Security Considerations

The purpose of these guidelines is to assist DHIS2 implementers and system owners to take reasonable and appropriate measures to identify and manage the risks associated with running the DHIS2 system. The hope is that it will be particularly useful for system owners who might otherwise struggle to define and impose technical constraints on implementers.

DHIS2 is implemented by many different types of organisations at different scales and for different purposes. The primary system owner in mind here is a government health department or ministry, but many of the guiding principles should also be applicable to NGOs and private sector organisations.

The DHIS2, as a web-based system, reaches its maximum potential when it is accessible over the open internet by health workers using whatever devices might be available to them and through whatever internet connectivity providers are available (eg. 4G mobile phone systems). We have seen how when using such an open model it is possible to roll-out national systems across countries and programs over a matter of months rather than years.

Unfortunately, over the same period we have also seen a rising threat to internet based systems from both criminal and state actors. Attacks have become more frequent and more sophisticated. The need to be more rigorous and street smart is much more apparent now than when the first web-based versions of DHIS2 were being rolled out 10 years ago.

Comprehensive security practice is concerned with CONFIDENTIALITY, INTEGRITY and AVAILABILITY of data.

The DHIS2 has been remarkably successful in being adapted and sustained in many countries as the national health information system, typically as the aggregate routine reporting system. Whereas the confidentiality of routine data is arguably a not very important concern, the **integrity** and **availability** of the data becomes more important as the system becomes more institutionalised over time. The impact of data loss in particular becomes more serious.

The nature of the data collected in DHIS2 has also become more sensitive. Increasingly a DHIS2 database will contain a significant amount of personal identifiable info personal data. This can be patient demographic data, but also health worker (email, telephone, address, messages) captured as User information. Adequa need to be in place to protect the **confidentiality** of such data and the privac persons involved.

Ask AI

Context of use

Legal and regulatory context

There are no universal set of laws, practices and principles which apply everywhere. The dominant recent legislation regarding privacy in countries of the European Union, for example, is the GDPR (General Data Protection Regulation, in force from May 2018). This legislation introduces a set of guiding principles and accompanying terminology which differs in scope, justificatory narrative and intent from the U.S. HIPAA (Health Insurance Portability and Accountability Act), which is the primary legislation governing health data in that country.

These are both relatively new and complex pieces of legislation. Countries where DHIS2 is being used are generally not subject to either HIPAA or GDPR compliance, but many have developed or are developing national legislation in the area - for example the Protection Of Personal Information Act 2013 in South Africa, and the Personal Data Protection Bill, 2019 (draft) in India. Implementers and system owners should make the effort to familiarize themselves fully with the legislation in their jurisdiction of use. The UNCTAD maintains a page with up-to-date privacy legislation for each country across the world.

For public sector systems (perhaps the majority of cases of DHIS2 usage) there might be additional policies and standard operating procedures related to the security of systems and data which also carry the weight of law.

In most cases, pleading ignorance of the law is not a defense.

Operating outside the context of any relevant legislation and policy is difficult, but in contexts where the existing regulatory environment is outdated or not adequate, appropriate controls need to be established by consensus within the scope of the DHIS2 system itself.

Human and organisational context

It is a characteristic of "advanced" capitalist economies that there is a highly developed division of labor. We see this clearly in the IT sector in Europe and the US where there are very clear distinctions between system administrators, programmers, network engineers, information end users as well as highly developed IT management structures, roles and practices, particularly in large organisations.

It is foolish to expect to find the same sort of structures and roles in all countries, particularly where the DHIS2 might be the first, or at least the most important, national system in a national health ministry. Implementing a complex web-based system like DHIS2 without a relatively modern base of management and skilled labor brings with it unique risks and challenges. Developing the appropriate organisational forms to manage the risk and allow the system to flourish and sustain is at least as important as any technical considerations.

The challenge is exacerbated where there is a complex mix of government departments, partner organisations and donors, all of whom might not share the same perspectives and priorities regarding security and privacy.

Measures

Organisational measures

In the face of the organisational challenges that system owners might face, it becomes more important, rather than less so, for the system owners to develop an appropriate plan to manage the security of the system. What follows is a small collection of practical advice.

Having a security management plan is the first step to asserting any sort of ownership over the system. Where the ministry of health is a passive user of the system developed and managed by partner organisations they are not asserting ownership.

Security is a management issue. You cannot delegate it to the lowliest, most technical person in the organisation (common!) nor can you outsource it to a technical partner (also common). You will almost certainly lean on these resources but the motivation should be driven from management.

In an ideal world there might be a chief security officer (CSO) with professional background in some of the many security and governance frameworks (TOGAF, ITIL, ISO27000x etc). It is much more likely that this will not be the case and people need to make a more agile plan with what resources they have. Improvisation can be key. Having a bad, or at least poorly developed, plan for managing security is much better than having no plan at all. A weak plan can be improved and further developed.

We recommend that organisations adopt some of the methodology of the likes of ISO27002 (Information Security Management) without necessarily embarking on a route towards ISO27000 compliance. At a very minimum this would imply that:

> 1. You have a high level statement summarising your organisation\'s security posture. A one pager which should highlight principles and intentions and signal the commitment of senior management to the process.
>
> 2. You have clearly identified someone (reasonably senior) in the team who will take on the role of developing, maintaining and implementing the security plan. We can call it the security manager.
>
> 3. The security manager is committed to a process of identifying, documenting and mitigating risks. This is an ongoing process which generally

> revolves around the maintenance of a risk register which is subject to regular review.
>
> 4. There is a process in place (including time and budget) for regular internal and/or external audit of the DHIS2 deployment, configuration and metadata, including the organization\'s security plan.
>
> 5. There is a Data Sharing Agreement among the parties that define what data is handled, for what purpose and how, setting clear limits and boundaries to avoid the breach of patient data, as well as protecting the integrity and confidentiality of data.
>
> 6. Data and technical ownership is established for the DHIS2 system.

Many of the other artifacts and processes envisaged in a framework like ISO 27000 could emerge naturally from this cycle. For example, if there is no disaster recovery plan or backup strategy that would be highlighted as a major risk in the register. Assembling and maintaining a register like this allows the team to identify and prioritize tasks which need to be done and assess progress towards achieving a better posture.

As a minimum, the following documents should be created as first step of any security program: - Asset inventory - Risk assessment/Risk register document - Backup policy - Disaster Recovery policy - Incident Response plan - Identity and Access Management plan

To help implementers to kick-start their security programs, we have developed a set of templates anyone can use and adapt to their own needs, called Security Starter Kit.

System Configuration measures

There are also a number of measures which can be taken to improve security at the level of DHIS2 configuration, for example related to ensuring appropriate system and data access. A proposed high priority (top 10) list of system configuration measures are included here:

> **System administration**
>
> 1. There is a limited number (less than 5) of people with superuser (full) access to the system. *Can easily be assessed through the API:* `/api/users.json?filter=userCredentials.userRoles.authorities:!in:[_ALL_]&filter=userCredentials.userRoles.authorities:in:\[ALL]`
>
> 2. System administrators are only given authority to perform functions that are relevant for their system administration roles. *For example, an administrator responsible for managing charts and dashboards does not need rights to edit organisation units.*

3. The default DHIS2 user account (username "admin") is deleted or disabled. *The admin account should only be used when DHIS2 is started for the first time, to set up a personal superuser. It should then be disabled and/or deleted. The status of the admin account can be verified using the API:* `/api/users.json?filter=userCredentials.username:eq:admin&fields=name,userCredentials\[name,disabled\]`

User management

4. There are procedures in place to disable or remove user accounts of people who leave the service. *There should be clear procedures in place to disable/delete user accounts of people who leave the (health) service. Some indication of this can be derived from the API, by looking at user accounts that are not disabled and have not logged in to the system e.g. in the current year:* `/api/users.json?filter=userCredentials.disabled:eq:false&filter=userCredentials.lastLogin:lt:2021`

5. All user accounts in the system are personal, i.e. not shared by several individuals. *User accounts should not be shared by several individuals, as this makes auditing impossible. This is especially critical if Tracker is used for individual-level data.*

6. There are clearly defined user roles and user groups, with guidance on what roles and groups should be used according to the positions within the (health) service of the user.

7. If self-registration of users is enabled, the user role given to these users should be very limited, e.g. to only viewing public dashboards.

8. Disabling accounts might be a good way to limit the access to some users that have been forgotten in the system. DHIS2 provides a scheduled task to automate this. However, be aware that this might have consequences (leading to data loss) while using Android devices as explained in the official documentation.

Tracker

9. Access to Tracker data is limited to users with a legitimate need for the edit/view the data through appropriate use of sharing and user groups. No tracker programmes intended for use to record information on individual persons are configured with public access. *Tracker data is typically linked to individuals, and should therefore be restricted to users with a legitimate use of*

> *this data. While it might be a good idea that aggregate data is accessible to all users, this is not the case with Tracker data.*
>
> 10. Tracker programmes are configured so that users can only search for and access data for people they have a legitimate reason for viewing. *For example, a user working within one health facility should not be assigned to a district. The "tracked entity search organisation unit" should not be set broader than what is practically necessary, if used.*

> **Android**
>
> Using mobile devices (Android) in DHIS2 is becoming more common due to their offline and last-mile capabilities. However it comes with additional requirements to look at from the security perspective as the exposure increases passing from one server containing information to multiple devices that might contain sensitive information.
>
> If sensitive information is being stored in the devices, concern should be raised via training and/or documentation. And system administrators might want to enable different measures that could help reduce the risks for which the Android Settings Web App (ASWA) is available.
>
> The ASWA allows system administrators (among other things) to:
>
> - Force the DHIS2 local database encryption on the devices to prevent the leak of data by malicious actors in case of having access to a device.
> - Allowing/disallowing the screenshot capabilities reduces (but not limits) the risk of leaking confidential information.
>
> A section of the official documentation (DHIS2 Android App) describes all these in detail.
>
> On top of this the Android application might be individually configured to ask for a PIN code as another layer of security to the username/password pair.
>
> In implementations where risk of devices being lost/stolen exists, system administrators might want to add another layer of security brought by tools like Mobile Device Management which could allow remote wiping, location, etc. A specific guide is available in the official documentation: managing mobile devices.

Technical measures

There are many ways that a DHIS2 system can be provisioned, including on different physical environments (on-premises, co-location, private cloud, public cloud) using different operating systems, using containers, load-sharing, replication etc. There are different detailed sets of security controls which can and should be applied depending on these design choices which are made in provisioning.

In the most general sense we can that there should be:

- a documented set of technical controls mandated
- an audit process against those controls

Organisations such as the Centre for Internet Security (https://cisecurity.org) maintain detailed benchmarks for software products which can be used to compile a set of controls for your implementation. In most cases you won\'t apply all of them but will select the ones which are most relevant. From the list available at https://www.cisecurity.org/cis-benchmarks/ you should download and study the benchmarks for Apache Tomcat, Postgresql, nginx (or Apache2). In addition, depending on your technology choices you might find benchmarks for Ubuntu linux, lxd, Docker or Microsoft Windows relevant to your implementation.

A proposed high priority (top 10) list of technical measures that should be in place:

> 1. Operating system is a LTS (long term service edition).
>
> 2. There is an automatic process for applying OS security patches.
>
> 3. Host and/or network based firewall configured exposing only the necessary services to the network.
>
> 4. Administrative access to DHIS2 server is via SSH according to agreed good practices - keys authentication only, no root access, explicit users allowlist, low number of max authentication attempts.
>
> 5. DHIS2 version is not more than 3 versions behind the latest release. Process exists to apply patch releases regularly.
>
> 6. Automated backup system is in place and regularly tested, including offsite.
>
> 7. Postgres and system users follow the least privilege principle: allow only minimal permissions and access.
>
> 8. DHIS2 is exposed via a web-proxy server configured with TLS/SSL (must score a minimum of A in ssllabs).
>
> 9. Database data is in a separate location (data partition, hard disk, cloud storage, etc) allowing encryption at rest.
>
> 10. Monitoring and alerting systems are in place for system metrics (CPU, memory, disk, network, database, web proxy at minimum) with adequate

> authentication mechanisms (e.g. 2FA, SSO, strong password requirements) and role based access.

2024-04-22

← Previous: Setting Up a New Database

Next: Server Hosting →