

MomConnect

Security Findings and Recommendations

May 2017

TR-17-231

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

momconnect

PEPFAR

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation SIFSA

MomConnect
Security Findings and Recommendations

Annah Ngaruro, MS

May 2017

Photo credit: A mother uses a mobile phone outside a health clinic in Tanzania.
© 2015 Chelsea Solmo, Courtesy of Photoshare

MEASURE Evaluation–Strategic Information for South Africa (MEval-SIFSA) Project
138 Muckleneuk Street
Nieuw Muckleneuk, Pretoria
South Africa
Tel: + 27 12 346 7490
http://www.measureevaluation.org/sifsa

This research has been supported by the President's Emergency Plan for AIDS Relief (PEPFAR) through 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. MEASURE Evaluation–SIFSA is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of PEPFAR, USAID, or the United States government. TR-17-231

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

momconnect

PEPFAR

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation SIFSA

ACKNOWLEDGMENTS

The author would like to thank Praekelt.org for their cooperation, and especially for making their engineering, networking, security and project management staff available to facilitate the performance of this assessment. Many thanks to the MomConnect Task Team for their review of the report and provision of useful feedback.

This assessment would not have been possible without support from the National Department of Health, namely Dr. Peter Barron and Dr. Antonio Fernandes, who oversee the MomConnect program. In addition, the author greatly appreciates the support of Joy Kamunyori of the MEASURE Evaluation Strategic Information for South Africa (MEval-SIFSA) project who facilitated, organised and provided guidance for the successful completion of the assessment, as well as Derek Kunaka, MEval-SIFSA's then Chief of Party for lending his support to this assessment activity. We would also like to acknowledge MEASURE Evaluation's knowledge management team for editorial, design, and production assistance.

Lastly, this assessment was supported by the President's Emergency Plan for AIDS Relief (PEPFAR) through the United States Agency for International Development (USAID).

CONTENTS

Acknowledgments ..... **iii**

Abbreviations ..... **vi**

Executive Summary ..... **vii**

Introduction **1**

Assessment Purpose **1**

Assessment Process **2**

Assessment Scope **2**

Findings **4**

Criticality and Sensitivity Assessment 4

Data and System Assessment 4

Vulnerability Testing and Scan 9

Recommendations **11**

References **18**

Appendix. Stakeholder Comments **19**

FIGURES

Figure 1. MomConnect system technical components 3

TABLES

Table 1. Criticality and sensitivity assessment findings 4

Table 2. Data and system assessment findings 5

Table 3. MomConnect vulnerability scan results 10

Table 4. MomConnect security recommendations 12

ABBREVIATIONS

API	application program interface
HTTPS	Hypertext Transfer Protocol Secure
IT	information technology
MEval-SIFSA	MEASURE Evaluation—Strategic Information for South Africa
NDOH	National Department of Health
OpenHIE	Open Health Information Exchange
PHI	protected health information
PII	personally identifiable information
POPI	Protection of Personal Information
SMS	Short Message Service
SOP	standard operating procedure
SSH	Secure Shell
SSL	Secure Sockets Layer
USAID	U.S. Agency for International Development
USSD	Unstructured Supplementary Service Data

EXECUTIVE SUMMARY

The U.S. Agency for International Development-funded MEASURE Evaluation—Strategic Information for South Africa (MEval-SIFSA) project and other partners have provided support to the South African National Department of Health in the implementation and rollout of the MomConnect mobile health intervention since its launch in August 2014. As part of this support, in 2016 MEval-SIFSA conducted a system and data assessment to assess the MomConnect system's compliance with the existing legal requirements for data privacy and security best practices, identify any vulnerabilities, and assist with identifying and addressing vulnerabilities. This security assessment was conducted by a Certified Information Systems Security Professional using a step-by-step process that included extensive questionnaires, in-person assessment and examination, and the use of automated security testing tools.

The MomConnect system was determined to be a medium impact system based on the three criticality areas assessed: confidentiality, integrity, and availability. Overall, the assessment found gaps in 11 of the 13 assessment categories, resulting in 18 high, 9 moderate, and 3 low priority recommendations to address and mitigate the gaps identified. This report discusses the assessment purpose, process, and results, and it presents the implementation recommendations identified. These recommendations, regardless of priority level, have been categorised as short-, medium-, and long-term action items to help guide the implementation process.

INTRODUCTION

South Africa has high infant mortality rates (29 per 1,000 live births) and maternal mortality rates (140 per 100,000 births). To reduce these rates, the South Africa National Department of Health (NDOH) is leading the charge to tackle the health challenge from all angles, including educating and providing quality healthcare to infants and mothers. MomConnect is one component of these efforts.

An NDOH initiative, MomConnect was launched on 21 August 2014 by the Minister of Health, Aaron Motsoaledi. The initiative is implemented on a national scale, using mobile phone technologies, Short Message Service (SMS), and Unstructured Supplementary Service Data (USSD). MomConnect is offered free-of-charge to mothers. This comprehensive system registers pregnant women, delivers targeted stage-based health information to pregnant and postpartum women, enables women to reach out with pressing questions, and establishes an important feedback loop to improve services at healthcare facilities.

ASSESSMENT PURPOSE

MomConnect recently celebrated its second year anniversary. Since its inception, the system has been collecting sensitive information from women. As of November 2016, more than one million women have registered on MomConnect. In the process of registering, their phone numbers, due dates, and South African ID or passport numbers are collected and stored in the system. This information all qualifies as personally identifiable information (PII) and protected health information (PHI).

The South African Protection of Personal Information (POPI) Act of 2013 is very specific regarding personally identifiable information and lays out the legal framework for:

- Protection of personal information processed by public and private bodies
- Adherence to certain conditions to establish minimum requirements for processing of personal information
- Regulations for the flow of personal information

The National Health Act (61 of 2003) also provides the current legal framework to protect the confidentiality of patients' health records.

Conducting a security assessment allows for the assessment of risks, identification of potential security flaws, and recommendations for remediation. According to the joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission, "In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated. Risks associated with an organization's information assets need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization" (International Organization for Standardization, 2016).

A security assessment can be a loss prevention strategy. For example, a security breach of the system could cause loss of confidence in the application because users' personal information would be lost; this

in turn could lead to loss of stakeholder credibility and the effectiveness of the initiative. Compromising PII and PHI can result in discrimination of individuals due to release of personal information, such as stigma regarding HIV status especially in the case of underage girls. Conducting a security assessment shows that the NDOH is aware of the current global environment, in which data security threats are common, and is proactively planning by creating a highly focused and specific information security plan that is targeted and helps stay ahead of the curve.

Because MomConnect is a prominent NDOH mobile health initiative, this risk assessment is expected to lead to increased awareness in the department that information security risks and threats need to be considered during the implementation of digital health projects. This assessment will be the basis for the creation of a strong and responsible culture of information security in the NDOH, and it will lay the foundation for effective and strong data governance. The MomConnect system will serve as a model to promote best practices for how to protect sensitive user information.

ASSESSMENT PROCESS

A Certified Information Systems Security Professional conducted the assessment using a step-by-step process that included extensive questionnaires, in-person assessment and examination, and the use of automated security testing tools. The five steps of the process are as follows:

1. A preliminary requirements-gathering task determined the scope of the assessment and ensured that it covered the appropriate data, systems, and functions in the purview of the MEASURE Evaluation—Strategic Information for South Africa (MEval-SIFSA) project. This included all system elements whose development was funded by the U.S. Agency for International Development (USAID) through MEval-SIFSA.
2. A sensitivity and criticality determination of the system and data was based on three protection categories: confidentiality, integrity (including authentication, nonrepudiation, and accountability), and availability.
3. A confidentiality assessment used a privacy impact assessment questionnaire to determine sensitivity and criticality of the data collected, stored, and transmitted by the system.
4. A system assessment questionnaire assessed the presence and implementation of management, operational, and technical controls.
5. A system vulnerability testing scan was conducted and recommendations on remediation were made based on the results.

The in-person assessments, examinations, and questionnaires were conducted in May and June 2016, and the system vulnerability scanning was conducted in October 2016. The security assessment findings and recommendations in this report come from synthesizing the results from the in-person assessments, examinations, collated questionnaires, and automated security testing tools.

ASSESSMENT SCOPE

The scope of the assessment included all elements of the MomConnect system that were directly funded by USAID through the MEval-SIFSA project. This focus was necessary because attempting to assess system elements funded or supported by all partners would have introduced financial and logistical challenges. Therefore, the system elements included in the assessment scope were as follows:

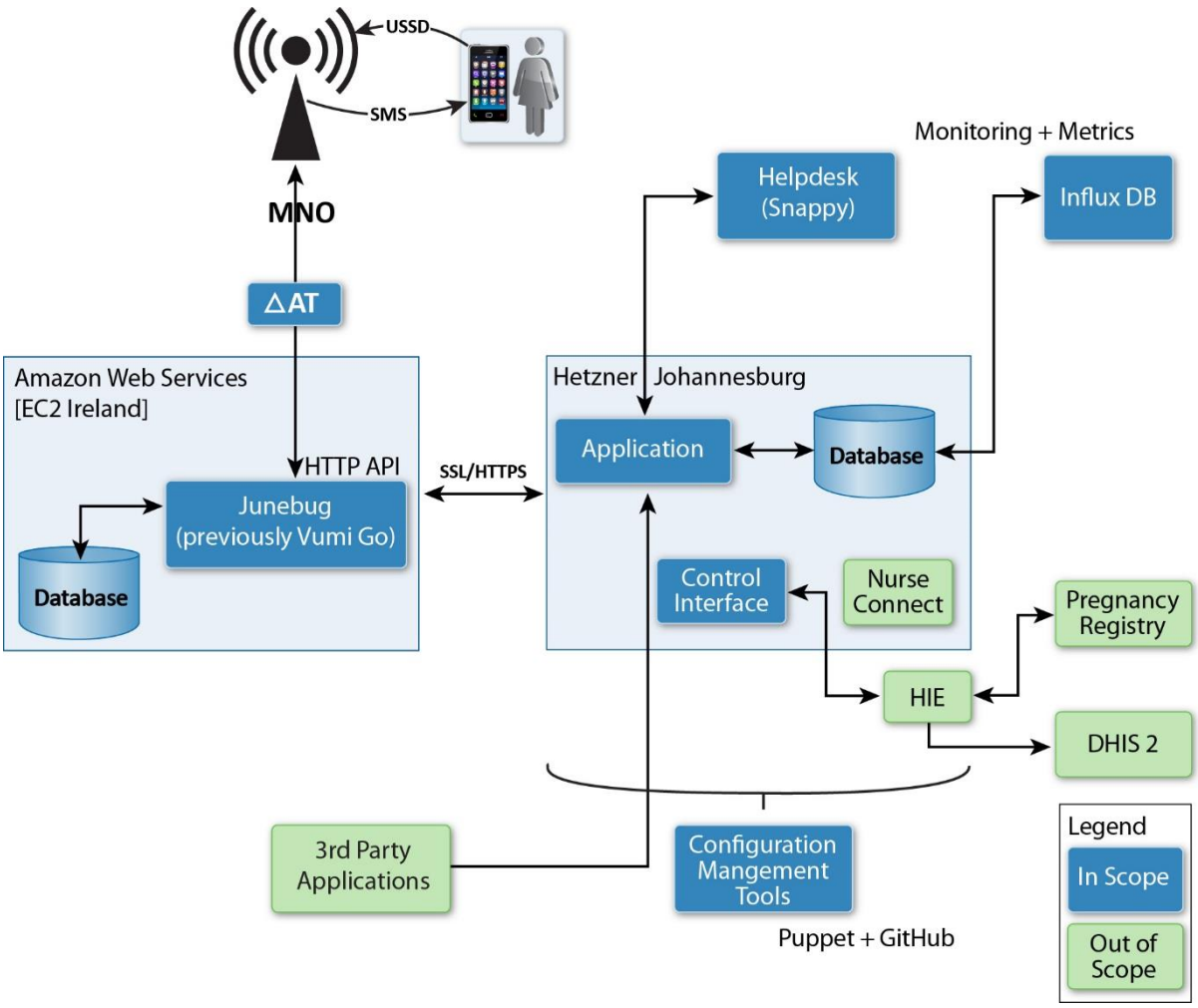
- The MomConnect Seed and Junebug platforms developed and run by Praekelt.org
- All application program interfaces (APIs) and web services sending data to external systems such as the USSD messaging provider, Open Health Information Exchange (OpenHIE) platform, and DHIS 2
- The linkage to be BeSnappy Help Desk system

The following system elements were out of scope for the assessment:

- Configuration management tools (e.g., GitHub and Puppet)
- External systems such as the following:
    - The wireless application service provider that provides the link for USSD sessions and SMS messaging
    - The mobile phone network operators
    - The OpenHIE platform
    - The DHIS 2 instance

Figure 1 describes the technical components of the MomConnect system and shows which elements are in scope and out of scope.

Figure 1. MomConnect system technical components



FINDINGS

Criticality and Sensitivity Assessment

The goal of performing a criticality and sensitivity assessment and determination is to assist an organisation in identifying and quantifying the risks to the information and system assets and the level of impact to the system. This information can be used to determine how best to mitigate those risks and effectively preserve the organisation's mission. The preservation of confidentiality, integrity, and availability of data and the system are vital to data and system security (International Organization for Standardization, 2016). Table 1 provides the definitions of each criterion and the associated impact level based on the findings from the assessment.

Table 1. Criticality and sensitivity assessment findings

Criteria	Criticality and sensitivity assessment determination	Overall assessment
Confidentiality: Refers to the system's ability to provide assurance that data and information are not made available or disclosed to unauthorized individuals, entities, or processes	**Medium:** The loss and cost accrued to the stakeholders' interest if the system's confidentiality is compromised would be **serious** disruption, **significant** financial loss, and **substantial** reputational loss, requiring require legal action for correction.	Overall, the MomConnect system should be considered a **medium impact system** based on the assessment of the confidentiality, integrity, and availability criteria because it collects, stores, and transmits sensitive personal and health information. Systems that collect, store, and transmit sensitive personal information are typically assessed at medium impact level at a minimum. The loss and cost accrued to the stakeholders' interest if the system's confidentiality is compromised would be serious disruption, significant financial loss, and substantial reputational loss, requiring legal action for correction.
Integrity: Includes authentication, nonrepudiation, and accountability, and refers to the system's ability to be accurate and complete and provide protection from unauthorized modification.	**Low:** The loss and cost accrued to the stakeholders' interest if the system's integrity is compromised would be **minor** disruption, **minor** financial loss, and **minor** reputational loss, requiring administrative action for correction.	
Availability: Refers to a system's ability to be accessible and usable on demand by an authorized entity	**Low:** The loss and cost accrued to the stakeholders' interest if the system's integrity is compromised would be **minor** disruption, **minor** financial loss, and **minor** reputational loss, requiring administrative action for correction.	

Data and System Assessment

The goal of performing a data and system assessment is to assess the presence and implementation of:

- **Management controls** that focus on the management of the information technology (IT) security system and the management of risk for a system (Swanson, 2001). These controls are typically addressed by all organizational stakeholders.
- **Operational controls** that address security methods focusing on mechanisms primarily implemented and executed by people (Swanson, 2001). These controls are put in place to improve the security of a system.

- **Technical controls** that focus on security controls that the system executes (Swanson, 2001). These controls can provide automated protection against unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Table 2 shows system findings and gaps for each assessment category.

Table 2. Data and system assessment findings

Assessment category	System findings and gaps
IT Governance: IT governance is a subset discipline of corporate governance, focused on IT and its performance and risk management	**Findings:** MomConnect is an NDOH initiative currently funded by USAID. Although the NDOH is the overall data and system owner, as well as the data and system custodian, it has contracted and engaged Praekelt.org to develop and manage some parts of the system and perform data and system custodian functions on its behalf.
	Gaps: Currently the MomConnect system does not have an IT governance structure that would provide security management and oversight of the both the system and the data collected. Therefore, there are no formal policies or clearly defined roles to allow for embedding a strong security management culture that would continuously manage and mitigate data and system security risks. Although the MomConnect system is subject to the POPI Act, it lacks an IT governance structure to drive the implementation and compliance with this legal requirement.
Security Risk Management: Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Risk is the possibility of something adverse happening.	**Findings:** The current system configuration and links to external systems have been well documented, including interfaces with the Wireless Application Service Provider, BeSnappy Help Desk, OpenHIE platform, and DHIS 2. Some scopes of work for subcontractors (e.g., Western Cape Labs) do contain a section on risk.
	Gaps: Currently the MomConnect system does not have a formal documented risk management policy that would allow for security risk to be routinely identified, managed, and mitigated. It also lacks there are comprehensive risk management procedures. The MomConnect system has several interfaces with external systems sending and receiving data from third-party providers. However, the associated security risks have not been analysed and documented, and risk mitigation processes have not been identified and implemented to reduce risks associated with connecting with these external systems. Security risks associated with external systems include unauthorized access to personal information and contamination of existing personal records with the system—both of which would be a violation of the POPI Act.
Review of Security Controls and Incident Response Capability: Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. Computer security incidents, such as system breach, data loss, and unauthorized access for malicious purposes, are an adverse event in a system or network. Such incidents are	**Findings:** A number of system outages have been formally documented in internal incident reports. The system has a template and a three-step process for incidence reporting. In one reported incident, corrective action was taken to mitigate and reduce the likelihood of the same incident occurring again.
	Gaps: The MomConnect system is not subject to routine evaluations of its system and data security controls. Security testing, such as application vulnerability scans, network penetration tests, and security analysis of demilitarized zones, routers, and switches, has not been performed. Although several incident reports have documented system outages, comprehensive security analysis was not conducted to

Assessment category	System findings and gaps
becoming more common and their impact far-reaching.	identify potential security risks and implement security-based remedial actions to the system. In the case of the one reported incident where corrective action was taken, the remedial actions were mostly operational and not specifically related to security. This means that a potential security vulnerability could be overlooked and remain uncorrected.
System Development Life Cycle: Managing security throughout the IT system life cycle—including initiation, development and acquisition, implementation, operation, and system disposal—is a key aspect of managing system security.	**Findings:** The MomConnect system has implemented a robust system development life cycle methodology for the initiation, development and acquisition, implementation, and operation phases of the system. This includes the use of an Agile process methodology for developing new and enhancing existing system features, a change process for documenting and approving changes to the system, and test plans to verify and validate the correct operation and implementation of features. System re-design reviews are also conducted and documented.
	Gaps: Although the MomConnect system has a robust system development life cycle methodology, it does not have a plan for system disposal, which should include describing how sensitive data would be archived or destroyed if the system is decommissioned.
Certification and Accreditation: A process for authorizing access to the system provides a form of assurance of the security of the system.	**Gaps:** The MomConnect system lacks a formal process for certification and accreditation that would provide assurance of the security of the system.
System Security Plan: System security plans provide an overview of the system security requirements and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behaviour of all individuals who access the system.	**Findings:** The MomConnect project team has demonstrated awareness of POPI requirements and are developing scenarios to document and work through various data privacy requirements.
	Gaps: The MomConnect system lacks a system security plan. Security requirements for the development and operation of the system have not been documented. Specifically, there are no plans that map POPI requirements to MomConnect security requirements. A security plan is the considered a minimum requirement for managing security risks on a system. According to the Guide for Developing Security Plans for Federal Information Systems, "the purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behaviour of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system" (Swanson, Hash, & Bowen, 2006).
Personnel Security, Security Awareness, Training, and Education: Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the	**Findings:** The Praekelt.org MomConnect project team has several defined roles for system engineers and administrators and project management staff who implement ad hoc separation of duties in the system. This provides for a level of security so that the ability to access sensitive data and perform various critical functions is limited to a small number of project team members. For each role, documented job descriptions reflect levels of general accountability. The Praekelt.org standard employment contract also includes a confidentiality

Assessment category	System findings and gaps
access and authorities they need to do their jobs. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Training also develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.	agreement. Praekelt.org has personnel hiring and termination procedures, including some procedures to request, issue, and deactivate MomConnect project team accounts. Praekelt.org staff receive information on rules of behaviour and some informal ad hoc security awareness training.
	Gaps: Praekelt.org does not perform reference and qualification checks before hiring MomConnect project staff. In addition, there are no documented procedures routinely implementing least privilege system access and robust separation of duties at different levels for project staff, especially regarding access to sensitive personal information collected by the system. Praekelt.org's MomConnect project staff do not receive any formal training or education on security awareness.
Physical, Environmental, and Server Protection: These measures are taken to protect servers, systems, buildings, and related supporting infrastructures against threats associated with their physical environment.	**Findings:** The MomConnect system is currently hosted on Hetzner Johannesburg and Amazon Web Services cloud, which are third-party cloud computing hosting providers. The servers on which MomConnect is deployed are virtualized shared environments. Aside from staff at Hetzner and Amazon, only two senior members of the system administration team at Praekelt.org have access to critical server infrastructure.
	Gaps: NDOH, USAID, and Praekelt.org do not manage or have control over the system's physical, environmental, and server protections. The MomConnect system is wholly reliant on security provided by Hetzner and Amazon. This may not be appropriate for a system that collects and stores sensitive personal information. MomConnect stakeholders do not have control over contingency planning in the event of a disaster at the physical location housing the Hetzner and Amazon servers, and information on contingency plans is not currently available. It is also unknown whether Hetzner and Amazon have implemented any intrusion detection or intrusion prevention systems, which are standard practice for hosting providers.
Data Confidentiality, Integrity, and Information Media Access Controls: Data confidentiality controls are used to protect data privacy and unauthorized access. Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations regarding quality and integrity. Information media access controls are procedures for storing, handling, and destroying media.	**Findings:** The MomConnect system collects, stores, and transmits personal information for citizen and noncitizen women both under and over the age of 18. As of May 2016, the system had collected, stored, and transmitted personal information for approximately 740,000 women (this number has since grown to more than 1 million women). The system's primary purpose is to provide health-related messages, collect health centre service-level ratings, and record compliments and complaints about service received at health centres. Sensitive personal information collected includes: MSIDSN (i.e., mobile phone number) (mandatory), expected date of delivery (mandatory), South African identity number (optional), passport number for non-South Africans (optional), date of birth (optional), clinic code (mandatory), and other information (i.e., free text information received by the help desk such as "I have had a miscarriage"). The system contains some data integrity and validation controls. Unit testing is conducted to validate data during system development. Information media is labelled using the designations internal or external. Secure Sockets Layer (SSL) and Hypertext Transfer Protocol Secure (HTTPS) encryption have been implemented for communications between internal and external system components. SSL is a standard security technology for establishing an encrypted link between two systems. HTTPS is a

Assessment category	System findings and gaps
	protocol for secure communication over a computer network that is widely used on the Internet. Praekelt.org is currently identifying key aspects of the POPI Act that are applicable to MomConnect and developing use case scenarios to identify and develop appropriate controls that map to the Act's requirements. After registering with the system, all users are presented with consent screens to allow for active consent for the system. These screens are displayed in various languages. Users can opt out of receiving messages from the system. Individual requests for data require filling out a form that is reviewed by Praekelt.org for approval or denial.
	Gaps: Although the MomConnect system collects sensitive personal information for a large number of women, it does not meet the requirements of the POPI Act, which requires safeguarding personal information, regulating the manner in which personal information may be processed, and providing individuals with rights and remedies to protect their personal information from processing (Government of the Republic of South Africa, 2013). MomConnect does not include mechanisms for users to opt out and delete their records from the system, correct any erroneous information, and control the sharing of their data with other third-party systems. The consent screens presented at the time of registration do not provide users with the minimum level of relevant information needed to understand the implications of registering, such as information on the kinds of personal information that will be collected, how it will be used, and with whom it will be shared. The systems that are interconnected with MomConnect (DHIS 2, USSD provider, OpenHIE), through which sensitive personal information is sent and received, lack data-sharing criteria, policies, and agreements. There are no processes or guidelines for the handling, retention, and disposal of sensitive personal information collected by the system. Data at rest (i.e., data stored in the MomConnect database) are not encrypted, meaning that sensitive personal user information is stored in plain text, human readable format and can be viewed by unauthorized project staff or external parties if a data breach occurs.
Hardware and System Software Maintenance and Data Backups: Controls are used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that data backup procedures are being performed.	**Findings:** The MomConnect system and data are backed up weekly to an Amazon 3 server. Access to production servers, software, and data is restricted to a limited number of project team members. Documented processes and procedures on hardware and system software maintenance and data backups are in place and implemented routinely. A number of best practices have been implemented, including separation of production from development environments, routine backups, and appropriate access restrictions.
Access Controls and Identification and Authentication Measures: Access controls are the system-based mechanisms used to designate who or what has access to a specific system resource and the type of	**Findings:** Passwords are used extensively in the MomConnect system to provide access control. The system administration team occasionally performs testing on password complexity and strength. Role-based access control that corresponds to project team roles is currently implemented. Only a few members of the system administration team at Praekelt.org are designated as system administrators with access to critical system functions,

Assessment category	System findings and gaps
transactions and functions that are permitted. Identification and authentication measures are controls that prevent unauthorized people (or unauthorized processes) from entering an IT system.	data, and servers. Data transmission to and from the system is done using encrypted SSL and HTTPS communication channels. Almost all APIs to external systems are subject to authentication using passwords.
	Gaps: Although APIs use password authentication, this is the most basic form of access management and is not appropriate for authentication with external systems. Although the access controls, and identification and authentication measures implemented are in line with common best practices, it is unclear whether the level of implementation is adequate to protect the sensitive personal information collected by the system.
Audit Trails: Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability and a means to reconstruct events, detect intrusions, and identify problems.	**Findings:** Currently, administrator access to critical system hardware and servers is logged, and private key cryptography is used for the Secure Shell (SSH) Admin console.
	Gaps: Individual actions performed using administrator access and the SSH console are not currently logged, and an audit trail does not exist. Modification and access to sensitive personal information are not logged and a record of authorized, or unauthorized, activity does not exist.
Documentation and Configuration Management Tools: The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system document, and it formalizes the system's security controls. Configuration management tools provide automated methods of managing the system and data environments using tools with built-in best practices.	**Findings:** The MomConnect system leverages several configuration management tools, such as GitHub, Puppet, Jira, Sideloader, Sentry, South, Nose, Haystack, and Memcached, to manage various aspects of the system and data environments. Praekelt.org has developed and maintains online documentation of the standard operating procedures (SOPs) used by its engineering and administration teams. Using these automated configuration management tools and the defined SOPs is in line with established industry best practices to reduce human error and ensure stability of the development and production environments.

Note: Assessment categories are taken from the *Security self-assessment guide for information technology systems* (Swanson, 2001).

Vulnerability Testing and Scan

Vulnerability testing is a type of technical testing used to identify, validate, and assess technical vulnerabilities and assist organizations in understanding and improving the security posture of their systems and networks (Souppaya & Scarfone, 2008). It is not meant to take the place of implementing security controls and maintaining system security, but to help organizations confirm that their systems are properly secured and identify any organizational security requirements that are not met as well as other security weaknesses that should be addressed.

Vulnerability scans were conducted on the multiple components that make up the MomConnect system using the Acunetix vulnerability testing tool. Acunetix Vulnerability Scanner is an automated security testing tool that audits applications by checking for security based on both known and newly emerging security flaws and hacking vectors.

Results of vulnerabilities present in the MomConnect system and identified by the Acunetix Vulnerability Scanner are described as follows and ranked based on their threat level severity and potential impact to the system if exploited.

The scan results are summarized in Table 3 and broken out by:

- **Type of vulnerabilities present and identified:** The number of unique vulnerabilities identified across all the Mom Connect system components
- **Number of occurrences:** The locations where each unique vulnerability is present and needs to be addressed. For example, the user credentials sent in clear text vulnerability was identified as a unique moderate threat level vulnerability that occurs in seven MomConnect system components.

Table 3. MomConnect vulnerability scan results

Threat level and description	Type of vulnerabilities present and identified	Summary of type of vulnerability	Number of occurrences
High: These vulnerabilities are the most dangerous and put the scan target (i.e., the MomConnect system) at the maximum risk for system hacking and data theft.	1	nginx SPDY heap buffer overflow	1
Moderate: These vulnerabilities are caused by server misconfiguration and site coding flaws, which can result in server disruption and intrusion and put the scan target at a moderate security risk.	5	• Application error message • Django debug mode enabled • Error message on page • User credentials are sent in clear text • HTML form without CSRF protection	187
Low: These vulnerabilities result from a lack of encryption of data traffic or directory path disclosure. Their impact on the scan target if exploited presents a low risk.	4	• Clickjacking: X-Frame-Options header missing • Cookie(s) without HttpOnly flag set • Login page password-guessing attack • Possible sensitive directories	30
Informational: These vulnerabilities result from some best practices not being implemented. Their impact on the scan target if exploited presents a minimal risk.	4	• Email address found • Password type input with auto-complete enabled • Broken links • Possible username or password disclosure	30

High threat level vulnerability explained: The nginx SPDY heap buffer overflow vulnerability was identified as the only high threat level vulnerability. It occurs once in the help desk component. In order to remediate this vulnerability, an upgrade of nginx to the latest version should be applied using the patch provided by the vendor.

The Acunetix Audit scan reports provide in-depth technical details of other vulnerabilities present and identified. Recommended remediation steps are also included for each vulnerability. Due to the lengthy nature of these reports (230 pages), they are available as a separate document.

RECOMMENDATIONS

Based on the comprehensive assessment conducted, MEval-SIFSA recommends that MomConnect adopts a multi-layered security approach to ensure the embedding of a strong security management culture that will continuously implement, manage, and mitigate data and system security risks during the life and operation of the system. Such an approach would involve:

- Implementation of IT governance structures to provide overall management and oversight
- Development and operationalising of robust security polices, plans, and procedures
- Implementation of management, operational, and technical security controls at all levels
- Continuous risk management and mitigation to ensure responsiveness to emerging security threats and changing industry best practice, as well as efforts to ensure POPI Act compliance

Table 4 provides specific recommendations, which have been assigned a priority level (high, moderate, low, informational) for implementation. Priority levels are assigned based on the level of importance and criticality of implementing the recommendation. A timeline for planning, implementation, and review (short-term, medium-term, long-term) has also been identified for each recommendation.

Table 4. MomConnect security recommendations

Time Key:

Colour	Type	Timeline Specifics
	Short	Action items identified as short term should begin immediately and be completed within six months of receipt of this report.
	Medium	Action items identified as medium term should begin within approximately 6 months of receipt of this report and be completed within 12 months.
	Long	Action items identified as long term should begin within approximately 12 months of receipt of this report and be completed within 18 months.

Category	Recommendation	Priority	Action item by timeline
Information Technology Governance	The MomConnect system stakeholders should implement an IT governance structure that communicates a strong commitment to data and system security and provides for and drives the development and implementation of processes and procedures that support the necessary legal, regulatory, and best practice requirements. At a minimum, an IT governance structure should include the following roles: **Management and Oversight Committee:** Responsible for overall supervision to ensure that policies, procedures, and plans are developed and implemented. Ensures that periodic security reviews and continuous improvement processes are in place. Ensures that appropriate funding is provided for the security of the system. **Data and System Owner:** Designated by the Management and Oversight Committee to have due care and due diligence responsibilities over the data and system, including ultimate responsibility for data and system protection. Works closely with the Data and System Custodian to define specific security requirements, performs data classification, and determines levels of security necessary to protect the system and its data. **Data and System Custodian:** Mandated by the Data and System Owner to be responsible on a daily basis for continuous monitoring of security risks, implementation of security controls, development of risk mitigation plans, and real-time monitoring of the system and data for security vulnerabilities and potential breaches. **Data and System Auditor:** Responsible for conducting periodic independent system and data reviews and assessments, including automated security scans and testing.	High	1. Conduct meetings with all MomConnect system stakeholders to discuss, agree upon, and document the appropriate IT governance structure. 2. Create a plan in consultation with all MomConnect system stakeholders for the implementation of the IT governance structure. Implement the IT governance structure in accordance with the plan. In consultation with all MomConnect system stakeholders, review and refine as needed to ensure that it meets the needs of all stakeholders and the system.

Category	Recommendation	Priority	Action item by timeline
Security Risk Management	Develop a security plan in line with the risk management policy, POPI Act requirements, and regulatory and best practice requirements. A system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan may also reference other key security-related documents for the information system as appropriate, such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements.	High	1. Identify the appropriate security staff resources to undertake all security risk management tasks. 2. Create the security plan, including prioritization of activities and implementation timelines. 3. Review and approve the security plan (appropriate MomConnect system stakeholders). 4. Implement the plan based on outlined priorities and timelines.
			Review and refine as needed to ensure that it meets the needs of all stakeholders and the system.
	Define and document roles and responsibilities for day-to-day security risk management, including (1) who is responsible for ensuring personal data privacy protections and (2) associated system access rights, privileges, and functions.	High	Plan for and implement roles and responsibilities.
			Review and refine as needed.
	Formalize processes for risk identification, documentation, and mitigation.	High	Plan for and implement risk identification, documentation, and mitigation processes.
			Review and refine as needed.
	Map compliance requirements for legal, regulatory, and best practices to implementable security procedures and controls.	High	1. Conduct an activity to identify and map compliance requirements for all legal, regulatory, and best practices. 2. Plan for, prioritize, and schedule the implementation of all implementable security procedures and controls.
			1. Implement security procedures and controls in accordance with the outlined plan. 2. Review, test presence of, and correct implementation of procedures and controls.

Category	Recommendation	Priority	Action item by timeline
	Develop and implement a process to develop solutions for newly identified and ongoing security and data risks for the life of the system.	High	Develop, prioritize, schedule, and implement a process to develop solutions for newly identified and ongoing security and data risks for the life of the system.
			Review and refine as needed.
	Detail and implement procedures for continuous assessment of security risks, such as yearly independent assessments.	Moderate	Identify, document, and prioritize continuous assessment procedures.
			Schedule and implement procedures; review and refine as needed.
	Implement routine evaluations, such as periodic and yearly risk assessments, application vulnerability scans, and network penetration tests, using industry-recognized automated tools to identify vulnerabilities.	High	1. Identify and document evaluation criteria. 2. Plan for and schedule scans and tests.
	Implement formal processes for reviewing evaluation results with stakeholders, and develop and implement specific plans to remediate security vulnerabilities.	Moderate	Proceed with activities to plan for and conduct at least one formal review with stakeholders.
	Implement routine verification and validation of controls implemented to ensure that they are effective as newly emerging risks are encountered.	High	1. Plan, identify, and document routine verification and validation methods. 2. Implement, review, and refine as needed.
Incident Response Capability	Expand on the three-step process for incidence reporting to include incident containment, investigation, analysis, tracking, and follow-up steps to close the loop on this process.	Low	Implement, review, and refine as needed.
System Development Life Cycle	Develop a system transition or disposal plan with provisions that map directly to the POPI Act and that outline how sensitive data would be handled in the event of system decommissioning or transition to a different system or data custodian.	Moderate	Develop, document, and obtain approval for the system transition or disposal plan. Implement, review, and refine as needed.
Certification and Accreditation	The NDOH should undertake to define a process for certifying and accrediting systems developed on its behalf. This process could be used as the baseline for managing security for all systems developed for NDOH.	High	Begin consultation with NDOH for the development of a certification and accreditation criteria and process; implementation of this recommendation will go beyond 18 months.

Category	Recommendation	Priority	Action item by timeline
Personnel Security, Security Awareness, Training, and Education	Periodically review system access controls for project staff to ensure that they are appropriate to their job descriptions, mirror their current job roles and responsibilities, and, if necessary, reduce access control to mitigate security risks.	High	Schedule and perform an access control review activity and reduce access control based on review findings.
	Develop formal security awareness information materials that outline staff responsibilities, especially regarding handling sensitive personal information.	Moderate	1. Develop or procure appropriate security awareness training materials. 2. Schedule and conduct training activities. 3. Review and refine as needed.
Physical, Environmental, and Server Protection	Define the appropriate physical protection, environmental protection, and contingency planning requirements that third-party hosting providers are required to meet. These requirements would be enforced through service-level agreements between the parties that should include provisions to verify and validate implementation and continuous monitoring of compliance.	High	1. Engage with third-party hosting providers to develop plans. 2. Approve, formalize, and implement plans. 3. Conduct scans and tests. 4. Review and refine as needed.
	Third-party hosting providers should periodically perform and make available to the stakeholders any results from vulnerability scans and penetration testing as well as subsequent remediation plans.		
Technical Access Controls, Identification and Authentication Measures	Review currently implemented access controls and identification and authentication measures against legal and regulatory requirements set forth by the POPI Act. Identify and map controls to requirements, implement additional controls based on this analysis, and continuously monitor and periodically audit the effectiveness of these controls using security testing and reviews. Because the system collects sensitive personal information, more complex multifaceted access controls and identification and authentication measures may need to be implemented.	High	1. Plan for and schedule this review. 2. Document requirements, and prioritize and schedule the implementation. 3. Implement and monitor controls and measures.
Data Confidentiality, Integrity, and Information Media Access Controls	Determine the legal and regulatory requirements set forth by the POPI Act. Prioritize identifying and implementing policies and procedures as well as technical, management, and operational controls that ensure compliance and safeguard data confidentiality.	Moderate	1. Determine and document requirements. 2. Plan, prioritize, and schedule implementation activities
			Implement requirements.
	Review the type of sensitive personal information being collected for appropriateness and streamline any data deemed not essential for the system purpose.	High	Plan for, schedule, and document results of this review.

Category	Recommendation	Priority	Action item by timeline
	Research already existing best practices for implementing robust consent, opt-out, user record correction, and deletion solutions implemented by other applications globally and use tested approaches to develop these features.	Moderate	Conduct research activities and document results.
	Implement encryption and hashing of sensitive personal user information collected by the system to safeguard against unauthorized access by both internal and external parties.	Moderate	Determine and operationalise encryption and hashing procedures.
	Work with system stakeholders to develop data-sharing criteria and policies for downstream systems and individuals that receive sensitive personal user information from the MomConnect system, such as DHIS 2 and OpenHIE, to ensure compliance with the POPI Act.	High	Develop, agree upon, and operationalise data-sharing criteria, policies, and agreements.
	Draft and execute specific data-sharing and nondisclosure agreements with all third-party systems and individuals involved in sending and receiving sensitive personal user information that are tailored to the specific purpose for which the external parties are using the data.	High	
	Develop policies for data handling, retention, and disposal of sensitive personal information collected by the system that comply with the POPI Act and with best practice guidelines. This will ensure proper data management and reduction, where necessary, of the amount of sensitive personal information, thus mitigating the risk of exposure in the event of a security breach.	High	Review and refine as needed.
	Determine audit trail requirements, especially those relating to access and modification of sensitive personal information. Implement robust automated audit trail functions to closely monitor access to and modification of critical system hardware, servers, and sensitive personal information.	Moderate	
Hardware and System Software Maintenance and Data Backups	Review the documented process and procedures to ensure alignment with POPI Act requirements.	High	Conduct the review and document results.
Vulnerability Testing and Scans	Remediate and immediately address vulnerabilities identified as having a **high** threat level severity and maximum potential impact.	High	Review scan results and remediate all high threat level vulnerabilities.
			Review and perform scanning to verify presence of vulnerabilities and correct implementation.

Category	Recommendation	Priority	Action item by timeline
	Remediate and address immediately vulnerabilities identified as having a **moderate** threat level severity and moderate potential impact. If immediate action is not possible for all threats, prioritise remediation of vulnerabilities in multiple phases.	High	Review scan results and identify schedule for implementation based on prioritization of each vulnerability. Remediate in phases all moderate threat level vulnerabilities based on the schedule. Review and perform scanning to verify presence of vulnerabilities and correct implementation.
	Prioritize remediation of vulnerabilities identified as having a **low** threat level severity and low potential impact and subsequently address each vulnerability.	Low	Review scan results and identify schedule for implementation based on prioritisation of each vulnerability. 1. Remediate in phases most low threat level vulnerabilities based on the schedule. 2. Review and perform scanning to verify presence of vulnerabilities and correct implementation.
	Prioritize remediation of vulnerabilities identified as being **informational** and having minimal potential impact and subsequently address each vulnerability after all high, moderate, and low threats have been remediated and addressed.	Low	Review scan results and identify, prioritise, and determine a course of action for each vulnerability. Many of these vulnerabilities will not need remediation or further action.

REFERENCES

Government of the Republic of South Africa. (2013). Act No. 4 of 2013: Protection of Personal Information Act. Retrieved from http://www.justice.gov.za/legislation/acts/2013-004.pdf.

International Organization for Standardization. (2016). Information technology—Security techniques—Information security management systems—Overview and vocabulary (ISO/IEC 27000:2016[E] Fourth edition). Retrieved from: http://www.iso27001security.com/html/27000.html.

Souppaya, M., & Scarfone, K. (2008). *Technical guide to information security testing and assessment: Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-115. Washington, DC: National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment.

Swanson, M. (2001). *Security self-assessment guide for information technology systems.* NIST Special Publication 800-26. Washington, DC: National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/security-self-assessment-guide-information-technology-systems.

Swanson, M., Hash, J., & Bowen, P. (2006). *Guide for developing security plans for federal information systems.* NIST Special Publication 800-18 Revision 1. Washington, DC: National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.

APPENDIX. STAKEHOLDER COMMENTS

This appendix summarizes comments from MomConnect stakeholders in response to the draft MomConnect Security Assessment Report after review.

General Comments

Reviewers noted the robust process used to analyse MomConnect security and the resulting comprehensive report. However, they noted that this assessment focuses on the Praekelt.org systems, funded by USAID, and not on other components of the overall MomConnect system. The assessment did not include much of the DHIS2 infrastructure or the interoperability layer infrastructure, except for possible vulnerability testing of the OpenHIM endpoints. OpenHIM endpoints are also all protected by strong passwords and HTTPS, which should be sufficient to pass penetration testing but could be strengthened to use certificate authentication. The report also did not mention issues related to the data coming in from the Mobile Network Operators via USSD and SMS. Although the MTN, Vodacom, and WASP systems are largely out of MomConnect's control, reviewers felt that it would be appropriate to get confirmation on their security practices. There was consensus that a similar assessment should be carried out on other MomConnect components. Reviewers noted that PMTCT data are now being stored in the system and should have been considered during the assessment, because the inclusion of these data may increase the overall sensitivity assessment for the system. Reviewers also noted that security testing was conducted on the MomConnect system before the help desk's migration to OpenHelpdesk and that testing did not include Vumi (the previous MomConnect platform). Reviewers commented that application vulnerability scan findings of this report would not be relevant after a platform migration to RapidPro, and they recommended that new vulnerability scans be commissioned after platform migrations are complete.

Comments on Data and System Assessment Findings Section

Assessment category	Stakeholder comments
IT Governance	Reviewers commented that findings in this area are **accurate** because the system does not have the full complement of policies, roles, and capacity needed to manage the security for the system. Currently, Mary Racter, a Praekelt.org staff member, is tasked with security, and her role explicitly specifies oversight in security management and data protection, leading to gaps in capacity that reduce the efficacy of security initiatives. Formally, documentation of Praekelt.org's approach to POPI compliance is available at https://docs.google.com/document/d/16zNmKxuNaoJhKFJE4rTOgfQeom9iko0t5MmGBeofQV4/edit); however, implementation has lagged behind due to budget and capacity limitations. Reviewers suggested that Praekelt.org could investigate the possibility of increasing security management and data protection capacity for MomConnect. An additional role of "owner" (directly responsible individual) of security management for MomConnect was suggested; this role would not need to be a technical role, although technical expertise would be advantageous. The role would assume responsibilities similar to project management but would explicitly concern itself with the maintenance of a strong security position on the platform, as well as the prioritisation of security deliverables and scheduled assessment and remediation. This role would also concern itself with the delivery and maintenance of POPI compliance, which would be required due to the ever-changing state of the MomConnect platform's architecture,

Assessment category	Stakeholder comments
	necessitating proactive prioritisation of security processes in line with the project's budget structure and roadmaps.
Security Risk Management	Reviewers commented that findings in this area are **partially accurate** and provided links to the system's risk management strategy as follows: • Cybersecurity Tools and Approaches Handbook https://docs.google.com/document/d/1yM5QThVZRZ_AfRJkEBPJTS5x2jVBMEjh1hUdcWVP0uk/edit This handbook outlines the tools and processes that should be used in risk management and mitigation for Praekelt.org's systems, and it covers the Prevention, Detection, Response, and Recovery phases of the cybersecurity life cycle. This is the methodology currently used by the Security Engineering team, although additional work is required to bring operations up to the level proposed by the document. • Vulnerability Disclosure and Handling Protocol https://docs.google.com/document/d/1weluFHGs_o6bwGecriI8JmkRtVCIV2JKGiW-PeaBxYY/edit This document explains the process of risk mitigation after vulnerabilities have been identified in the system and its integration points. However, no formal policies exist as of February 2017 outlining the frequency and scope of any routine security assessments that would identify such vulnerabilities. Although formal budget allocation exists for infrastructural security maintenance, such formal budget considerations do not currently extend to routine security assessments and risk management processes. • Cybersecurity Incident Response Framework https://docs.google.com/document/d/1-sB7KHP3xK_bX33r66Q_rHtAiyoJx-CTiMXaPTNkypY/edit This framework is intended to mitigate risks of an active data breach. Although not explicitly stated, this framework would also be applicable if data were leaked through our integration points with external systems. • Seed Maternal Health Attack Surface Map https://docs.google.com/document/d/1mlJN5br6v5yR77fv11nhB9Uf79izI5tqByJLdfpobP4/edit This map is used to identify and manage the risks related to Seed and its subsystems. Its function includes the representation of MomConnect integration points as key areas for consideration. However, as mentioned above, no routine budget or protocol exist for assessing these integration points. Another problem is that the rapid development and architectural shifts to which the MomConnect platform is subject increase the overhead required to maintain an up-to-date view of the platform's attack surface. • MomConnect Data Breach User Flows https://docs.google.com/document/d/1gCaa86-L2ywTly7proU98nKi0XzqdiT0vVU2lWbmvAI/edit Reviewers also suggested that additional risk management policies were needed to fulfil the MEval-SIFSA recommendations, which could be developed by Praekelt.org's security subject matter experts (SMEs) and include (1) policies that address security risk management when new features are added to the platform; (2) policies that address security risk management when the platform undergoes a significant architectural change (e.g., a migration); (3) policies that dictate the scope and frequency of routine security assessment and maintenance tasks; and (4) policies that address risk mitigation for critical security controls in the platform's attack surface, such as external integration points and access control mechanisms. In addition, it was suggested that Praekelt.org could commission security assessments for MomConnect's integration points with

Assessment category	Stakeholder comments
	external systems. This could be performed by Praekelt.org's security SMEs or contracted to a trusted security assessment vendor. As with the gaps identified in the area of IT governance, it was suggested that a project-management-level role overseeing security management and ensuring protocols be devised and carried out effectively. Budget-friendly tools, such as Nessus or Nitko, could be purchased and used to perform internal testing.
Review of Security Controls and Incident Response Capability	Reviewers commented that findings in this area are **partially accurate**, noting that only a partial coverage of the attack surface of the platform to assess system security controls has been done due to budget constraints. Subsequent to the assessor's visit, a partial internal penetration test of the Sideloader components was conducted; the resulting report is contained here: https://docs.google.com/document/d/1kI9U36IaXuFtcQOVYbYD1CuZi1kgnEllG4yP9irO-VI/edit. However, a strategy to address and mitigate the vulnerabilities found on Sideloader has not been devised, because it was agreed that complete graduation from Sideloader was the most desirable strategic choice. It should be noted that there are currently no concrete plans for graduation, owing to a lack of investigation into the solution landscape and a capacity shortage on the part of the Site Reliability Engineering (SRE) team, which is the responsible constituency within Praekelt.org. Reviewers agreed that additional penetration testing was required as well as strategic management to incorporate any findings into the long-term roadmap of the platform. Reviewers commented that although Praekelt.org has an Incident Response Plan for security incidents, it has not been implemented in practice because no significant security events have occurred to their knowledge. Reviewers agreed that forensic investigation into the causes of security incidents forms part of the incident response process, along with a review and retrospective of the event after it has been contained.
System Development Life Cycle	Reviewers agreed that findings in this area are **accurate** and noted a need to create an official plan to scrub data from the systems; these plans would outline all the areas in which data are likely to persist (e.g., databases, logs, backups).
Certification and Accreditation	Reviewers noted that the goal of certification is to have some external ratification for a strong security position, further noting that there are several ways to achieve this in negotiation with MomConnect stakeholders. They suggested that robust external security assessments coverage and a report that confirms a strong security position can fulfil goals similar to certificates issued by a certification body.
System Security Plan	Reviewers commented that findings in this area are **partially accurate** because they deemed the assessor's view of the system state to be out of date, and provided the following details: • POPI Compliance Tools and Approaches Handbook https://docs.google.com/document/d/16zNmKxuNaoJhKFJE4rTOgfQeom9iko0t5MmGBeofQV4/edit This handbook documents the processes that system stakeholders will follow in order to bring new and existing projects to POPI compliance. The directly responsible individuals in this case would be the Project and Program Managers, who will ensure that the process is followed and that deliverables are actioned. This POPI plan contains considerations for bringing the security position of the platform to an acceptable standard in order to fulfil POPI requirements.

Assessment category	Stakeholder comments
	• Seed Maternal Health Secure Deployment Guidelines https://docs.google.com/document/d/1mEjn7yxcDVh3ZhtxXS2vT0F_0CAePgMs83xoDvwIsaQ/edit This plan outlines best practices for security of the Seed stack given its current attack surface. It also includes action items and JIRA tickets for the fulfilment of such best practices. However, reviewers noted that this plan may need to be revised from time to time, because the rapid shifts in the features and architecture of the MomConnect platform mean that the appropriate security approaches could also change. Reviewers however noted that the existing security plan needs to address the following key issues: • Access control policies and protocols • Role delineation and conditions of access (i.e., expected behaviour) • Staff training on access control and conditions of access
Personnel Security, Security Awareness, Training, and Education	Reviewers commented that findings in this area are **partially accurate**, noting that the thoroughness of personal references and reference and qualification checks had not been verified, and that no documented procedures exist to ensure that least-privileged system access and robust separation of duties according to roles are implemented and enforced. Also noted was that an internal operational security training session was to be hosted for Praekelt.org staff in February 2017, covering aspects of personal security, credential security, operational security considerations, and procedures on handling sensitive information. Also suggested was that further training be conducted after the development of access control policies, protocols, and role-based access delineations.
Physical, Environmental, and Server Protection	Reviewers noted that it would be difficult to compare Hetzner's level of robustness to Amazon's without formal investigation into physical structures and management of both platforms. On the issue regarding self-hosting and controlling hardware assets, reviewers noted that system stakeholders were not cloud-hosting providers, but would negotiate risk management for hosting on cloud-hosting providers with system security stakeholders.
Data Confidentiality, Integrity, and Information Media Access Controls	Reviewers pointed out that MomConnect stakeholders had taken steps towards implementing some of the requirements for POPI compliance as detailed below: • MomConnect POPI Compliance Iteration 1 https://docs.google.com/document/d/1TLiJytIDA3UCEAE-gPI0XSD9ZaPnpY51-5DhOR5lx0M/edit In particular, this report documented the inadequacy of information in the consent screen and the proposed solution of implementing frequently asked questions to deliver the required information, because it was determined that it is not feasible to deliver vast quantities of information over USSD due to usability constraints of unstable USSD connections. The specification document for iteration 1 also includes facilities for users to view, update, and delete their information. Other requirements to fulfil POPI compliance are scheduled for consideration in subsequent iterations. Reviewers also noted that the system does not encrypt its data stores at rest because of performance and exposure constraints. Further investigation would be needed to look into this possibility. It was also noted that databases can be breached in many different ways, and encryption on production databases would only protect against scenarios in which the database servers are compromised directly and would not prevent leakage of decrypted data displayed in control interfaces and help desks. Reviewers also suggested the implementation of client-side encryption for data

Assessment category	Stakeholder comments
	backups as an immediate and easy solution while feasibility studies are conducted into encrypting production databases. An iterative approach to POPI compliance was suggested.
Access Controls and Identification and Authentication Measures	Reviewers commented that findings in this area are **accurate**, noting that most of the systems' APIs were guarded by password-based HTTPS authentication. Suggestions were made to conduct further investigation into more robust access controls in line with the systems' long-term technical roadmap. Reviewers also noted was that access to critical server infrastructure extends to at least the entirety of the SRE team.
Audit Trails	Reviewers commented that findings in this area are **accurate**, noting that currently there is no adequate logging system in place for access to critical infrastructure or sensitive information and that this would require implementation on both the infrastructure and application levels. Reviewers agreed that a lack of logging systems could significantly impede the progress of any security-related forensic investigations and could reduce the effectiveness of routine security maintenance tasks. Reviewers suggested that investigation and implementation of logging and monitoring systems should be conducted.

Comments on MomConnect Security Recommendations Section

Reviewers noted that negotiation with stakeholders on the feasibility of the report recommendations, as well as formulating a long-term security roadmap to ensure risks are mitigated, is needed. The recommendations suggested propose a large number of additions to existing capacity, which may not be feasible given Praekelt.org's budget and organisational constraints. Reviewers also highly recommended that a formal meeting that includes all stakeholders be convened to determine next steps after the report has been finalised and accepted by Praekelt.org and the NDOH.

MEASURE Evaluation–Strategic Information for South Africa
(MEval-SIFSA) Project
138 Muckleneuk Street
Nieuw Muckleneuk, Pretoria
South Africa
Tel: + 27 12 346 7490
http://www.measureevaluation.org/sifsa

This research has been supported by the President's Emergency Plan for AIDS Relief (PEPFAR) through 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. MEASURE Evaluation–SIFSA is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of PEPFAR, USAID, or the United States government. TR-17-231

momconnect

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

PEPFAR

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation SIFSA