September 2015

# Overview of Security Considerations for eHealth

Security is of fundamental importance when dealing with health information, especially data that contains identifiable patient information, which may be particularly sensitive.

The South African National eHealth Strategy explicitly states the need for regulations on privacy, confidentiality, and security and the need to protect information and patient privacy at all times. It is therefore important that when electronic patient records are rolled out, thorough security is implemented. This requires assigning a dedicated specialised team to information security.

The Health Normative Standards Framework for Interoperability in eHealth v2[1] (HNSF) (2014) identified 42 health information systems (HIS) working in the health sector in South Africa. Of those, 22 HIS used a username and password to access patient information, 14 utilised encryption for confidentiality, and only four anonymised patient data. This highlights the fact that security has not always been a central consideration for projects implementing eHealth.

The HNSF explicitly mentions standards associated with privilege and access control, which are key principles of security. However, there are a number of other elements to consider.

The technical committee of the **International Organisation for Standardisation (ISO),** which manages standards for eHealth, is called TC215. This committee maintains the **privilege management and access control standards** (ISO 22600[2]) mentioned by the HNSF. However, the ISO also manages standards covering information security management (ISO 27799:2008 and ISO/IEC 27002[3]). These are standards that should govern all sensitive eHealth systems that process patient information.

This ISO/IEC 27002 standard can be mapped to the key concepts promoted by the **International Information Systems Security Certification Consortium** (ISC)[2]. This consortium has produced a vendor-neutral certification called **Certified Information Systems Security Professional (CISSP)**,[4] which has become the primary qualification for information security professionals. CISSP has eight domains covering different areas of security that all need to be addressed by eHealth and information and communications technology (ICT) managers. The domains present an accessible way to understand the implementation of security in eHealth. The eight domains are:

a. Security and risk management;
b. Asset security;
c. Security engineering;
d. Communications and network security;
e. Identity and access management;
f. Security assessment and testing;
g. Security operations; and
h. Software development security.

These domains are detailed in the sections that follow.

## Security and Risk Management

*(Security, risk, compliance, law, regulations, and business continuity)*

The **Security and Risk Management** domain includes guiding principles for the safe utilisation, flow, and storage of information. The main guiding principles are confidentiality, integrity, and availability.

With **confidentiality**, the primary aim is to ensure that information should not be accessed by people who are not authorised to view it. This means that confidentiality levels must be assigned to all data and measures must be taken to prevent unauthorised access.

**Integrity** means that the data must maintain consistency, accuracy, and trustworthiness over the entire life cycle. This means that all transfers and changes to data must

[1] CSIR and NDoH. (2014). *Normative Standards Framework for Interoperability in eHealth v2.* Pretoria: Council for Scientific and Industrial Research and South Africa National department of Health in collaboration with Nelson Mandela Metropolitan University.

[2] International Organisation for Standardisation. (2009). *ISO/TS 22600-3:2009 – Privilege Management and Access Control – Part 3: Implementations,* Retrieved 14 March 2012, from http://alturl.com/sjyau.

[3] South African National Standard SANS 27002:2014 Edition 2 ISO/IEC 27002:2013 Edition 2 Information technology – Security techniques – Code of practice for information security controls. Retrieved 8th September 2015 from http://www.store.sabs.co.za/sans-27002-ed-2-00-1.

[4] (ISC) website. 2015. *CISSP® – Certified Information Systems Security Professional.* Retrieved 02 September 2015 from: https://www.isc2.org/cissp/default.aspx.

be considered and security measures taken to maintain integrity at all points.

**Availability** means that the data that should be available for authorised users should also be available at all times. This requires good policies and standard operating procedures for backups and disaster recovery, as well as sufficient server capacity and network bandwidth.

The security and risk management domain also deals with legal and regulatory compliance, and ensuring that security policies, standards, procedures, and guidelines are in place.

In South Africa, the major legislation that impacts eHealth is:

- The National Health Act 61 of 2003;
- Protection of Personal Information Act 4 of 2013 (POPI Act);
- The Electronic Communications and Transactions Act 25 of 2002; and
- The Electronic Communications Security Act 68 of 2002.

A key element of risk management is exercising due care. Due care describes stakeholder responsibility and duty to protect computer and information assets. Due care is the minimum security best practice standard and is demonstrated when stakeholders take the necessary steps to help protect assets, resources, and information.

## Asset Security

*(Protecting security of assets)*

The **Asset Security** domain considers data assets. It covers information and asset **classification**, data and system ownership, and privacy protection. It also deals with appropriate retention, data security controls, and handling requirements such as markings.

All data assets need to be classified according to a classification scheme. Typical classification schemes look at the value of the information/data as well as the age, or useful life, of the data. Other classifications may be required for regulatory purposes. For example, in the USA, medical records are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, which addresses the saving, accessing, and sharing of medical and personal information, and the HIPAA Security Rule, which outlines national security standards to protect health data created, received, maintained, or transmitted electronically.[5]

The classification scheme should also specify how data should be handled, labelled, and stored. Additionally, it should detail how and when data should be destroyed.

All data should have a defined owner responsible for that specific data. It should be noted that the owner may change according to where the data is stored, and the issue of ownership while the data is being transferred must also be considered. All systems should also have a specified owner who will have responsibility for the system.

Data asset security controls need to be implemented by the data and system owners to ensure adherence to specified requirements of classified data.

## Security Engineering

*(Engineering and management of security)*

The **Security Engineering** domain considers how security is practically implemented. There are various security models and rules that are used by security engineers, including:

- The Simple Security Rule, which addresses confidentiality by preventing access to data that has a higher security level than a user is authorised to view.
- The Star Property Rule, which prevents a user from changing data at a lower classification level.
- The Discretionary Security Property Rule, which uses a matrix to specify who has permission to do what on specific data sets.

The **vulnerabilities** of systems, designs, and solution elements need to be assessed and mitigated. Particular consideration should be given to web-based systems, embedded, and mobile systems, which may have additional vulnerabilities not present in traditional computer networks.

**Cryptography** is an important element of security engineering. Encryption is used to protect the confidentiality of data. There are various types of encryption methods that provide different security levels.

**Physical security** is another element that needs to be considered in depth. Site and facility design should adhere to secure design principles. A layered defence model should be used incorporating multiple security methods. The physical security plan should aim to deter crime, detect and delay intruders, assess the situation, and respond appropriately to threats. There should also be disaster management plans to deal with fire, power outages, and environmental issues.

[5] Online Tech; retrieved from http://www.onlinetech.com/resources/references/what-is-hipaa-compliance.

## Communications and Network Security

*(Designing and protecting network security)*

Communications and networks are fundamental elements of many health information systems. **Secure network architecture design** needs to be implemented both on internet- and intranet-based networks. This includes hardware, such as modems and routers, as well as security software, and data transport protocols.

Secure communication channels are important, and there is a need to consider both data and voice channels over regular and mobile telecommunications networks. It may be appropriate to establish Virtual Private Networks (VPN) and Virtual Local Area Networks (VLAN). Remote access and network collaboration tools can present a number of security challenges that need to be mitigated.

Networks may be subject to attack in a variety of ways. For example, *spoofing* occurs when someone masquerades as another person in order to gain unauthorised access to data. A *denial of service* attack will aim to overload a system to make it fail. All types of network attacks should be assessed for risk, and measures taken to prevent and respond to them.

## Identity and Access Management

*(Controlling access and managing identity)*

Identification and authentication of people and devices is necessary to maintain secure systems. When access is granted, it is called **provisioning** and when access is taken away, it is called **deprovisioning**. Things that can be provisioned include hardware, software licenses, and system accounts.

All acts of provisioning and deprovisioning need to be documented, and this should be linked with human resource and procurement processes. For example, when a new employee is hired, they will need to be provisioned with rights according to their role. If their role or access levels need to change, then specific system rights may need to be provisioned or deprovisioned. When their employment ends, their rights should be deprovisioned.

It is good practice to strive for a **single sign-on (SSO)** approach within an enterprise where a person has only one account. This minimises duplication of identity and mitigates many risks. To achieve this, it is necessary to document all potential points of access and integration and specify appropriate rules that are linked to business processes. Whenever new systems are introduced, or changes are made to existing systems, there should be a review of access control affected by the changes. Likewise, the impact of business process changes must be reviewed.

To check the integrity of access management, there should be **access and privilege management audits**. In addition, all events related to access control and provisioning/deprovisioning should be logged. This will allow authorised staff to identify who has accessed what system, at what time, and whether there have been any attempts to access unauthorised data.

## Security Assessment and Testing

*(Designing, performing, and analysing security testing)*

Security measures in place should be tested and assessed in order to maintain confidence in the level of security provided. To do this effectively, all security measures should be documented and a plan developed with respect to how they can be tested.

Common assessments may include an **analysis of vulnerabilities** of any part of a system. This analysis can be used to plan for penetration testing. Other tests may include simulating attacks, or disaster events, that could compromise confidentiality, integrity, or availability. For example, a **back-up process** may be in place, but **the disaster recovery process** to get data from the back-up needs to be tested on a regular basis.

Some vulnerabilities may be tested using automated tools to provide regular checks. However, it is important to note that documentation of the findings of security tests is essential. Documenting how people, systems, and processes reacted during the test is also vital. With adequate documentation, the results of the tests can be presented to managers so that they are aware of security issues found.

**Outsourced systems** and/or third-party providers can present a security risk. Assessments of security vulnerabilities with respect to outsourced systems should undergo the same level of rigour as those of internal systems.

## Security Operations

*(Foundational concepts, investigations, incident management, and disaster recovery)*

**Security Operations** are concerned with managing the threats that exist in a live operating environment. They cover the people, data, hardware, and media.

There are many administrative risks associated with maintaining security operations. It is good practice to ensure that **background checks** are conducted, **non-disclosure agreements** are signed, and that staff are only given access to what they actually need in order to do their jobs and no more. Where possible, there should be **separation of duties** (meaning more than one person is required to do a specific critical task) and **rotation of**

**duties** (meaning that the task is not always done by the same person). This will mitigate the risk of security staff abusing the system. However, it should be noted that two or more people could potentially collude, so checks on security staff need continual vigilance.

**Sensitive data** must be identified and marked as sensitive. It is good practice to always encrypt sensitive data as this will decrease the risk of compromising confidentiality. There should also be a process to effectively dispose of/destroy data after its retention period has expired.

**Continuity of operation** must be ensured and therefore efforts should be made to ensure that the system is resilient against different risks. An example of this is **system redundancy,** which means that if one part of a system fails, it automatically switches to using another part that has been made available for exactly that eventuality. The use of a redundant array of inexpensive disks (RAID) helps to address the risk of hard disk drive failures.

Security operations also deal with incident response. This details how an organisation should identify, react, and recover from security incidents. A security incident response team will generally follow the process below.

1. **Detection** of potential security issues/events;
2. **Containment** to ensure damage is minimised;
3. **Eradication** to remove the threat from the system;
4. Cautious **recovery** of systems to operational status; and
5. **Reporting** to management where the incident occurred, how it was resolved, and actions required.

## Software Development Security

*(Understanding, applying, and enforcing software security)*

Software that does not effectively incorporate security may be easy to attack or exploit. Therefore, attention should be paid to security throughout the software development life cycle and all stakeholders should include security considerations in their processes. Documentation of security measures is important, as this will help to assess the vulnerability of the software.

A secure software development methodology will consider role-based access rights from the outset for all of the software's functionality. It will consider whether personal identifiable information will be held and how it should be encrypted and transported. Addressing security early in the software development life cycle will simplify the process and resolve potential issues before they manifest.

Whichever software development methodology is used, the source code should be audited to ensure that there are no security design flaws. Using coding standards and source code control is also a good practice that will facilitate auditing code and removing flawed code. Before software is operationalised, it should be assessed and tested. The same is true when software is patched or upgraded.

## Conclusion

There are many security domains that need to be considered when deploying eHealth systems. Personally identifiable health data is particularly sensitive and its security must be ensured. Because of this, security professionals should be involved at all stages of the design, development, procurement, and implementation of patient-based health information systems. Significant attention must be paid to access controls and assessing risk. When risks and vulnerabilities are found, there should be a plan in place to mitigate that risk.

This technical brief has been supported by the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation – Strategic Information for South Africa associate award AID-674-LA-13-00005. Views expressed are not necessarily those of USAID or the United States government. FS-15-155