision of the two reviewers, this was solved by a third reviewer. In order to be included, the titles and abstracts should indicate that the article addresses security or privacy in the context of health IT-systems for developing countries. Articles written in a language other than English were excluded. The same applies to articles that were only a summary of conference proceedings or that clearly did not cover all relevant topics. This procedure resulted in a list of 198 included articles for full-text reviewing.

At the time of writing, the full-text review by two reviewers has not been completed. Even though the review is not completed, we lean on the preliminary results as they provide interesting insights into the research trends and can be compared to the reflections coming out of our long-term engagement in the field of health information systems in developing countries.

2.2. Reflections from action research

As practitioner-researchers engaged in both developing and maintaining the DHIS2 software, as well as providing direct or indirect support to tens of implementations of it in the health sector in the Global South, we categorise our main research approach as action research [7]. We did not begin by framing a research project with the aim of collecting data on security incidents. In that sense it is a reflection on past activities which were geared primarily towards supporting

implementations and providing troubleshooting support as requested. The security related incidents emerged through these activities in a non-systemic way and alongside many other issues. The DHIS2 core team at the time did not maintain any sort of incident register.

For this study, we draw on two perspectives of this action research; first, the larger Health Information Systems Programme (HISP), a project not bound in time or space, but an AR-project with global reach and of a networked nature [8]; second, a range of more specific engagements with formalized structures typically focused on collaboration with ministries of health in the Global South. For the sake of anonymity we do not list countries or partners here. Taken together, our empirical basis spans tens of countries over several continents for 15 years, where we hold and have held various roles. Most important for this study has been that some of the authors have been active in helping countries with all issues related to hosting, held training sessions and workshops related to hosting and information security management, and been the first line of support when countries need assistance with their DHIS2 instances. One of the authors is also engaged with improving security management internally in HISP, working to improve not just the software but the routines and structures appropriate for handling the myriad security issues of a global network.

3. Related literature

Information security is a broad discipline that covers different levels from software implementation details to organizational and governmental security management. Confidentiality, integrity and availability (CIA) are important properties to protect software systems and in particular its users [9]. The term confidentiality refers to the goal of making data available to authorized parties using cryptography and authentication. Integrity means that it must be ensured that data has not been modified without being noticed. The goal of availability is to make sure that applications and data are accessible and thus to avoid downtime. Similarly, user awareness and acceptance for information security is critical, and capacity building about security risks when using digital systems is important [10]. In particular, health information is very sensitive and requires the highest security standards [11]. A number of regulations have been developed in response to this, such as the EU General Data Protection Regulation (GDPR)[1] or the US Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] to protect their citizens.

We now turn to findings from the in-process scoping review. A main observation is that there is a large and growing literature related to information security originating in the global south. However, a large part of this deals little with contextual factors and focuses on technical solutions with global applicability. One strand of the literature concerns development of security protocols and cryptography (see for example [12], [13]). Another strand looks at the potential of blockchain technology, which can have a role to play in fragmented health information systems which plague countries both rich and poor (see for example [14], [15]).

Of studies that engage with the development context, many point out that awareness and skills around information security vary greatly, with several pointing out that this is generally lacking. Jack et al. [16] conducted a survey among health care providers in South Africa on information privacy and security, and found that many are ignorant or lack the ability to follow even simple info security procedures. A study from Sri Lanka found that security awareness was actually quite good among health staff, but that their less secure behavior contradicts with their actual concerns [17]. A survey of 15 countries in Africa, Asia, and the Americas on HIV clinics notes that some sites do not backup their data regularly [18]. Gesicho et al. [19] does not cover security explicitly, but finds that, despite increased activity to implement national health data warehouses in developing countries, little attention has been paid in these implementations to ethical issues, including providing data confidentiality and security.

A second strand of studies look at the legal framework, its existence, its relevance, and how it is enforced with various sanctions. Namara et al. [20] find that only a few countries in Africa have developed comprehensive legal frameworks and have meaningful enforcement policies. Interestingly, they do point out that privacy values are cultural, and differ significantly across countries. They fail to provide any examples of this however. Being more specific, they mention how lack of oversight leads health staff to ignore regulations by for instance conversing around patients on facebook and whatsapp, and in general store data outside the patients' jurisdictions. Related to the relevance of legal framework, Antonio et al. [21] looks at health information privacy in the Philippines and concludes that technological development has outpaced policy and practice in this regard. In a review of security assessment frameworks such as HIPAA, Gerson and Shava [22] examines the applicability to Namibia's public health sector and calls for security controls to conform with international standards.

One notable topic on which little is written is security incidents, apart from anecdotal reference to data loss and virus more generally. Antonio et al. [21] mentions a few cases from the Philippines where for example videos from students attending operations were publicly circulated. Moreover, some attacks on health records in India were addressed by Misra et al. [12]. There are some studies that contextualize security management. For instance, a delay tolerant architecture, with emphasis on latency, is found to be important in resource-constrained countries [23]. Pankomera and

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736

van Greunen [24] does point to some of the challenges in developing countries, such as poor funding and infrastructure, and a shortage of qualified staff. They also point to natural hazards such as floods, fires, tornados, which can be a larger threat to physical security infrastructure than in more resourced environments. A relevant contextual finding is that as health staff in general do not have access to computers, they use memory sticks for their personal files, introducing malware to their office computers [25]. On the impact of development agencies, Hai et al. [26] looked at how the short-term funding of development projects can negatively impact confidentiality and security. When donor-funded special HIV clinics closed down at the end of the project, patients had to shift to general clinics which were seen as not adhering to the same data confidentiality standards, negatively impacting the patients. Khan and Hoque point out that Bangladesh is lacking a centralized method of identification such as the social security number, making it difficult to link data from separate databases. They propose an approach to solve this problem in a secure and privacy preserving manner [27].

4. Empirical findings

The project from which we report, the Health Information Systems Programme (HISP), has its roots in participatory action research in South Africa in the 90s. It is a global network engaged in software development and implementation with stakeholders, typically ministries of health in developing countries, to strengthen HIS. Over the last two decades, the network has grown globally, and the software developed has progressed from an early standalone desktop application to a flexible, web-based HIS platform called DHIS2, now in use in more than 70 countries. Participatory approaches are still applied to both software development and systems implementation [28]. The University of Oslo, Norway, is leading the development, and is also supporting, sometimes extensively, the implementation of DHIS2 in country HIS'. Our case then, is not only of a software developer, but also of a community who are morally, and sometimes also formally, engaged in country HIS implementation activities. This places a special responsibility on the community given that many of the implementing countries have comparatively weak institutions, and poor information security management in the public sector. We now move to some observations from the last decade, coinciding with the move from desktop to online technology, and an increase in scale and scope of the implementation activities.

The shift that happened from around 2011 from the earlier version of DHIS as a desktop system towards a DHIS2 web-based system that ran over the public internet brought with it human resource and physical infrastructure challenges which few countries were well positioned to address. The IT staff in ministries of health and the technical support from regional support entities by and large did not have the linux technical system administration skills nor the organisational structures to effectively manage security. Critically, even today, there are very few country deployment teams who have amongst them a defined security role of any sort. This has led to a reality that most deployments live with a considerable amount of unmanaged risk. A significant one in many deployments is the over-dependence on a single person who has all the knowledge and all the keys to the system. In risk identification exercises carried out in three countries, this emerged as the highest scoring risk in each. Given this, the actual incidents of data loss, exposure or breach have been relatively few. Below is a short summary of typical incidents:

4.1. Some incidents we are aware of

The following is a short list of incidents which are in some way security related which have occurred in the past decade. Note that we (the authors) are not actively maintaining any production DHIS2 system. Some of us are involved in advising, training and occasionally assisting with incident response. We are not at liberty to disclose details which would allow the system to be identified.

4.1.1. Physical Infrastructure related

In one country the national Health Management Information System (HMIS) was running on a server in a national government data centre. One evening there was a fire caused by an overloaded electrical connection and the server was badly damaged. The disk on which the data was stored was apparently unreadable. In the aftermath of the fire it was discovered that the Ministry of Health had no functioning backup of the data that was less than six months old.

In another country, the Ministry of Health hosted the national system in a purpose built data centre within the Ministry main building. The building had an ongoing problem with rodents and at one stage the rodents penetrated the data centre. Intermittent faults, breakdowns and performance degradation was finally, on physical inspection, traced to rodent damage to the insulation on network cables.

Where systems have been implemented on physical infrastructure, for example in ministry or government data centres, there have also been challenges related to the management and monitoring of the surrounding network environment (for example domain name services) and the reliability of the internet connection. It has been observed in a number of settings that the single internet connection to the service provider is shared by both the servers in the data centre and also all of the office dwellers in what is often a multi-storey, multi-ministry building. With the result that there is massive congestion during working hours effectively rendering the system unusable from the outside.

4.1.2. Cloud hosted systems

Whereas it is clear that systems can be fragile when hosted in poorly commissioned or poorly managed physical infrastructure, just moving them to "the cloud" has not been without its own risks. A handful of incidents stand out over the past few years.

In one case an external consultant was providing technical support by managing a national HMIS on a VPS from a commercial cloud infrastructure provider. At the end of his contract, after what seems to have been a misunderstanding over whether the country had brought up to date backups on-shore, the consultant deleted the VPS, resulting in the loss of one year's data.

In another case, a Ministry of Health in a country set up their own account with a cloud VPS provider and secured funding for one year to provision a VPS for running both the national HMIS and an HIV/AIDs patient monitoring system. At the end of the year when the bill became due, it was discovered that no budgetary provision had been made for renewal. The services were cut off and remained inaccessible for approximately 6 weeks while the government department scrambled to find alternative payment sources to cover the bill. (There have been a number of variations on this same scenario over the past few years, where the Ministry of Health have temporarily lost access to their systems and data).

There are other issues which are more particular to the geo-political context of the systems and system owners. Most of the commercial cloud providers operate off a credit card payment system. One of the authors has direct experience of trying and failing to open cloud based accounts from various West African countries and also from India. The transactions were automatically failed without explanation, but presumably linked to the origin IP address. When the same transaction was made through a VPN back through Europe, it succeeded. When the same "trick" was tried by a colleague using a local West African credit card it proved impossible to open an account. The commercial world of private cloud hosting is not a flat world and all credit cards are not created equal.

We have also seen cases where countries have been denied access to commercial cloud services (and SSL/TLS certificates) due to economic sanctions.

An unusual event in 2012 confirmed that the laws of physics and geography can still play a part in the modern age. Following the successful installation of the Kenya system on Linode in 2010, Rwanda also rolled out a national DHIS2 system in 2011, but this time hosted locally within the MOH. One morning a ship trailed anchor through the harbour of Mombasa and snagged the undersea fibre optic cable linking Kenya to the world. The Kenya system was effectively offline for a week. During that same week the connectivity to the Rwanda system was excellent, particularly as the network within the country was generally quieter than normal.

4.1.3. Security breaches

There have been numerous incidents of data exposure due to misconfiguration of database access control or breach of the server backend through compromised ssh user accounts. We have seen no evidence to date that the data itself was targeted in any of these cases. Of course we cannot conclude this with any certainty, but we haven't seen any obvious subsequent use of the data (e.g. for extortion). We can guess that, particularly given the low resource environment, the commercial value of the data is not sufficiently high to attract more determined attackers with criminal intent to engage in identity theft or ransomware attacks. Though, given the political importance of many of these national systems, the possibility of ransomware attacks is a very real concern. Given that many DHIS2 implementations are in areas experiencing significant internal and external conflict, there is also a real dimension of concern that attackers might seek out personal data for purposes that might threaten their physical rather than financial well-being.

What we have seen in all of the breaches that we know about is that the attackers have seen the machine as a more attractive target than the data, being recruited into bit-coin mining or being taken over to potentially attack other systems. It should be noted that intrusion detection systems of any sort are usually absent, so there is no definitive way to claim that data has not been targeted.

Examples of known deliberate security breaches:

- Successful attacks on the backend using ssh. In one case we know that a superuser account was legitimately created in the afternoon and credentials were shared with the new user over the mobile phone (whatsapp or email). Later that evening there were three successful logins from two different countries (China and France). The account had been setup to allow password authentication. Given that the user was an administrator, effectively full access to the machine had been gained by one or more parties.
- Zero-day vulnerabilities. A critical vulnerability was discovered in March of 2017 in the Apache Struts library that is used within DHIS2. It was a particularly nasty vulnerability that potentially gave an attacker the ability to execute arbitrary commands on the server. The vulnerability was being actively exploited around the world and a number of DHIS2 systems were effected. Although a patch was produced by the DHIS2 core developer team within 24 hours, they did not at that time have a formal process for dealing with such events so there was some delay between patching and announcing publicly (during which time there was vigorous internal discussion on what action to take regarding public disclosure). Even after patches were released and

announcements made publicly, we were receiving reports for some months afterwards of un-patched systems getting attacked.

Again we don't believe that systems affected by either of the above were deliberately targeted for their data, but cannot prove either way.

Actors who are really interested in the data have not always had to rely upon attacking the system physically or with code. One country has reported that it is a common practice amongst foreign backed NGOs to recruit people from within the public health service (with credentials in the system) in order to access data which they would not otherwise have had access to. Processes around user management, particularly the disabling of user accounts on leaving of the service are usually absent.

5. Discussion

Our point of departure was a review of relevant literature on information security in the health sector in developing contexts. Our study adds to all the strands of the literature identified earlier. In particular, we highlight more detailed accounts of how for instance infrastructural and environmental hazards are significant [24].

5.1. Incidents and nature of threats

As discussed above, we are not aware of any significant targeted breaches of production DHIS2 systems or the data they contain. The rapid adoption and high profile of large-scale DHIS2 implementations addressing the COVID-19 pandemic has likely increased the size, value, and visibility of security penetration for systems built upon DHIS2, increasing the likelihood that a serious breach might be perpetrated in the future.

The nature of threats do not seem to spring out of any perceived value of the data itself, though ransom could be an issue as the data is necessary for the functioning of the health services. What has been documented is more about using the servers for other purposes, i.e. the hardware and processing power is more attractive than the data. Access to data is a concern due to the role of foreign organizations, who may be interested in the data for reporting or research purposes, where access can be gained without necessarily having the formalities in place.

This empirical observation (which we cannot readily prove) that attackers seem not to be trying to get at the data is not a reason to be complacent. Even if we theorize that the financial value of the data is low, we also need to take into account that the consequences of abuse of data relating to extremely vulnerable individuals who are somehow marginalised or living on the edge of legality in society can be severe.

5.2. Hosting issues

When deploying a service, one of the most important questions is: shall the service be hosted locally on our own hardware or shall we rent resources at a cloud provider? Since the introduction of Amazon Web Services in 2006, cloud computing has become the most widespread hosting platform. More and more small, medium and large enterprises are outsourcing their resources to platforms such as Google, Microsoft and of course Amazon, who is still the market leader. Cloud computing promises mainly economic advantages including reduced investment costs, easy self-service setup, and rapid scalability of resources. However, in addition cloud computing has many security benefits, at least when operated professionally. For example, the large cloud providers' data centers have very good redundancies in terms of power supply and Internet connectivity and high standards regarding physical access to the servers. Further, they offer "standard" security measures, like backup, anti-virus scanning, firewalling etc. as easy to use services and usually for an additional fee.

HISP implementers have explored these cloud hosted Virtual private Server (VPS) options since the early days of DHIS2 going "live" on the internet. When the DHIS2 was rolled out nationally in Kenya in 2010 it was hosted on a VPS from a company called Linode. Besides using the large cloud providers, DHIS2 implementers have a long history of working with smaller providers such as Linode, Dediserve and Contabo who all offer various niche advantages. For example Dediserve allowed the setting up of an account without a credit card which had proved to be a major stumbling block for government procurement working with the larger providers. Contabo offers rock bottom prices which have proven extremely popular in Africa.

Another phenomenon that has emerged in recent years is the rise of private companies adding value to the basic cloud VPS and offering DHIS2-as-a-service.

Despite the many touted (and actual) benefits of the new cloud business models, as we saw in the cases above, country systems which have been deployed on commercial cloud environments have faced different types of problems. There is still a risk of data loss without a costed and tested backup plan. Security still needs to be managed, but the types of risk to be managed are different. For example a missing budget item for cloud "rent" can lead to unavailability of the system.

As an illustration of the complexity of factors around this question, one author recalls attending a workshop of WAHO (the West African Health Organisation) on server management in Bobo, Burkina Faso, 2018. Of the ten or so WAHO member states who were represented in the meeting, they were split down the middle on the current state and future

plans. One half were hosting systems physically in the country and were without exception looking forward to moving to the cloud. The other half were hosted on the cloud, which they, again without exception, viewed as temporary contingency as they aspired to bring the systems back into the country.

5.3. User data

The management and protection of users in the system (mostly employee data) has received very little attention, including until quite recently in the software itself. There is a growing awareness of the obligation to protect vulnerable groups in the health sector, like HIV+, sex workers, refugees etc, and in general for patient data. However user data, including telephone numbers, email, internal messages etc. have not been seen as high value data and have sometimes been available indiscriminately to any other user of the system. This should be a cause of considerable concern. In particular aggregate routine reporting systems which contain no individual patient data are generally considered non-sensitive, yet they contain details of often 10s of thousands of health workers. In addition to the potential exposure of the personal information of these users themselves, personal information such as phone number and email could be abused to conduct phishing attacks against system administrators. This could in theory allow unprivileged users to maliciously gain access to credentials providing them access to much more sensitive information and controls within the system. The exposure of user details to other users of the system has been removed from recent versions of the software, but this type of data has not received significant attention as a privacy concern or as a vector for attack on the larger system.

5.4. The need for global awareness

The role of funders of health information system projects has also been given limited attention in relation to security. The core DHIS2 development team works to develop the DHIS2 software platform, supporting increasing numbers of high-profile implementations around the world. The organic growth of DHIS2 software complexity and global adoption yielded a culture lacking in many fundamental security controls within the core development team. This has largely been the result of limited resources, and limited interest from funding organizations in allocating those resources to champion security practices in a context which undervalues them. Largely as a result of muted interest in and awareness of security within the governments and international development organizations implementing and funding DHIS2, the need for strong security practices and policies has not been emphasized within the core team. Additionally, the nature of DHIS2 as an open-source, freely available software platform provided without warranty or guarantee has limited the political and financial pressures which often incentivize commercial enterprise software products to reduce their own legal risk by investing in security practices.

There is a need for leadership within the global health implementation and vendor communities. The identification of security risks and pressure to limit them have to date not been championed by implementing countries or funding organizations. This dearth of conventional incentive should not reduce the moral obligation of community members such as DHIS2 to push for increased security and privacy controls. A small set of high-impact changes have the potential to significantly reduce security risks in production software implementations and increase awareness of those risks amongst implementers and funders.

6. Conclusion

The main conclusion is that, consistent with the literature above, we have found there are a range of organisational factors, infrastructure fragilities and perhaps cultural factors related to risk acceptance which conspire to make it difficult to adequately secure health information systems in many developing countries. We have conjectured that the low financial value of the data might be a factor in explaining why attacks on such systems have not been more widespread.

To add to the difficulty, the DHIS2 software itself has been a complex and difficult system to maintain securely, even by experienced implementers. Great strides have been made in recent years in improving the development process as described above. One positive indication of progress has been the different impact of the Apache Struts vulnerability in 2017, and the more recent and equally critical log4shell[3] vulnerability which was discovered in December 2021. Whereas the former created considerable chaos and a scramble to reach consensus on a response from the core team, by the time of the latter in December 2021 there was a team ready to mitigate and manage communication and a vulnerability management plan to follow.

But the expansion of the global project and subsequent "industrialization" of the software development process has in some ways moved us away from the strong participatory tradition of the early years. One consequence of this has been that developers are perhaps only weakly aware of the security challenges in the field. The security challenges are so enormous and growing, that it is only through a stronger collaborative and informed effort, that the software development process itself can better support the software implementation process. A drive towards increasingly sophisticated digital technology risks leading to a DHIS2 that is increasingly difficult to manage and secure in practice.

As a leader in the public health space, the DHIS2 core development team endeavors to champion security within HISP as well as in the larger community. Within the past year the team has embarked on this journey by creating and

[3] https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know

implementing thorough software vulnerability management and transparent public disclosure processes, some of the first in the sector. In addition, two experienced information security managers have been recruited to serve in the CISO role within the University of Oslo. This role will have the mandate to promote secure development and implementation practices within the core team and more broadly within the international development and global public health ecosystem.

Having dedicated CISO roles both at the HISP Centre of the University of Oslo, which coordinates the development of DHIS2, and amongst system implementer teams will not necessarily solve these problems, but the hope is that they will reinforce the effort to bring these into view and provide more strategic and systemic responses.

In summary, documentation of the nature and prevalence of security threats against health information systems in developing contexts is under-developed. Security incidents and risks are not well understood, largely due to limited understanding and awareness of security in the organizations and government departments implementing health information systems. The increasing prevalence of individual data in the systems and the high-profile use of them to address, as an example, the global COVID-19 pandemic are likely to increase the risk of malicious security breaches. In addition to malicious action, accidental confidentiality, integrity, and availability degradation continues to be a cause for concern. More study of security risks and mitigations in this context is needed, as is increased awareness and advocacy from stakeholders in the public health space.

7. References

[1] E. Adu-Gyamfi, P. Nielsen, and Sæbø, Johan, "The Dynamics of a Global Health Information Systems Research and Implementation Project," p. 7, 2019.

[2] B. Jolliffe, O. Poppe, D. Adaletey, and J. Braa, "Models for Online Computing in Developing Countries: Issues and Deliberations," *Information Technology for Development*, vol. 21, no. 1, pp. 151–161, Jan. 2015, doi: 10.1080/02681102.2014.902354.

[3] B. Nicholson, P. Nielsen, and J. Saebo, "Special issue: Digital platforms for development," *Information Systems Journal*, vol. 31, no. 6, pp. 863–868, 2021, doi: 10.1111/isj.12364.

[4] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

[5] D. Werner, C. Thuman, and J. Maxwell, *Where there is no doctor: a village health care handbook*. Hesperian health guides, 2020.

[6] H. Arksey and L. O'Malley, "Scoping studies: towards a methodological framework," *International Journal of Social Research Methodology*, vol. 8, no. 1, pp. 19–32, Feb. 2005, doi: 10.1080/1364557032000119616.

[7] R. L. Baskerville, "Distinguishing action research from participative case studies," *J of Systems and Info Tech*, vol. 1, no. 1, pp. 24–43, Mar. 1997, doi: 10.1108/13287269780000733.

[8] J. Braa, E. Monteiro, and S. Sahay, "Networks of Action: Sustainable Health Information Systems Across Developing Countries," *Management Information Systems Quarterly*, vol. 28, no. 3, Sep. 2004, [Online]. Available: http://aisel.aisnet.org/misq/vol28/iss3/3

[9] M. G. Solomon and M. Chapple, *Information Security Illuminated*. Jones & Bartlett Publishers, 2004.

[10] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, vol. 8, no. 1, pp. 31–41, Jan. 2000, doi: 10.1108/09685220010371394.

[11] R. Hulkower, M. Penn, and C. Schmit, "Privacy and Confidentiality of Public Health Information," in *Public Health Informatics and Information Systems*, J. A. Magnuson and B. E. Dixon, Eds. Cham: Springer International Publishing, 2020, pp. 147–166. doi: 10.1007/978-3-030-41215-9_9.

[12] M. K. Misra, A. Chaturvedi, S. P. Tripathi, and V. Shukla, "A unique key sharing protocol among three users using non-commutative group for electronic health record system," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 8, pp. 1435–1451, Nov. 2019, doi: 10.1080/09720529.2019.1692450.

[13] P. Kamble and A. Gawade, "Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks," in *2019 International Conference on contemporary Computing and Informatics (IC3I)*, Dec. 2019, pp. 69–73. doi: 10.1109/IC3I46837.2019.9055531.

[14] P. K. Sari and S. Yazid, "Design of Blockchain-based Electronic Health Records for Indonesian Context: Narrative Review." https://ieeexplore.ieee.org/abstract/document/9255571?casa_token=aPIf9bowQucAAAAA:JOJd5MYSIOa6l2Hn3ic_i0HgOevIFgCyvVYyzY6I9G8k1eKXijDkYBWkCHvoUEgz_qb7WuZ33A (accessed Jan. 17, 2022).

[15] S. Osebe *et al.*, "Enabling Care Continuity using a Digital Health Wallet," in *2019 IEEE International Conference on Healthcare Informatics (ICHI)*, Jun. 2019, pp. 1–7. doi: 10.1109/ICHI.2019.8904625.

[16] C. Jack, Y. Singh, and M. Mars, "Pitfalls in computer housekeeping by doctors and nurses in KwaZulu-Natal: no malicious intent," *BMC Med Ethics*, vol. 14 Suppl 1, p. S8, 2013, doi: 10.1186/1472-6939-14-S1-S8.

[17] S. R. Tissera and S. N. Silva, "Attitude Towards Health Information Privacy and Electronic Health Records Among Urban Sri Lankan Adults," *Nursing Informatics 2016*, pp. 1003–1004, 2016, doi: 10.3233/978-1-61499-658-3-1003.

[18] M. Forster *et al.*, “Electronic medical record systems, data quality and loss to follow-up: survey of antiretroviral therapy programmes in resource-limited settings,” *Bull World Health Organ*, vol. 86, no. 12, pp. 939–947, Dec. 2008, doi: 10.2471/BLT.07.049908.

[19] M. B. Gesicho, T. D. Moon, E. Heitman, and M. C. Were, “Ethical Issues in Implementing National-Level Health Data Warehouses in Developing Countries,” *MEDINFO 2017: Precision Healthcare through Informatics*, pp. 718–722, 2017, doi: 10.3233/978-1-61499-830-3-718.

[20] M. Namara, D. Wilkinson, B. M. Lowens, B. P. Knijnenburg, R. Orji, and R. L. Sekou, “Cross-cultural perspectives on eHealth privacy in Africa,” in *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, New York, NY, USA, Dec. 2018, pp. 1–11. doi: 10.1145/3283458.3283472.

[21] C. A. T. Antonio, I. D. Patdu, and A. B. Marcelo, “Health Information Privacy in the Philippines: Trends and Challenges in Policy and Practice,” *Acta Medica Philippina*, vol. 50, no. 4, Art. no. 4, Dec. 2016, doi: 10.47895/amp.v50i4.760.

[22] N. Gerson and F. B. Shava, “A Review of Security System Assessment Tools - ProQuest.” https://www.proquest.com/docview/2455896172/fulltextPDF/237C474A4684F42PQ/1 (accessed Jan. 17, 2022).

[23] A. Zainudin, A. Sudarsono, and B. M. Prakoso, “An implementation of secure medical data delivery for rural areas through delay tolerant network,” in *2016 International Electronics Symposium (IES)*, Sep. 2016, pp. 414–419. doi: 10.1109/ELECSYM.2016.7861042.

[24] R. Pankomera and D. van Greunen, “Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries,” in *2017 IST-Africa Week Conference (IST-Africa)*, May 2017, pp. 1–11. doi: 10.23919/ISTAFRICA.2017.8102384.

[25] A. Koivu, N. Mavengere, Mikko. J. Ruohonen, L. Hederman, and J. Grimson, “Exploring the Information and ICT Skills of Health Professionals in Low- and Middle-Income Countries,” in *Stakeholders and Information Technology in Education*, Cham, 2016, pp. 152–162. doi: 10.1007/978-3-319-54687-2_15.

[26] N. Khac Hai, S. Lawpoolsri, P. Jittamala, P. Thi Thu Huong, and J. Kaewkungwal, “Practices in security and confidentiality of HIV/AIDS patients’ information: A national survey among staff at HIV outpatient clinics in Vietnam,” *PLoS One*, vol. 12, no. 11, p. e0188160, 2017, doi: 10.1371/journal.pone.0188160.

[27] S. I. Khan and A. S. Md. L. Hoque, “Health data integration with Secured Record Linkage: A practical solution for Bangladesh and other developing countries,” in *2017 International Conference on Networking, Systems and Security (NSysS)*, Jan. 2017, pp. 156–161. doi: 10.1109/NSysS.2017.7885818.

[28] L. K. Roland, T. Sanner, J. I. Sæbø, and E. Monteiro, “P for Platform. Architectures of large-scale participatory design,” *Scandinavian Journal of Information Systems*, vol. 29, no. 2, Dec. 2017, [Online]. Available: http://aisel.aisnet.org/sjis/vol29/iss2/1