The Privacy, Confidentiality and Security Assessment Tool

Protecting personal health information

Contents

Foreword

With the scale-up of HIV and other health services in low- and middle-income countries, an increasing amount of personally identifiable health information is being collected at health facilities and in data repositories at the regional and national levels.

Countries need to protect the confidentiality and security of identifiable and de-identified personal health information, and this can be accomplished in part through the existence and implementation of relevant privacy laws.

A UNAIDS and United States President's Emergency Plan for AIDS Relief (PEPFAR) workshop with

multi-stakeholder input that was held in Geneva, Switzerland, in 2006 led to the development of country guidelines to protect the confidentiality and security of HIV information. Those *Guidelines on protecting the confidentiality and security of HIV information: proceedings from a workshop (1)* (interim guidelines) can be used by countries to adapt, adopit and implement their own guidelines

In 2008, 96 low- and middle-income countries were surveyed to determine whether or not they had developed and implemented their own guidelines *(2)*. The findings indicated that very few countries had developed comprehensive guidelines on protecting the confidentiality and security of HIV information.

Based on the interim guidelines, an assessment tool was drafted in 2011 to help national stakeholders assess the existence and implementation of national country policies on protecting the confidentiality and security of personal health information collected and held at the facility and data warehouse levels.

This draft was reviewed at a workshop of health-care professionals and community members in Lusaka, Zambia, in 2012. The suggestions were compared and combined with existing data security and confidentiality guidelines, and in June 2014, a penultimate version of the assessment tool was produced. This draft was field-tested in

Kingston, Jamaica, in September 2014. The feedback from this field test resulted in the production of this *UNAIDS/PEPFAR Privacy, confidentiality and security assessment tool: protecting personal health information*, which provides guidance for countries to facilitate, where required, the assessment of the security of the collection, storage and use of data in order to maintain privacy, confidentiality and security.

For those unfamiliar with the use of this assessment tool and its three modules, please consult *The Privacy, Confidentiality and Security Assessment Tool: user manual l (user manual) (3)*. The user manual provides guidance for health professionals who want to use the assessment tool to gather the information required to assess the extent to which the confidentiality and security of identifiable and de-identified personal health information are protected.

Summary

This assessment tool comprises three modules that provide health-care professionals with a set of standardized questions that will enable them to

gather country-based information to assess whether the privacy, confidentiality and security of personal health information are protected throughout the service delivery and data management settings in a particular country.

The three modules in this tool are as follows:

- Facility-level assessment tool.
- Data warehouse-level assessment tool.
- Policy-level assessment tool.

Concepts relevant to the protection of data

Three interrelated concepts affect the protection of data: privacy, confidentiality and security.

- **Privacy** is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information. Privacy provides the overall framework within which both confidentiality and security are implemented. Privacy protections vary between jurisdictions and are defined by law and regulations.
- **Confidentiality** relates to the right of individuals to the protection of their data during its storage, transfer and use in order to prevent unauthorized disclosure of that information. Confidentiality policies and procedures should

include discussion of the appropriate use and dissemination of health data, with systematic consideration of ethical and legal issues, as defined by privacy laws and regulations.

- **Security** is a collection of technical approaches that address issues covering physical, electronic and procedural protection for information collected. Security discussions should include identification of potential threats to systems and data, and they must address both the protection of data from inadvertent or malicious inappropriate disclosure and the non-availability of data due to system failure and user errors.

While all data have confidentiality and security requirements, there are important differences in terms of their sensitivity and the potential impact if confidentiality is breached. Five main types of information exist.

- **Personally identifiable health information** is individual-level information that includes personal identifiers (such as names and addresses) that are generally obtained at the point of service delivery. This also includes national identification numbers, such as social security numbers in the United States of America.
- **Pseudo-anonymized or de-identified health information** is individual-level information that has been stripped of certain identifiers, such as names and addresses. In many cases, the identifying information has been replaced with a randomized identifier or key value that can be used, if necessary, to link it with a person's record that is being maintained at a service facility.
- **Anonymized or non-identified health information** is information that has been stripped of all identifiers. Since no keys are kept, these data can no longer be linked to the person's record that is being maintained at a service facility.
- **Aggregated health information** is data based on aggregating individual-level information into an indicator. They may be obtained from communities, health facilities or data warehouses. These data are usually managed at the level of regional or national databases and also are collected by many international organizations.
- **Non-personal health information** is information on facilities, geographic data, information on medicines and medicine supplies, and other logistics.

Main points: how to use the assessment tool

A detailed user manual on how to apply the assessment tool and its three modules has been prepared. The assessment tool and the user manual complement one another, and those unfamiliar with the assessment tool should consult the user manual *(3)*.

This section of the assessment tool provides a brief description of the content of the modules and a summary of how the assessment should be applied at the health facility, data warehouse and policy levels, respectively. For more detailed guidance, please consult the user manual.

Each of the three modules contains a set of questions under the following major headings:

- Governance and policy.
- Data collection (not included at the policy level).
- Data storage.
- Data backup (not included at the policy level).
- Authorization and access control.
- Data release.
- Transmission security.
- Data disposal.

These headings, in turn, have a number of subheadings and relevant questions, as can be seen in the following example of governance and policy:

- Policy.
- Governance structure.
- Review of security practices.

- Responsibilities and training.
- Monitoring, detecting and responding to security breaches.
- Conducting risk assessments.
- Connectivity to other networks.

Table 1 summarizes the main steps required to perform an in-country assessment.

Table 1

Checklist for administering the assessment tool

- The ministry of health—specifically the office of the permanent secretary of health—should lead and coordinate this initiative, co-managed by the director of health informatics and the records department.
- A steering committee must be created with membership from ministry of health and key stakeholders (including other government ministries, donors and civil society).
- A terms of reference and a selection process must be developed for the selection of an external professional (the assessor) to conduct the assessment.
- A work plan needs to be developed based on discussions between members of the steering committee. The work plan outlines the process for administering the assessment tool and lists relevant members of the ministry of health, other government officials, health and legal professionals, and members of civil society who will participate in the process.
- An entry meeting provides the launching point to start the assessment and an opportunity to agree on the process and the logistics of administering the assessment tool. The permanent secretary needs to send out an invitation letter to entry meeting participants.
- The entry meeting should be led by the director of health informatics, along with members of the records department of the ministry of health. The assessor and the ministry of health present the draft work plan.
- Prior to each site visit, the records department of the ministry of health must designate a meeting coordinator at each site. The meeting coordinator should identify and contact those who should be present at the meeting and brief them on the reason for the meeting. Prior to the meeting the representatives at the facility where the questionnaire is being administered are requested to furnish electronic or paper based policies, guidelines, legislation or other such material that will be used as part of the verification process.
- At the onset of the meeting at each site, hard copies of the assessment tool need to be distributed to the participants. The ministry of health or the assessor shall introduce the reason for the meeting and describe the assessment tool to the participants.
- Data collection uses the paper-based or electronic version of the assessment tool. Images of the said policies, guidelines, legislation must be captured as part of the verification process. Also, images of the rooms where records are collected must be captured. A (v) in the question indicates that the response must be verified.
- Following the completion of the assessment process at all levels, an exit meeting should be held where the results of the assessment are presented to a wider audience (including members of civil society). The results should then be discussed with this broader group of stakeholders.
- The assessor and member of the ministry of health review the results of the assessment, incorporating issues raised through the feedback process and developing a report based on the findings. This report will inform the way forward in terms of developing and implementing guidelines for protecting the confidentiality and security of personal health information.

The privacy, Confidentiality and Security Assessment Tool

Facility-level assessment tool

The following facility-level questions are set to determine the security, confidentiality and appropriate use, including sharing, of data

collected by health programmes at the primary, secondary and tertiary facilities.

The questions are grouped into eight sections:

- Governance and policy.
- Data collection.
- Data storage.
- Data backup.
- Authorization and access control.
- Data release.
- Transmission security.
- Data disposal.

A brief purpose statement introduces each section, followed by a set of questions.

Table 2

Recommended facility-level questions

1. Governance and Policy		
Category	**Questions**	**Instruction**
1.1 Policy Purpose: to determine the existence, accessibility, distribution, development and review of a written policy document that ensures the confidentiality and security of personally identifiable health data.	1.1.1 Do you have clearly defined roles and access levels for all persons with authorized access to personally identifiable data? 1. Yes (v) 2. No	
	1.1.2. Do you have clearly defined standard procedures or methods that must be followed when accessing personally identifiable data? 1. Yes (v) 2. No	
	1.1.3. Does a written policy document regarding the requirements for ensuring the confidentiality and security of personally identifiable health data exist in this facility (referred to as the "Data Confidentiality and Security Policy" or "the Policy")? 1. Yes, a single all-inclusive Data Confidentiality and Security Policy exists (v) 2. No, but a policy is in the process of development 3. No, but various informal policies exist 4. No, but various formal policies exist 5. No, we do not have any policy or written guidelines	IF "2," "3" OR "4," GO TO QUESTION 6.
	1.1.4. Is the Data Confidentiality and Security Policy readily accessible to all staff members in this facility who have access to confidential, individual-level data? (By "readily accessible," we mean that staff can easily access the policy online or in hard copy while at work.) 1. Yes 2. No	

Category	Questions	Instruction
	1.1.5. To which stakeholders and organizations is the Data Confidentiality and Security Policy document distributed? (Please select all that apply.) 1. Staff who request it 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Health-care volunteers 6. Other health professionals 7. Information technology staff (including data entry staff, analysts, managers and programmers) 8. Administrative staff 9. Cleaners, security guards and other providers of support services 10. Policy document is not distributed 11. Health records staff 99. Other (please specify): 1.1.6. In which of the following formats is the Data Confidentiality and Security Policy document available to staff for reference? (Please select all that apply.) 1. Printed hard copies (v) 2. Electronic, distributed via e-mail (v) 3. Electronic, distributed via CD or other media (v) 4. Electronic, available on the Internet (please specify the URL): 99. Other (please specify):	
1.2 Governance structure Purpose: to determine the governance structure that is in place to provide oversight for the appropriate collection, use and dissemination of data, including regular review of the policy document and security practices.	1.2.1. Is there a local governance structure (e.g. steering committee/ advisory board) in place to provide oversight for the appropriate collection, use and dissemination of data, including regular review of the policy document and security practices? 1. Yes 2. No 99. Other (please specify): 1.2.2. How often does the steering committee or advisory board meet? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular meeting schedule 1.2.3. Which uses of personally identifiable information are covered by your local guidelines on the security and confidentiality of data? (Please select all that apply.) 1. Individual health care (v) 2. Public health practice (including monitoring and evaluation) (v) 3. Human subject research (with consent) (v) 4. Exceptional statutory purposes (v) 5. Not specified 99. Other (please specify):	IF "2," GO TO QUESTION 9.

Category	Questions	Instruction
	1.2.4. Is Information Security and its Management reviewed at regular intervals? 1. Yes 2. No	
1.3 Review of security practices Purpose: to determine the security practice and review as documented in the policy.	1.3.1. Are security practices reviewed by independent auditors? 1. Yes 2. No	IF "2," GO TO QUESTION 13.
	1.3.2. How often do independent auditors review security practices? 1. Yearly 2. Every 1–2 years 3. Every 2+ years 4. Not specified 99. Other (please specify):	
1.4 Responsibilities and training Purpose: to determine the security practice and review as documented in the policy.	1.4.1. Are staff explicitly informed of their individual responsibilities for protecting the systems (paper-based or electronic) that are used to access and utilize personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 15.
	1.4.2. How are staff informed of their individual responsibilities for protecting the systems (paper-based or electronic) that are used to access and utilize personally identifiable health data? (Please select all that apply.) 1. Policy documents distributed to staff 2. Informal on-the-job training received by staff 3. Formal training received by staff 99. Other (please specify):	
	1.4.3. Do policies state that staff are personally responsible for protecting paper records, computer workstations, laptop computers or other devices associated with confidential public health information or data? 1. Yes (v) 2. No	
	1.4.4. Are all persons authorized to access personally identifiable health data trained on the organization's information security policies and procedures? 1. Yes 2. No	IF "2," GO TO QUESTION 19.
	1.4.5. How often must staff repeat the training on confidentiality and security measures? 1. Yearly 2. Every 1–2 years 3. Every 2+ years 99. Other (please specify):	

Category	Questions	Instruction
	1.4.6. Which of the following is the format of the training on confidentiality and security measures? (Please select all that apply.) 1. Material read by staff from printed document 2. Material read by staff on a website 3. Instructor-led web training at scheduled intervals 4. Instructor-led training in a classroom setting 5. One-on-one training with another staff member (peer-led model) 99. Other (please specify):	
	1.4.7. Is the date of the training or test documented in the employee's personnel file? 1. Yes (v) 2. No	
	1.4.8. Do all newly hired staff members sign a confidentiality agreement before they are given authorization to access personally identifiable health data? 1. Yes (v) 2. No	
	1.4.9. Which of the following authorized staff members in your program sign a confidentiality agreement? (Please select all that apply.) 1. Records department staff 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Health-care volunteers 6. Other health professionals 7. Information technology staff (including data entry staff, analysts, managers and programmers) 8. Administrative staff 9. Professional service providers 10. Cleaners, security guards and other providers of support services 11. Staff are not required to sign an agreement 99. Other (please specify):	IF "12," GO TO QUESTION 24.
	1.4.10. Do staff have to repeat the review and signing of the confidentiality statement indicating they understand the policies and agree to implement them? 1. Yes 2. No	IF "2," GO TO QUESTION 24.
	1.4.10. Do staff have to repeat the review and signing of the confidentiality statement indicating they understand the policies and agree to implement them? 1. Yes 2. No	IF "2," GO TO QUESTION 24.

Category	Questions	Instruction
	1.4.11. How often must staff repeat the review and signing of the confidentiality statement indicating they understand the policies and agree to implement them? 1. Every year 2. Every 1–2 years 3. Every 2+ years 4. Never 99. Other (please specify):	
	1.4.12. Are staff explicitly informed of the possible consequences of failing to properly protect personally identifiable health data? 1. Yes (v) 2. No	
	1.4.13. Depending on the severity of the breach, which of the following are possible consequences for members of staff who fail to protect personally identifiable health data? (Please select all that apply.) 1. Education or counselling to prevent repeat minor breaches 2. Reduction or loss of security clearance 3. Reduction or loss of data access privileges 4. Demotion 5. Suspension 6. Dismissal/termination of employment 7. Civil legal action 8. Criminal legal action 9. Not specified 99. Other (please specify):	IF "9," GO TO QUESTION 28.
	1.4.14. How are staff informed of the possible consequences of failing to protect personally identifiable health data? (Please select all that apply.) 1. Policy documents distributed to staff 2. Informal on-the-job training received by staff 3. Formal training received by staff 4. Confidentiality statement signed by staff 99. Other (please specify):	
	1.4.15. When a staff member's employment is terminated, when are data access privileges revoked? 1. Immediately upon termination 2. Within a specified period of time after termination (e.g. 30 days) 3. Not automatically revoked 99. Other (please specify):	
	1.4.16. Is it a requirement that the Data Confidentiality and Security Policy is shared with patients in facilities that are collecting personally identifiable data? 1. Yes 2. Yes, only if they ask 3. No	IF "2," GO TO QUESTION 30.

Category	Questions	Instruction
	1.4.17. How is the Data Confidentiality and Security Policy shared with patients? 1. Available on website, but not explicitly shared (v) 2. Provided only upon request 3. Provided to all patients as a hard copy or a link to the website as a matter of practice (v) 4. Provided only verbally to patients 99. Other (please specify):	
	1.4.18. Is there a designated information security manager at the facility? 1. Yes 2. No	IF "2," GO TO QUESTION 33.
	1.4.19. Is there a written description of the information security manager's responsibilities? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 33.
	1.4.20. Which of the following tasks are part of the information security manager's responsibilities? (Please select all that apply.) 1. Identify and review all applicable guidelines 2. Advocate for the resources needed for information confidentiality and security 3. Ensure that information confidentiality and security goals are identified, that they meet organizational requirements, and that they are initiated and integrated into relevant processes 4. Improve confidentiality and security awareness by initiating appropriate plans and programs 5. Test, review and validate the effectiveness of the implementation of the information confidentiality and security policy 6. Provide clear direction and visible management support for confidentiality and security initiatives 7. Approve assignment of specific roles and responsibilities for information confidentiality and security across the organization 99. Other (please specify):	
1.5. Monitoring, detecting and responding to security breaches Purpose: to identify and manage security breaches as documented in the policy.	1.5.1. Do written guidelines exist for managing security breaches for both electronic and paper-based systems? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 35.
	1.5.2. Which of the following procedures for responding to security breaches for both electronic and paper-based systems are included in written procedures? (Please elect all that apply.) 1. Roles and responsibilities of staff for managing security breaches 2. Preparing to handle security breaches by rehearsing potential responses 3. Detecting security breaches when they occur and determining the type of incident and appropriate response 4. Analyzing available information related to the security breach to determine the type of incident and the appropriate response 5. Prioritizing the response to the security breach based on criticality of the affected resources (including notifying appropriate individuals)	

Category	Questions	Instruction
	6. Containing the security breach (e.g. shutting down a system, disconnecting it from a wired or wireless network, disconnecting its modem cable or disabling certain functions) 7. Eradicating the security breach and removing the effects of the cause (such as disabling compromised user accounts) 8. Recovering from the security breach and restoring systems to normal operations 9. Acquiring, preserving, securing and documenting evidence related to the security breach 10. Creating additional security checks to prevent similar security breaches 99. Other (please specify):	
	1.5.3. Are electronic systems monitored to detect potential or actual security breaches? 1. Yes 2. No	IF "2," GO TO QUESTION 38.
	1.5.4. How often are electronic systems monitored? 1. Real time, continuous 2. Daily 3. Weekly 4. When a security breach is suspected 99. Other (please specify):	
1.6. Conducting risk assessments Purpose: to determine the presence and scheduling of risk assessments documented in the policy.	1.6.1. Are risk assessments conducted? 1. Yes 2. No	IF "2," GO TO QUESTION 41.
	1.6.2. How often are risk assessments performed? 1. Every year 2. Every 1–2 years 3. Every 2+ years 99. Other (please specify):	
	1.6.3. Which of the following steps are performed during the risk assessment process? (Please select all that apply.) 1. System characterization: identify the boundaries of the IT system, along with the resources and information that constitute the system. 2. Threat identification: identify the potential threat sources and compile a threat statement that lists the potential threat sources that are applicable to the IT system being evaluated. 3. Vulnerability identification: develop a list of the system flaws or weaknesses that could be exploited by the potential threat sources. 4. Control analysis: analyze the controls that have been implemented (or are planned for implementation) by the organization as part of efforts to minimize or eliminate the likelihood of an exploitation of a system vulnerability. 5. Likelihood determination: derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exploited. 6. Impact analysis: determine the adverse impact resulting from the successful exploitation of a vulnerability.	

Category	Questions	Instruction
	7. Risk determination: assess the level of risk to the IT system. 8. Control recommendations: provide controls that could mitigate or eliminate the identified risks. 9. Results documentation: document results in an official report or briefing. 99. Other (please specify):	
1.7. Connectivity to other networks to determine if the policy sufficiently details connectivity to other networks.	1.7.1. Are computers permitted to be connected to more than one network? 1. Yes 2. No 1.7.2. Which of the following methods are used to connect computers to more than one network? (Please select all that apply.) 1. Virtual private network (VPN) 2. Remote desktop software that uses virtual network computing (VNC) and/or remote frame buffer protocol (RFB) 3. Remote desktop software that uses remote desktop protocol (RDP) 4. Remote desktop software that uses another protocol (AIP, NX, X11 or proprietary) or the protocol is unknown 5. Multiple network interface cards (NIC) 6. Network bridge 99. Other (please specify): 1.7.3. Is there built-in encryption on the methods used to connect to other networks? 1. Yes 2. No	IF "2," GO TO QUESTION 44.

2. Data Collection

Category	Questions	Instruction
2.1. Data collection mechanisms to determine data collection methods, content and quality regarding personally identifiable health data.	2.1.1. Which of the following data are received? (Please select all that apply.) 1. Personally identifiable health data 2. De-identified health data 3. Non-identifiable health data 4. Aggregated data 5. Non-personal data 2.1.2. What types of data collection methods are used? 1. Paper-based only 2. Computer-based only 3. Both 99. Other (please specify): 2.1.3. Do you have an updated list of databases containing personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 48.

Category	Questions	Instruction
	2.1.4. Do you have an updated inventory of computers and mobile devices containing these databases or any other personally identifiable health data? 1. Yes (v) 2. No	
	2.1.5. Which of the following personally identifiable health data elements are collected as part of providing individual health care? (Please select all that apply.) 1. Name 2. Date of birth 3. Government-issued identification number (such as national identification number, welfare number, driver's license number or passport number) 4. Facility-issued identification number (including medical record numbers) 5. Photographic identifiers (such as photos on a driver's license or passport) 6. Biometric identifiers (such as a fingerprint) 7. Mailing address 8. Phone numbers 9. Medical notes 10. E-mail address 11. Employment information 12. None 99. Other (please specify):	
	2.1.6. Which of the following personally identifiable health data elements are collected for public health practice? (Please select all that apply.) 1. Name 2. Date of birth 3. Government-issued identification number (such as national indentification number, welfare number, driver's license number or passport number) 4. Facility-issued identification number (including medical record numbers) 5. Photographic identifiers (such as photos on a driver's license or passport) 6. Biometric identifiers (such as a fingerprint) 7. Mailing address 8. Phone numbers 9. Medical notes 10. E-mail address 11. Employment information 12. None 99. Other (please specify):	
	2.1.7. When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose? 1. Yes 2. No	

Category	Questions	Instruction
	2.1.8. Do the data collection methods capture the origin of how, when and by whom data were collected, modified or deleted in order to protect against improper modification (falsification) or destruction? (Please select all that apply.) 1. How data were collected, modified or deleted 2. When data were collected, modified or deleted 3. Who collected, modified or deleted data 4. No 99. Other (please specify):	
	2.1.9. How often are data reviewed for accuracy? 1. Daily 2. Weekly 3. Monthly 4. Annually 5. Never 99. Other (please specify):	IF "5," GO TO QUESTION 55.
	2.1.10. What methods are used to review data for accuracy? (Please select all that apply.) 1. Computerized verification during data entry 2. Computerized verification during data collection 3. Computerized analysis of data files (i.e. outlier analysis) 4. Manual review of individual data records 5. No method in place to review data 99. Other (please specify):	IF "5," GO TO QUESTION 55.
	2.1.11. Are there documented processes for handling data inaccuracies? 1. No 2. Yes, for reporting inaccuracies (v) 3. Yes, for correcting inaccuracies (v) 4. Yes, for both reporting and correcting inaccuracies (v)	
	2.1.12. For personally identifiable health data that will be transferred, are personal identifiers removed before transfer for any of the following purposes? (Please select all that apply.) 1. Individual health care 2. Public health practice (including monitoring and evaluation) 3. Human subject research (with consent) 4. Public use 5. Not specified 99. Other (please specify):	IF "5," GO TO QUESTION 60.
	2.1.13. When data are transferred, where are personal identifiers removed from the data? 1. At the data collection site before transferring 2. At the data warehouse before further transfer 99. Other (please specify):	

Category	Questions	Instruction
	2.1.14. How are the personal identifiers removed? 1. By removing a specified list of identifiable fields 2. By creating a non-identifiable key that is constructed from identifiable data 99. Other (please specify): 2.1.15. How are the keys for the personal identifiers stored? 1. Electronically (v) 2. Hard copy (v) 99. Other (please specify): 2.1.16. Is access restricted to the files containing keys? 1. Yes, with user identification and password or lock and key 2. No, access is not restricted 99. Other (please specify):	
2.2 Physical security measures at site Purpose: to determine the physical precautions taken to secure personally identifiable health data.	2.2.1. Which of the following physical measures are used for protecting patient privacy while collecting information? (Please select all that apply.) 1. Minimize exchange of information verbally 2. Use a partition or curtain in open rooms (v) 3. Use of a separate room with a soundproof barrier (v) 4. Use of window films that provide visual privacy(v) 5. Use of cover sheets on paper documents to provide visual privacy(v) 6. Use of a computer screen guard that provides visual privacy(v) 7. Use of a work space only accessible to authorized staff(v) 8. No measures in place 99. Other (please specify): 2.2.2. What other physical precautions are taken to secure personally identifiable health data? (Please select all the apply.) 1. Workspaces, cabinets, paper copies and computers with personally identifiable information are located within a secure area with no public access. (v) 2. Sensitive documents are stored in cabinets and locked. (v) 3. Only authorized personnel can access these cabinets and computers. (v) 99. Other (please specify):	

3. Data Storage		
Category	**Questions**	**Instruction**
3.1 Policy Purpose: to determine if there are clear guidelines on data archiving within the policy.	3.1.1. Do you have written guidelines or standard operating procedures (SOPs) on archiving data? 1. Yes (v) 2. No 3.1.2. Which of the following are included in the guidelines/SOPs on archiving data? (Please select all that apply.) 1. How often data must be archived(v) 2. Approved storage locations of archived data(v) 3. Approved media for archiving data(v) 4. Roles that are responsible for archiving data 99. Other (please specify):	IF "2," GO TO QUESTION 64.
3.2 Physical security storage measures Purpose: to determine the physical precautions taken to secure personally identifiable health data in storage.	3.2.1. Are buildings and rooms containing personally identifiable health data locked for both electronic and paper documents? 1. Yes(v) 2. No 3.2.2. What physical security controls are in place to prevent unauthorized access to buildings and rooms containing personally identifiable health data? 1. Window locks(v) 2. Security guard or other authorized staff control access(v) 3. Video monitoring(v) 4. Bars/grills for doors or windows(v) 5. Alarm system(v) 6. No physical security control measures are in place 99. Other (please specify): 3.2.3. Are records maintained that indicate which staff are authorized to access buildings and rooms containing personally identifiable health data? 1. Yes (v) 2. No 3.2.4. Do staff need a user identifier and password to gain access to databases and documents containing personally identifiable health data? 1. Yes(v) 2. No 3.2.5. Are staff required to wear identification badges when accessing and working in rooms containing personally identifiable health data? 1. Yes (v) 2. No 3.2.6. Are records maintained that indicate the date and time that staff accessed rooms containing personally identifiable health data? 1. Yes(v) 2. No	

Category	Questions	Instruction
	3.2.7. The location used for storing paper-based confidential information is safe from the following (please select all that apply): 1. Risk of fire(v) 2. Risk of flooding(v) 3. Risk of animal or insect damage (such as mice or termites) (v) 4. Power interruptions(v) 5. Natural disasters(v) 6. Theft(v) 7. None of the above	
	3.2.8. The location used for storing computers containing confidential information is safe from the following (please select all that apply): 1. Risk of fire(v) 2. Risk of flooding(v) 3. Risk of animal damage (such as rodents) (v) 4. Power interruptions(v) 5. Natural disasters(v) 6. Theft(v) 7. None of the above	
	3.2.9. Are persons who are not authorized to access personally identifiable health data allowed to access rooms that contain the records or data? 1. Yes 2. No	IF "2," GO TO QUESTION 74.
	3.2.10. Are persons who are not authorized to access personally identifiable health data required to provide proper identification to authorized staff before being granted access to rooms containing personally identifiable health data? 1. Yes 2. No	
3.3 Inventory management Purpose: to determine if there is clear guidance within the policy regarding the migration of data to newer technologies.	3.3.1. What types of identification tags are applied to equipment? (Please select all that apply.) 1. Temporary adhesive labels that are not tamper-proof or tamper-evident(v) 2. Permanent or semi-permanent adhesive labels that are tamper-proof or tamper-evident(v) 3. Engraved metal plates attached to equipment(v) 4. Identification is engraved directly on the equipment surface(v) 5. None 99. Other (please specify):	
	3.3.2. How are the facility's inventory records for equipment maintained? (Please select all that apply.) 1. Handwritten or typed paper documents (v) 2. Spreadsheet software(v) 3. Database software(v) 4. Asset management software(v) 5. No inventory records are maintained 99. Other (please specify):	IF "5," GO TO QUESTION 77.

Category	Questions	Instruction
	3.3.3. How often are the facility's inventory records updated? 1. Continuously—items are tagged and entered in the inventory record immediately upon receipt. 2. Items are tagged and entered in the inventory record within 1 month of receipt. 3. Items are tagged and entered in the inventory record after more than 1 month of receipt. 4. Regularly, but not on a specific schedule. 5. Never. 99. Other (please specify):	

4. Data Backup

Category	Questions	Instruction
4.1 Computers and laptops Purpose: to determine the physical precautions taken to backup personally identifiable health data on computers.	4.1.1. Are patient data on desktop and laptop computers backed up? 1. Yes 2. No	IF "2," GO TO QUESTION 85.
	4.1.2. How often are patient data on desktop and laptop computers backed up? 1. Immediately when the data are revised 2. Daily 3. Weekly 4. As needed or requested 99. Other (please specify):	
	4.1.3. Where are backup copies stored? (Please select all that apply.) 1. On the same computer on which data are collected 2. On a central server 3. In cloud-based storage 4. On removable media	
	4.1.4. Are backup patient data from desktop and laptop computers encrypted? 1. Yes, during the backup process 2. Yes, before backup process 3. No 99. Other (please specify):	
	4.1.5. When removable media are used for backup, are the removable media encrypted? 1. Yes 2. No	
	4.1.6. How often are backup media for desktop and laptop computers containing patient data transferred to an off-site storage facility? 1. Daily 2. Weekly 3. Monthly	

Category	Questions	Instruction
	4. Quarterly 5. Annually 6. Never 99. Other (please specify): 4.1.7 Are your backups rotated: ie. are you backing up the backup? 1. Yes 2. No 4.1.8 How often are stored data migrated when newer storage media become available? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular migration schedule 7. Never	
4.2 Servers Purpose: to determine the physical precautions taken to backup personally identifiable health data on computers.	4.2.1. Are patient data on servers backed up? 1. Yes, by the system administrator as needed or requested 2. Yes, by the system administrator on a regular schedule 3. Yes, using an automated, scheduled process 4. No 99. Other (please specify): 4.2.2. Are data periodically migrated to newer backup media as technology changes provide newer methods of storage? 1. Yes 2. No 4.2.3. Are data backups migrated when newer storage media become available? 1. Yes 2. No 4.2.4. How often are stored data migrated when newer storage media become available? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular migration schedule 7. Never 4.2.5. Are backup media regularly tested to ensure that they can be relied upon in case of emergencies? 1. Yes 2. No	IF "4," GO TO QUESTION 90. IF "2," GO TO QUESTION 89. IF "2," GO TO QUESTION 89.

Category	Questions	Instruction
4.3 Audit logs Purpose: to determine the use, review and backup of audit logs	4.3.1. Are audit logs created to assist in recording all system transactions? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 100.
	4.3.2. Are audit logs stored separately from the rest of the system that they are monitoring? 1. Yes 2. No	
	4.3.3. Which of the following data elements are recorded in the audit log? (Please select all that apply.) 1. IP address or MAC address of computer from which action originated 2. User identifier 3. Dates, times and details of key events (e.g. log on and log off) 4. Records of successful and rejected system access attempts 5. Activation and de-activation of protection systems (such as antivirus systems and intrusion detection systems) 6. Files accessed and the kind of access 7. Record identifier 99. Other (please specify)	
	4.3.4. How often is the audit log reviewed? 1. Real-time, continuous 2. Daily 3. Weekly 4. Only when needed or requested 5. Never 99. Other (please specify):	IF "5," GO TO QUESTION 95.
	4.3.5. Who reviews the audit log? (Please select all that apply.) 1. Data management staff 2. Clinical staff 3. Confidentiality and security officer/information security manager 4. Database administrator 5. Independent auditor 99. Other (please specify):	
	4.3.6. Are audit logs backed up? 1. Yes 2. No	IF "2," GO TO QUESTION 100.
	4.3.7. How are audit logs backed up? 1. By the system administrator as needed or requested 2. By the system administrator on a regular schedule 3. Using an automated, scheduled process 99. Other (please specify):	

Category	Questions	Instruction
	4.3.8. How often are audit logs backed up? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 99. Other (please specify):	
	4.3.9. How often are audit logs of back-up data transferred to an offsite storage facility? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 99. Other (please specify):	IF "4," GO TO QUESTION 100.
	4.3.10. Are the offsite storage facility for back-up media for audit logs locked? 1. Yes 2. No	

5. xxx

Category	Questions	Instruction
5.1 Policy Purpose: to determine if access to data is clearly defined within the policy and if security controls are independently validated.	5.1.1. Access to data has been defined for the following staff members (please select all that apply): 1. Staff access not defined 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Other health professionals 6. Information technology staff (including data clerks, analysts, managers and programmers) 7. Administrative staff 8. Professional service providers 9. Volunteers 10. Academic or other researchers 11. Cleaners, security guards and other providers of support services 12. Bilateral donor staff 13. Multilateral institution staff (e.g. staff from the Global Fund to Fight AIDS, Tuberculosis and Malaria) 99. Other (please specify):	IF "1," GO TO QUESTION 103.
	5.1.2. Are system security controls independently tested and validated? 1. Yes 2. No	

Category	Questions	Instruction
5.2 User access Purpose: to determine if levels of access are specified for using data for different purposes.	5.2.1 For roles that are defined as having access to data, are levels of access specified for the following types of data use?(Please select all that apply.) 1. Individual health care 2. Public health practice (including monitoring and evaluation) 3. Human subject research (with consent) 4. Exceptional statutory purposes 5. Public use 6. Not specified 99. Other (please specify):	IF "2," GO TO QUESTION 64.
5.3 Passwords Purpose: to determine if the policy requires user sessions to be locked after certain periods of inactivity.	5.3.1. Do staff need a user identifier and password to gain access to a computer? 1. Yes 2. No 3. Not applicable (non-computer situation) 5.3.2. How are user identifiers generated? 1. By the computer operating system 2. By the computer software application 3. By a system administrator, with user identifier composition rules 4. By a system administrator, without user identifier composition rules 5. By information security manager 99. Other (please specify): 5.3.3. Is the password file encrypted? 1. Yes 2. No 5.3.4. Are there established procedures for verifying the identity of a user prior to providing a new, replacement or temporary password? 1. Yes 2. No 5.3.5. How are user identifiers and passwords issued to users? (Please select all that apply.) 1. In person 2. By telephone 3. Through e-mail 99. Other (please specify): 5.3.6. After what period of inactivity are user identifiers disabled? 1. 14 days 2. 30 days 3. 60 days 4. 90 days 5. 180 days 6. 360 days 7. Not disabled 99. Other (please specify):	IF "3," GO TO QUESTION 120.

Category	Questions	Instruction
	5.3.7. When a staff member's employment is terminated, are there procedures for revoking access to personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 111.
	5.3.8. When a staff member's employment is terminated, when are data access privileges revoked? 1. Immediately upon termination via an automated process 2. Within a week 3. Within a month 4. Never 99. Other (please specify):	
	5.3.9 Are user sessions automatically locked after a certain specified period of inactivity for software applications that contain personally identifiable health data? 1. Yes 2. No	
	5.3.10. What is the minimum password length? 1. 6 or fewer characters 2. 7–8 characters 3. 9 or more characters 4. No minimum password length	
	5.3.11. Does the system enforce specifications for passwords, such as a combination of a minimum number of lower-case letters, upper-case letters, numbers and special characters? 1. Yes 2. No	
	5.3.12. Are passwords masked when entered into computer applications? 1. Yes 2. No	
	5.3.13. When a staff member's employment is terminated, when are data access privileges revoked? 1. Less than 1 day 2. 1–7 days 3. 8–14 days 4. 15–30 days 5. More than 30 days 6. No minimum time	
	5.3.14. Is a password reset mechanism established for computers and computer software applications that contain personally identifiable health data? 1. Yes—upon password expiration only 2. Yes—can be initiated by the user before the password expires (such as at the first indication of a possible security breach) 3. No	IF "3," GO TO QUESTION 119.

Category	Questions	Instruction
	5.3.15. How is the reset password provided to the user? (Please select all that apply.) 1. Through e-mail 2. By telephone 3. In person 99. Other (please specify):	
	5.3.16. Is reusing passwords prohibited for a specific number of generations (i.e. a certain number of previous passwords cannot be reused)? 1. Yes 2. No	IF "2," GO TO QUESTION 100.
	5.3.17. Are biometrics or other technologies (e.g. fingerprint verification, signature verification, hardware tokens or smart cards) being used for user identification and authentication? 1. Yes 2. No	

6. Data Release

Category	Questions	Instruction
6.1 Policy Purpose: to determine if the policy contains a detailed release section.	6.1.1. Do you have written guidelines for the data release policy? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 122.
	6.1.2. Which of the following information is included in the data release policy? (Please select all that apply.) 1. Class of use for which data may be released (e.g. individual health care or public health practice) (v) 2. Specific data elements that may be released(v) 3. Entities and organizations to whom data may be released(v) 4. Requirements for how recipients will protect the confidentiality of received data(v) 5. Specifications for time limitations on use of released data(v) 6. Data quality standards that must be met prior to data release(v) 7. Clearly defined individual(s) who are authorized to release data(v) 8. Clear procedures for handling data requests that are not covered under the data release policy(v) 99. Other (please specify):	

Category	Questions	Instruction
6.2 Mandatory requirements for data release Purpose: to determine the extent to which the policy covers requirements and conditions in terms of the release of data.	6.2.1. According to the Data Confidentiality and Security Policy, for what purpose may personally identifiable health data be released? (Please select all that apply.) 1. Not specified in the Data Confidentiality and Security Policy 2. Individual health care(v) 3. Public health practice (including monitoring and evaluation) (v) 4. Human subject research (with consent) (v) 5. Exceptional statutory purposes(v) 6. Public use(v) 99. Other (please specify):	IF "1," GO TO QUESTION 135. IF "2," GO TO QUESTION 123. IF "3," GO TO QUESTION 126. IF "4," GO TO QUESTION 129. IF "5," GO TO QUESTION 132.
	6.2.2. Under what circumstances is the release of personally identifiable health data for individual health care permitted? (Please select all that apply.) 1. Authorized transfer of a patient across facilities(v) 2. Authorized transfer between clinical services(v) 3. Request from patient(v) 4. Not specified 99. Other (please specify):	ANSWER ONLY IF #2 WAS CHOSEN FOR QUESTION 122.
	6.2.3. Which of the following conditions must be met before releasing personally identifiable health data for individual health care? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released(v) 5. Acquisition of formal approval for the data release(v) 6. Not specified 99. Other (please specify):	
	6.2.4. Which of the following conditions must be met by the organization receiving personally identifiable health data in order for data to be release for individual health care? (Please select all that apply.) 1. Signed confidentiality statements from recipient facility staff(v) 2. Documentation of security training of recipient facility staff(v) 3. Evidence of security assessment (eg. review of procedural, electronic 4. or physical security controls) (v) Documentation of internal steering group review and approval(v) 5. Agreement by the recipient to destroy information after the purpose of the data release has been fulfilled(v) 6. Assurance that the minimum amount of data needed to satisfy the purpose is being requested(v) 7. Not specified 99. Other (please specify):	
	6.2.5. Under what circumstances is the release of personally identifiable health data for public health practice permitted? (Please select all that apply.) 1. Not specified 2. Regulation of public health policy(v) 3. Public health program planning(v) 4. National reporting(v) 99. Other (please specify):	ANSWER ONLY IF #3 WAS CHOSEN FOR QUESTION 122.

Category	Questions	Instruction
	6.2.6. Which of the following conditions must be met before releasing personally identifiable health data for public health practice? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released(v) 5. Acquisition of formal approval for the data release(v) 6. Not specified 99. Other (please specify):	
	6.2.7. What requirements must be met by the organization receiving personally identifiable health data in order for data release to be authorized for public health practice? (Please select all that apply.) 1. Signed confidentiality statements(v) 2. Documentation of security training(v) 3. Security assessment (review of procedural, electronic and physical security controls) (v) 4. Review and approval by the internal steering group(v) 5. Agreement to destroy information after purpose of data release has been fulfilled(v) 6. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 7. Not specified 99. Other (please specify):	
	6.2.8. When is the release of personally identifiable health data for human subject research (with consent) permitted? (Please select all that apply.) 1. Ethics committee or institutional review board approval (v) 2. Not specified 99. Other (please specify):	ANSWER ONLY IF #4 WAS CHOSEN FOR QUESTION 122.
	6.2.9. Which of the following conditions must be met before releasing personally identifiable health data for human subject research (with consent)? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Acquisition of formal approval for the data release(v) 5. Not specified 99. Other (please specify):	ANSWER ONLY IF #4 WAS CHOSEN FOR QUESTION 122.
	2.2.10. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for human subject research (with consent)? (Please select all that apply.) 1. Signed confidentiality statements(v) 2. Documentation of security training(v) 3. Security assessment (review of procedural, electronic, and physical security controls) (v) 4. Proof of ethics or institutional review board approval(v) 5. Review of a scientific protocol by an internal steering group(v)	

Category	Questions	Instruction
	6. Agreement to destroy information after purpose of data release has been fulfilled(v) 7. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 8. Not specified 99. Other (please specify)	
	6.2.11. When is the release of personally identifiable health data for exceptional statutory purposes permitted? (Please select all that apply.) 1. Court order(v) 2. Subpoena(v) 3. Request from law enforcement agency(v) 4. Request from prosecuting attorneys(v) 5. Request from defense attorneys(v) 6. Request from a health-care practitioner providing treatment for a health-care worker or a law enforcement officer because of a medically significant exposure to blood or body fluids(v) 7. Not specified 99. Other (please specify):	ANSWER ONLY IF #5 WAS CHOSEN FOR QUESTION 122.
	6.2.12. Which of the following conditions must be met before releasing personally identifiable health data for exceptional statutory purposes?(Please select all that apply.) 1. Review of data for accuracy(v) 2. Removal of direct patient identifiers from released records(v) 3. Acquisition of formal approval for the data release(v) 4. Not specified 99. Other (please specify):	
	6.2.13. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for exceptional statutory purposes? (Please select all that apply.) 1. Review and approval of request by legal counsel(v) 2. Review and approval of request by confidentiality and security officer (or equivalent official) (v) 3. Review and approval by internal steering group(v) 4. Signed confidentiality statements from persons receiving data(v) 5. Documentation of security training(v) 6. Medical record release signed by patient(v) 7. Medical record release signed by the patient's attorney(v) 8. Security assessment (review of procedural, electronic and physical security controls) (v) 9. Agreement to destroy information after purpose of data release has been fulfilled(v) 10. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 11. Not specified 99. Other (please specify):	ANSWER ONLY IF #5 WAS CHOSEN FOR QUESTION 122.

7. Transmission Security		
Category	**Questions**	**Instruction**
7.1 Routers Purpose: to determine the extent to which the policy covers router usage.	7.1.1. Is a router that controls information flow between the local area network and the Internet or other networks installed? 1. Yes 2. No 7.1.2. Which of the following are characteristics of the router configuration? (Please select all that apply.) 1. Enables password protection 2. Limits router access to named users or user groups through command privilege levels 3. Displays banner indicating ownership of the system and that unauthorized access is prohibited 4. Disables unnecessary services 5. Prevents internal IP addresses from being revealed 6. Enables logging of access, including source IP address and the date, time and description of access 7. Accesses lists that contain information to deny or allow traffic by IP address or group 8. Turns off incoming IP-directed broadcasts (IP packets that are sent to a particular network or group of networks) 7.1.3. How often are router logs reviewed? 1. Daily 2. Weekly 3. Monthly 4. Quarterly 5. Never 6. As needed or requested 99. Other (please specify): 7.1.4. Who reviews and provides oversight of router logs? (Please select all that apply.) 1. Internal IT staff, manually 2. Internal IT staff, using log analysis software 3. Independent auditor 99. Other (please specify):	IF "2," GO TO QUESTION 139.
7.2 Firewalls Purpose: to determine the extent to which the policy covers router usage.	7.2.1. Are firewalls installed on computers, servers and networks? 1. Yes 2. No	IF "2," GO TO QUESTION 144.

Category	Questions	Instruction
	7.2.2. Which characteristics do the installed firewalls possess? (Please select all that apply.) 1. Apply a security level in accordance with the type of network 2. Block intrusion attempts (from wireless networks [Wi-Fi], hackers, etc.) 3. Specify which software application can access the network or the Internet 4. Block access of specified software applications 5. Offer outbound protection to control information that leaves the computer 6. Others (please specify): 7.2.3. How often are computers, servers and network firewall logs reviewed? 1. Real-time, continuous 2. Daily 3. Weekly 4. Monthly 5. Quarterly 6. As needed or requested 7. Never 7.2.4. Who reviews computer, server or network firewall logs? (Please select all that apply.) 1. Internal IT staff, manually 2. Internal IT staff, using log analysis software 3. Independent auditor 4. No one is assigned to review firewall logs 99. Other (please specify): 7.2.5. Which of the following are included in computer, server or network firewall audits? (Please select all that apply.) 1. Review rule sets 2. Review accounts 3. Ensure that logging is enabled and that the logs are reviewed periodically 4. Ensure that the latest patches and updates are tested and installed 5. Ensure that specific IP addresses are blocked 6. Ensure that specific ports are blocked 7. Perform vulnerability and penetration testing 8. No firewall audits are performed 99. Other (please specify):	
7.3 Antivirus on computers Purpose: to determine the extent to which the policy requires electronic systems containing personally identifiable health data to use antivirus software.	7.3.1. Is antivirus software installed on desktop and laptop computers containing personally identifiable health data? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 146.

Category	Questions	Instruction
	7.3.2. How often is antivirus software updated on desktop or laptop computers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. Never 99. Other (please specify): 7.3.3. When are individual files scanned on desktop or laptop computers containing personally identifiable health data? (Please select all that apply.) 1. As scheduled 2. When moved, copied, opened or saved 3. When downloaded 4. Only as part of a scheduled system scan 99. Other (please specify): 7.3.4. How often is the operating system scanned by antivirus software on desktop and laptop computers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify): 7.3.5. How often are removable media connected to desktop or laptop computers that contain personally identifiable health data scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	
7.4 Antivirus on servers Purpose: to determine the extent to which the policy requires servers containing personally identifiable health data to use antivirus software.	7.4.1. Is antivirus software installed on servers? 1. Yes(v) 2. No 7.4.2. How often is antivirus software updated on servers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	IF "2," GO TO QUESTION 154.

Category	Questions	Instruction
	7.4.3. When are individual files scanned on servers containing personally identifiable health data? 1. As scheduled 2. When moved, copied, opened or saved 3. When downloaded 4. Only as part of a scheduled system scan 99. Other (please specify): 7.4.4. How often is the operating system on servers containing personally identifiable health data scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify): 7.4.5. How often are all drives containing personally identifiable health data and connected to server(s) scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	
7.5 Transfer of paper data Purpose: to determine the physical precautions taken to store and secure personally identifiable health data in paper format.	7.5.1. Does your site store paper records containing personally identifiable health data? 1. Yes (v) 2. No 7.5.2. How often are data on paper transferred to an off-site storage facility? 1. Daily 2. Weekly 3. Monthly 4. Quarterly 5. Annually 6. Never 99. Other (please specify): 7.5.3. Which of the following security controls are implemented to ensure the security of paper-based data when they are being transferred within a facility or to an off-site storage facility? (Please select all that apply.) 1. A list of approved transport providers (such as site staff, courier services, and government and private postal services) (v) 2. A locked container for transferring or transporting the paper-based data(v) 3. A tamper-proof seal for the container used for transferring or transporting paper-based data(v)	IF "2," GO TO QUESTION 156.

Category	Questions	Instruction
	4. A transfer log that identifies the records being transferred, the sender, the recipient, the delivery person, and all relevant dates and times(v) 5. Authentication of the identity of the recipient on delivery(v) 6. Verification of successful delivery(v) 99. Other (please specify):	
7.6 Transmission of electronic data Purpose: to determine the physical precautions taken to transfer personally identifiable health data electronically	7.6.1. Does your site store electronic records containing personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 164.
	7.6.2. What methods or media are used to transfer electronic data within a site? (Please select all that apply.) 1. Intranet, local area network or wide area network 2. E-mail 3. Internet (via web browser) 4. File transfer protocol (FTP) 5. Tape 6. Optical media (CD or DVD) 7. Flash drive and/or memory stick 8. External hard drive 9. Smart card 99. Other (please specify):	
	7.6.3. What controls are implemented to ensure the security of electronic data when they are being moved within a site? (Please select all that apply.) (Please select all that apply.) 1. Authentication of the identities of the sender and receiver before information transfer 2. Password-protected data files (with or without encryption) 3. Encryption of the information during transfer 4. Post-transfer verification of the appropriate and successful transfer of information 5. None of the above 99. Other (please specify):	
	7.6.4. What methods or media are used to transfer electronic data between sites? 1. Int**ranet, local area network and wide area network** **2. E-mail** **3. Internet (via web browser)** **4. File transfer protocol (FTP)** **5. Tape** **6. Optical media (CD or DVD)** **7. Flash drive and/or memory stick** **8. External hard drive** **9. Smart card** **10. None of the above** **99.** Other (please specify):	

Category	Questions	Instruction
	7.6.5. For which of the following transfer methods or media and transfer types is encryption used when data are in transit within the site? (Please select all that apply.) 1. Not used 2. Intranet, local area network and wide-area network 3. E-mail 4. Internet (via web browser) 5. File transfer protocol (FTP) 6. Tape 7. Optical media (CD or DVD) 8. Flash drive and/or data stick 9. External hard drive 10. Smart card 99. Other (please specify) 7.6.6. Which controls are implemented to ensure the security of electronic data when they are being moved between sites? (Please select all that apply.) 1. Authentication of the identities of the sender and receiver before information transfer 2. Password-protected data files (with or without encryption) 3. Encryption of the information during transfer (such as SSLs) 4. Post-transfer verification of the appropriate and successful transfer 5. of information 99. Other (please specify): 7.6.7. When transferring data within and between sites, which methods are used to authenticate sending and receiving parties? (Please select all that apply.) 1. Sending and receiving parties are not authenticated 2. Two-factor authentication (TFA) 3. Public key infrastructure (PKI) 99. Other (please specify):	
7.7 Mail handling Purpose: to determine the procedures used for handling incoming mail at sites involved with personally identifiable health data.	7.7.1. Which of the following procedures are used for handling incoming mail at sites involved with personally identifiable health data? (Please select all that apply.) 1. All mail marked "confidential" must be checked by authorized personnel only and kept in a secured location until it is processed. 2. Mail marked "confidential" should only be opened by the addressee. 3. The person in charge of receiving the confidential mail must record the receipt of all mail into a log book by the end of each day; each log entry must note the name of the sender, what was received and the date of receipt. 4. The person in charge of receiving the confidential mail must contact the sender on the day of receipt with notification that the mail was received. 5. No procedures are in place. 99. Other (please specify):	

8. Data disposal		
Category	**Questions**	**Instruction**
8.1 Data disposal Purpose: to determine the extent to which the policy covers secure retirement and disposal of paper-based data.	8.1.1. Do you have written guidelines for the secure disposal and destruction of data? 1. Yes(v) 2. No	
	8.1.2. Do you maintain a data retirement schedule for destroying records when they are no longer needed? 1. Yes(v) 2. No	IF "2," GO TO 168.
	8.1.3. Which types of records are addressed in the data retirement schedule? (Please select all that apply.) 1. Paper records 2. Backup copies of paper records 3. Electronic records 4. Backup copies of electronic records 99. Other (please specify):	
	8.1.4. Which method(s) of destruction or disposal are used? (Please select all that apply.) 1. Burning 2. Demagnetizing 3. Overwriting 4. Pulping 5. Pulverizing, crushing or grinding 6. Reformatting 7. Shredding 99. Other (please specify):	
	8.1.5. Do you maintain documentation of the secure destruction or disposal of records (such as a certification or verification of destruction)? 1. Yes (v) 2. No	IF "2," THE FACILITY-LEVEL ASSESSMENT IS COMPLETE.

Category	Questions	Instruction
	8.1.6. What information must be included in documentation of the secure destruction or disposal of records? (Please select all that apply.) 1. Organization 2. Organization contact 3. Date of destruction or disposal 4. Name and signature of person who authorized the destruction or disposal of data 5. Description of information destroyed or disposed of, including type (paper or electronic) 6. Time period covered by the records to be destroyed 7. Method of destruction or disposal (e.g. burning, demagnetizing, overwriting, pulping, pulverizing, reformatting or shredding) 8. Name and signature of person who destroyed or disposed of data 9. Name and signature of person who witnessed destruction or disposal of data 10. Copy of contract with outside firm handling the destruction or disposal of data 99. Other (please specify):	

Data warehouse-level assessment tool

The following data warehouse-level questions are to determine the security, confidentiality and appropriate use (including sharing) of data collected by health programmes.

The questions are grouped into eight sections:

- Governance and policy.
- Data collection.
- Data storage.
- Data backup.
- Authorization and access control.
- Data release.
- Transmission security.
- Data disposal.

A brief purpose statement introduces each section. It is followed by a set of questions to be answered.

Table 3

Recommended data warehouse-level questions

1. Governance and Policy		
Category	**Questions**	**Instruction**
1.1 Legislation: To determine the existence and extent of legislation covering the use of personally identifiable health data for public health practice and research.	1.1.1. Do you have clearly defined roles and access levels for all persons with authorized access to personally identifiable data? 1. Yes (v) 2. No	
	1.1.2. Do you have clearly defined standard procedures or methods that must be followed when accessing personally identifiable data? 1. Yes (v) 2. No	
	1.1.3. Does a written policy document regarding the requirements for ensuring the confidentiality and security of personally identifiable health data exist in this country (referred to as the "Data Confidentiality and Security Policy" or "the Policy")? 1. Yes (If written documentation is determined to exist, identify the appropriate staff to answer this module) (v) 2. No, but a policy is in the process of development 3. No, but various informal policies exist 4. No, we do not have any policy or written guidelines	IF "2," "3" OR "4," GO TO QUESTION 6.
	1.1.4. Is the Data Confidentiality and Security Policy readily accessible to all staff members who have access to confidential individual-level data? (By "readily accessible," we mean that they can easily access the policy online or in hard copy while at work.) 1. Yes 2. No	
	1.1.5. To which stakeholders or organizations is the Data Confidentiality and Security Policy document distributed? (Please select all that apply.) 1. Staff who request it 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Health-care volunteers	

Category	Questions	Instruction
	6. Other health professionals 7. Information technology staff (including data entry staff, analysts, managers and programmers) 8. Administrative staff 9. Cleaners, security guards and other providers of support services 10. Policy document is not distributed 11. Health records staff 99. Other (please specify): 1.1.6. In which of the following formats is the Data Confidentiality and Security Policy document available for reference by staff? 1. Printed hard copies 2. Electronic, distributed via e-mail 3. Electronic, distributed via CD or other media 4. Electronic, available on the Internet (please specify the URL): 99. Other, specify:	
1.2 Governance structure Purpose – To determine the governance structure that is in place to provide oversight for the appropriate collection, use, and dissemination of data, including regular review of the policy document and security practices.	1.2.1. Is there a local governance structure (e.g. steering committee/ advisory board) in place to provide oversight for the appropriate collection, use and dissemination of data, including regular review of the policy document and security practices? 1. Yes 2. No 99. Other (please specify): 1.2.2. How often does the steering committee or advisory board meet? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular meeting schedule 1.2.3. Which uses of personally identifiable information are covered by your local guidelines on the security and confidentiality of data? (Please select all that apply.) 1. Individual health care 2. Public health practice (including monitoring and evaluation) 3. Human subject research (with consent) 4. Exceptional statutory purposes 5. Not specified 99. Other (please specify): 1.2.4. Is information security and its management reviewed at regular intervals? 1. Yes 2. No	IF "2," GO TO QUESTION 9.
1.3 Review of security practices Purpose – To determine the security practice and review as documented in the policy	1.3.1. Are security practices reviewed by independent auditors? 1. Yes 2. No	IF "2," GO TO QUESTION 13.

Category	Questions	Instruction
	1.3.2. How often do independent auditors review security practices? 1. Every year 2. Every 1–2 years 3. Every 2+ years 4. Not specified 99. Other (please specify):	
1.4 Responsibilities and training Purpose – To determine the security practice and review as documented in the policy.	1.4.1. Are staff explicitly informed of their individual responsibilities for protecting the systems used to access and utilize personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 15.
	1.4.2. How are staff informed of their individual responsibilities for protecting the systems used to access and utilize personally identifiable health data? (Please select all that apply.) 1. Policy documents distributed to staff 2. Informal on-the-job training received by staff 3. Formal training received by staff 99. Other (please specify):	
	1.4.3. Do policies state that staff are personally responsible for protecting paper records, computer workstations, laptop computers or other devices associated with confidential public health information or data? 1. Yes (v) 2. No	
	1.4.4. Are all persons authorized to access personally identifiable health data trained on the organization's information security policies and procedures? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 20.
	1.4.5. How often must staff repeat the training on confidentiality and security measures? 1. Every year 2. Every 1–2 years 3. Every 2+ years 99. Other (please specify):	
	1.4.6. Which of the following is the format of the training on confidentiality and security measures? (Please select all that apply.) 1. Material read by staff from printed document 2. Material read by staff on website 3. Instructor-led web training at scheduled intervals 4. Instructor-led training in a classroom setting 5. One-on-one training with another staff member (peer-led model) 99. Other (please specify):	

Category	Questions	Instruction
	1.4.7. Is the date of the training or test documented in the employee's personnel file? 1. Yes (v) 2. No	
	1.4.8. Do all newly hired staff members sign a confidentiality agreement before they are given authorization to access personally identifiable health data? 1. Yes (v) 2. No	
	1.4.9. Which of the following authorized staff members in your program sign a confidentiality agreement? (Please select all that apply.) 1. All staff with access to medical records or confidential health program information 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Health-care volunteers 6. Other health professionals 7. Information technology staff (including data entry staff, analysts, managers and programmers) 8. Administrative staff 9. Professional service providers 10. Cleaners, security guards and any other providers of support services 11. Staff are not required to sign an agreement 99. Other (please specify):	IF "12," GO TO QUESTION 24.
	1.4.10. Do the staff have to repeat the review and signing of the confidentiality statement indicating they understand of the policies and agree to implement them? 1. Yes 2. No	IF "2," GO TO QUESTION 24.
	1.4.11. How often must staff repeat the review and signing of the confidentiality statement indicating they understand the policies and agree to implement them? 1. Every year 2. Every 1–2 years 3. Every 2+ years 4. Never 99. Other (please specify):	
	1.4.12. Are staff explicitly informed of the possible consequences of failing to properly protect personally identifiable health data? 1. Yes (v) 2. No	

Category	Questions	Instruction
	1.4.13. Depending on the severity of the breach, which of the following are possible consequences for members of staff who fail to protect personally identifiable health data? (Please select all that apply.) 1. Education and/or counselling to prevent repeat minor breaches 2. Reduction or loss of security clearance 3. Reduction or loss of data access privileges 4. Demotion 5. Suspension 6. Dismissal/termination of employment 7. Civil legal action 8. Criminal legal action 9. Not specified 99. Other (please specify):	
	1.4.14. How are staff informed of the possible consequences of failing to protect personally identifiable health data? (Please select all that apply.) 1. Policy documents distributed to staff 2. Informal on-the-job training received by staff 3. Formal training received by staff 4. Confidentiality statement signed by staff 99. Other (please specify):	
	1.4.15. When a staff member's employment is terminated, when are data access privileges revoked? 1. Immediately upon termination 2. Within a specified period of time after termination (e.g. 30 days) 3. Not automatically revoked	
	1.4.16. Is there a designated confidentiality information security manager at the data warehouse/repository? 1. Yes 2. No	IF "2," GO TO QUESTION 31.
	1.4.17. Is there a written description of the information security manager's responsibilities? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 31.
	1.4.18. Which of the following tasks are part of the information security manager's responsibilities? (Please select all that apply.) 1. Identify and review all applicable guidelines 2. Advocate for the resources needed for information confidentiality and security 3. Ensure that information confidentiality and security goals are identified, that they meet organizational requirements, and that they are initiated and integrated into relevant processes 4. Improve confidentiality and security awareness by initiating appropriate plans and programs 5. Test, review and validate the effectiveness of the implementation of the information confidentiality and security policy	

Category	Questions	Instruction
	6. Provide clear direction and visible management support for confidentiality and security initiatives 7. Approve assignment of specific roles and responsibilities for information confidentiality and security across the organization 8. All of the above 99. Other (please specify):	
1.5 Monitoring security breaches Purpose: to determine the ability to identify and manage security breaches as documented in the policy.	1.5.1. Do written guidelines exist for managing security breaches? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 33.
	1.5.2. Which of the following procedures for responding to security breaches are included in written procedures? (Please select all that apply.) 1. Roles and responsibilities of staff for managing security breaches 2. Preparing to handle security breaches by rehearsing potential responses 3. Detecting security breaches when they occur and determining the type of incident and appropriate response 4. Analyzing available information related to the security breach to determine the type of incident and the appropriate response 5. Prioritizing the response to the security breach based on criticality of the affected resources (including notifying appropriate individuals) 6. Containing the security breach (e.g. shutting down a system, disconnecting it from a wired or wireless network, disconnecting its modem cable or disabling certain functions) 7. Eradicating the security breach and removing the effects of the cause (such as disabling compromised user accounts) 8. Recovering from the security breach and restoring systems to normal operations 9. Acquiring, preserving, securing and documenting evidence related to the security breach 10. Creating additional security checks to prevent similar security breaches 99. Other (please specify):	
	1.5.3. Are systems monitored to detect potential or actual security breaches? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 35.
	1.5.4. How often are electronic systems monitored? 1. Real time, continuous 2. Daily 3. Weekly 4. When a security breach is suspected 99. Other (please specify):	
1.6 Conducting risk assessments Purpose – To determine the presence and scheduling of risk assessments documented in the policy.	1.6.1. Are risk assessments mandated under the Data Confidentiality and Security Policy? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 38.

Category	Questions	Instruction
	1.6.2. How often are risk assessments performed? 1. Less than 1 year 2. Every yearly 3. Every 1–2 years 4. More thanEvery 2+ years apart 99. Other (please specify): 1.6.3. Which of the following steps are performed during the risk assessment process? (Please elect all that apply.) 1. System characterization: identify the boundaries of the IT system, along with the resources and the information that constitute the system. 2. Threat identification: identify the potential threat sources and compile a threat statement that lists the potential threat sources that are applicable to the IT system being evaluated. 3. Vulnerability identification: develop a list of the system flaws or weaknesses that could be exploited by the potential threat sources. 4. Control analysis: analyze the controls that have been implemented (or are planned for implementation) by the organization as part of efforts to minimize or eliminate the likelihood of an exploitation of a system vulnerability. 5. Likelihood determination: derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exploited. 6. Impact analysis: determine the adverse impact resulting from a successful exploitation of a vulnerability. 7. Risk determination: assess the level of risk to the IT system. 8. Control recommendations: provide controls that could mitigate or eliminate the identified risks. 9. Results documentation: document results in an official report or briefing. 99. Other (please specify):	
1.7 Connectivity to other networks Purpose – To determine if the policy sufficiently details connectivity to other networks.:	1.7.1. Are computers permitted to be connected to more than one network? 1. Yes 2. No 1.7.2. Which of the following methods are used to connect computers to more than one network? (Please select all that apply.) 1. Virtual private network (VPN) 2. Remote desktop software that uses virtual network computing (VNC) and/or remote frame buffer protocol (RFB) 3. Remote desktop software that uses remote desktop protocol (RDP) 4. Remote desktop software that uses another protocol (AIP, NX, X11 or proprietary) or the protocol is unknown 5. Multiple network interface cards (NIC) 6. Network bridge 99. Other (please specify): 1.7.3. Is there built-in encryption on the methods used to connect to other networks? 1. Yes 2. No	IF "2," GO TO QUESTION 41.

2. Data collection		
Category	**Questions**	**Instruction**
2.1 Data collection mechanisms Purpose – To determine data collection methods, content and quality regarding personally identifiable health data.	2.1.1. Which of the following data are received? (Please select all that apply.) 1. Personally identifiable health data 2. De-identified health data 3. Non-identifiable health data 4. Aggregated data 5. Non-personal data 99. Other (please specify): 2.1.2. In what form are data received? 1. Paper-based only 2. Computer-based only 3. Both 99. Other (please specify): 2.1.3. Do you have an updated list of databases containing personally identifiable health data? 1. Yes (v) 2. No 2.1.4. Do you have an updated inventory of computers and mobile devices containing these database or any other personally identifiable health data? 1. Yes (v) 2. No 2.1.5. Which of the following personally identifiable health data elements are received for public health practice? (Please select all that apply.) 1. Name 2. Date of birth 3. Government-issued identification number (such as a national identification number welfare number, driver's license number or passport number) 4. Facility-issued identification number (including medical record numbers) 5. Photographic identifiers (such as photos on a driver's license or passport) 6. Biometric identifiers (such as a fingerprint) 7. Mailing address 8. Phone numbers 9. Medical notes 10. E-mail address 11. Employment information 12. None 99. Other (please specify): 2.1.6. When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose? 1. Yes 2. No	

Category	Questions	Instruction
	2.1.7. Do the data collection methods capture the origin of how, when and by whom the data were collected, modified or deleted in order to protect against improper modification (falsification) or destruction? (Please select all that apply.) 1. How data were collected, modified or deleted 2. When data were collected, modified or deleted 3. Who collected, modified or deleted data 3. No 99. Other (please specify):	
	2.1.8. For personally identifiable health data that will be transferred, are personal identifiers removed before transfer? 1. Yes 2. No	
	2.1.9. When data are transferred, where are personal identifiers removed from the data? 1. At the data collection site before transferring 2. At the data warehouse before further transfer 99. Other (please specify):	
	2.1.10. How are the personal identifiers removed? 1. By removing a specified list of identifiable fields 2. By creating a non-identifiable key that is constructed from identifiable data 3. Other (please specify):	IF "1" OR "3," GO TO QUESTION 53.
	2.1.11. How are the keys for the personal identifiers stored? 1. Electronically 2. Hard copy 3. Both 99. Other (please specify):	
	2.1.12. Is access restricted to the files containing keys? 1. Yes, with user identification and password or lock and key 2. No, access is not restricted 99. Other (please specify):	
2.2 Physical security measures at site Purpose – To determine the physical precautions taken to secure personally identifiable health data.	2.2.1. Which of the following physical precautions are taken to secure personally identifiable health data? (Please select all the apply.) 1. Workspaces, cabinets, paper copies and computers with personally identifiable information are located within a secure area with no public access. 2. Sensitive documents are stored in cabinets and locked. 3. Only authorized personnel can access these cabinets and computers. 99. Other (please specify):	

3. Data Storage		
Category	**Questions**	**Instruction**
3.1 Policy Purpose – To determine if there are clear guidelines in terms of data archival within the policy.	3.1.1. Do you have written guidelines or standard operating procedures (SOPs) on archiving data? 1. Yes (v) 2. No 3.1.2. Which of the following are included in the guidelines/SOPs on archiving data? (Please select all that apply.) 1. How often data must be archived 2. Approved storage locations of archived data 3. Approved media for archiving data 4. Roles responsible for archiving data 99. Other (please specify):	IF "2," GO TO QUESTION 56.
3.2 Physical security storage measures Purpose – To determine the physical precautions taken to secure personally identifiable health data in storage.	3.2.1. Are buildings and rooms containing personally identifiable health data locked for both electronic) and paper documents? 1. Yes (v) 2. No 3.2.2. What physical security controls are in place to prevent unauthorized access to buildings and rooms containing personally identifiable health data? 1. Window locks (v) 2. Security guard or other authorized staff control access (v) 3. Video monitoring (v) 4. Bars/grills for doors or windows(v) 5. Alarm system(v) 6. No physical security control measures are in place 99. Other (please specify): 3.2.3. Are records maintained that indicate which staff are authorized to access buildings and rooms containing personally identifiable health data? 1. Yes (v) 2. No 3.2.4. Do staff need a user identifier and password to gain access to databases and documents containing personally identifiable health data? 1. Yes 2. No 3.2.5. Are staff required to wear identification badges when accessing and working in rooms containing personally identifiable health data? 1. Yes (v) 2. No	

Category	Questions	Instruction
	3.2.6. Are records maintained that indicate the date and time that staff accessed rooms containing personally identifiable health data? 1. Yes (v) 2. No	
	3.2.7. The location used for storing paper-based confidential information is safe from the following (please select all that apply): 1. Risk of fire(v) 2. Risk of flooding(v) 3. Risk of animal or insect damage (such as rodents or insects) (v) 4. Power interruptions(v) 5. Natural disasters(v) 6. Theft(v) 7. None of the above	
	3.2.8. The location used for storing computers containing confidential information is safe from the following (please select all that apply): 1. Risk of fire(v) 2. Risk of flooding(v) 3. Risk of animal damage (such as rodents) (v) 4. Power interruptions(v) 5. Natural disasters(v) 6. Theft(v) 7. None of the above	
	3.2.9. Are persons who are not authorized to access personally identifiable health data allowed to access rooms that contain the records or data? 1. Yes 2. No	IF "2," GO TO QUESTION 66.
3.3 Inventory management Purpose – To determine if there is clear guidance within the policy regarding the migration of data to newer technologies	3.3.1. What types of identification tags are applied to equipment? (Please select all that apply.) 1. Temporary adhesive labels that are not tamper-proof or tamper-evident(v) 2. Permanent or semi-permanent adhesive labels that are tamper-proof or tamper-evident(v) 3. Engraved metal plate attached to equipment(v) 4. Identification is engraved directly on the equipment surface(v) 5. None 99. Other (please specify):	
	3.3.2. How are the facility's inventory records for equipment maintained? (Please select all that apply.) 1. Handwritten or typed paper documents 2. Spreadsheet software 3. Database software 4. Asset management software 5. No inventory records are maintained 99. Other (please specify):	IF "5," GO TO QUESTION 69.

Category	Questions	Instruction
	3.3.3. How often are the facility's inventory records updated? 1. Items are tagged and entered in the inventory record more than 1 month after receipt. 2. Items are tagged and entered in the inventory record within 1 month of receipt. 3. Regularly, but not on a specific schedule. 4. Continuously—items are tagged and entered in the inventory record immediately upon receipt. 5. Never. 99. Other (please specify):	

4. Data backup

Category	Questions	Instruction
4.1 Computers and laptops Purpose – To determine the physical precautions taken to backup personally identifiable health data on computers	4.1.1. Are patient data on desktop and laptop computers backed up? 1. Yes 2. No	IF "2," GO TO QUESTION 77.
	4.1.2. How often are patient data on desktop and laptop computers backed up? 1. Immediately when the data are revised 2. Daily 3. Weekly 4. As needed or requested 99. Other (please specify):	
	4.1.3. Where are backup copies stored? (Please select all that apply.) 1. On the same computer on which data are collected 2. On a central server 3. In cloud-based storage 4. On removable media	
	4.1.4. Are backup patient data from desktop and laptop computers encrypted? 1. Yes, during the backup process 2. Yes, before creation of the backup 3. No 99. Other (please specify):	
	4.1.5. When removable media are used for the backup process, are the removable media encrypted? 1. Yes 2. No	
	4.1.6. How often are backup media for desktop and laptop computers containing patient data transferred to an off-site storage facility? 1. Daily 2. Weekly	IF "6," GO TO QUESTION 77.

Category	Questions	Instruction
	3. Monthly 4. Quarterly 5. Annually 6. Never 99. Other (please specify): 4.1.7. Are your backups rotated ie. are you backing up the backup? 1. Yes 2. No 4.1.8. How often are stored data migrated when newer storage media become available? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular migration schedule 7. Never	
4.2 Servers Purpose – To determine the physical precautions taken to secure personally identifiable health data in storage on servers.	4.2.1. Are patient data on servers backed up? 1. Yes, by the system administrator as needed or as requested 2. Yes, by the system administrator on a regular schedule 3. Yes, using an automated, scheduled process 4. No 99. Other (please specify): 4.2.2. Are data periodically migrated to newer backup media as technology changes provide newer methods of storage? 1. Yes 2. No 4.2.3. Are data backups migrated when newer storage media become available? 1. Yes 2. No 4.2.4. How often are stored data migrated when newer storage media become available? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular migration schedule 7. Never 4.2.5. Are backup media regularly tested to ensure that they can be relied upon in case of emergencies? 1. Yes 2. No	IF "4," GO TO QUESTION 82. IF "2," GO TO QUESTION 82. IF "2," GO TO QUESTION 82.

Category	Questions	Instruction
4.3 Audit logs Purpose – To determine the use, review and backup of audit logs	4.3.1. Are audit logs created to assist in recording all system transactions? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 92.
	4.3.2. Are audit logs stored separately from the rest of the system that they are monitoring? 1. Yes 2. No	
	4.3.3. Which of the following data elements are recorded in the audit log? (Please select all that apply.) 1. IP address or MAC address of computer from which action originated (v) 2. User identifier(v) 3. Dates, times and details of key events (e.g. log on and log off) (v) 4. Records of successful and rejected system access attempts(v) 5. Activation and de-activation of protection systems (such as antivirus systems and intrusion detection systems) (v) 6. Files accessed and the kind of access(v) 7. Record identifier(v) 99. Other (please specify):	
	4.3.4. How often is the audit log reviewed? 1. Real-time, continuous 2. Daily 3. Weekly 4. Only when needed or requested 5. Never 99. Other (please specify):	IF "5," GO TO QUESTION 87.
	4.3.5. Who reviews the audit log? (Please select all that apply.) 1. Data management staff 2. Clinical staff 3. Confidentiality and security officer/information security manager 4. Database administrator 5. Independent auditor 99. Other (please specify):	
	4.3.6. Are audit logs backed up? 1. Yes 2. No	IF "2," GO TO QUESTION 92.
	4.3.7. How are audit logs backed up? 1. By the system administrator as needed or requested 2. By the system administrator on a regular schedule 3. Using an automated, scheduled process 99. Other (please specify):	

Category	Questions	Instruction
	4.3.8. How often are audit logs backed up? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 99. Other (please specify):	
	4.3.9. How often are audit logs of backup data transferred to an off-site storage facility? 1. Daily 2. Weekly 3. As needed or requested 4. Never 99. Other (please specify):	IF "4," GO TO QUESTION 92.
	4.3.10. Are the off-site storage facility for backup media for audit logs locked? 1. Yes 2. No	

5. Authorization and Access Control

Category	Questions	Instruction
5.1 Policy Purpose – To determine if access to data is clearly defined within the policy and that security controls are independently validated.	5.1.1. Access to data has been defined for the following staff members (please select all that apply): 1. Staff access not defined 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Other health professionals 6. Information technology staff (including data clerks, analysts, managers and programmers) 7. Administrative staff 8. Professional service providers 9. Volunteers 10. Academic or other researchers 11. Bilateral donor staff 12. Multilateral institution staff (e.g. staff from the Global Fund to Fight AIDS, Tuberculosis and Malaria) 99. Other (please specify):	
	5.1.2. Are system security controls independently tested and validated? 1. Yes 2. No	

Category	Questions	Instruction
5.2 User access Purpose – To determine if levels of access are specified for using data for different purposes	5.2.1. For roles that are defined as having access to data, are levels of access specified for the following types of data use? Which of the following types of data have specified levels of access for those professionals with defined access roles? (Please select all that apply.) 1. Individual health care 2. Public health practice (including monitoring and evaluation) 3. Human subject research (with consent) 4. Exceptional statutory purposes 5. Public use 6. Not specified 99. Other (please specify):	
5.3 Passwords Purpose – To determine if the policy requires user sessions to be locked after certain periods of inactivity	5.3.1. Do staff need a user identifier and password to gain access to a computer? 1. Yes 2. No	IF "2," GO TO QUESTION 112.
	5.3.2. How are user identifiers generated? 1. By the computer operating system 2. By the computer software application 3. By a system administrator, with user identifier composition rules 4. By a system administrator, without user identifier composition rules 5. By information security manager 99. Other (please specify):	
	5.3.3. Is the password file encrypted? 1. Yes 2. No	
	5.3.4. Are there established procedures to verify the identity of a user prior to providing a new, replacement or temporary password? 1. Yes 2. No	
	5.3.5. How are user identifiers and passwords issued to users? (Please select all that apply.) 1. In person 2. By telephone 3. Through e-mail 99. Other (please specify):	
	5.3.6. After what period of inactivity are user identifiers disabled? 1. 14 days 2. 30 days 3. 60 days 4. 90 days 5. 180 days 6. 360 days 7. Not disabled 99. Other (please specify):	

Category	Questions	Instruction
	5.3.7. When a staff member's employment is terminated, are there procedures for revoking access to personally identifiable health data? 1. Yes 2. No	If "2," GO TO QUESTION 103.
	5.3.8. When a staff member's employment is terminated, when are data access privileges revoked? 1. Immediately upon termination via an automated process 2. Within a week 3. Within a month 99. Other (please specify):	
	5.3.9. Are user sessions automatically locked after a certain specified period of inactivity for software applications that contain personally identifiable health data? 1. Yes 2. No	
	5.3.10. What is the minimum password length? 1. 6 or fewer characters 2. 7–8 characters 3. 9 or more characters 4. No minimum password length	
	5.3.11. Does the system enforce specifications for passwords, such as a combination of a minimum number of lower-case letters, upper-case letters, numbers and special characters? 1. Yes 2. No	
	5.3.12. Are passwords masked when entered into computer applications? 1. Yes 2. No	
	5.3.13. Which of the following is the minimum time that you change passwords? 1. Less than 1 day 2. 1–7 days 3. 8–14 days 4. 15–30 days 5. More than 30 days 6. No minimum time	
	5.3.14. Is a password reset mechanism established for computers and computer software applications that contain personally identifiable health data? 1. Yes—upon password expiration only 2. Yes—can be initiated by the user before the password expires (such as at the first given indication of a possible security breach) 3. No	If "3," GO TO QUESTION 110.

Category	Questions	Instruction
	5.3.15. How is the reset password provided to the user? (Please select all that apply.) 1. Through e-mail 2. By telephone 3. In person 99. Other (please specify): 5.3.16. Is reusing passwords prohibited for a specific number of generations (i.e. a certain number of passwords cannot be reused)? 1. Yes 2. No 5.3.17. Are biometrics or other technologies (e.g. fingerprint verification, signature verification, hardware tokens or smart cards) being used for user identification and authentication? 1. Yes 2. No	

6. Data Release

Category	Questions	Instruction
6.1 Policy Purpose – To determine if the policy contains a detailed release section	6.1.1. Do you have written guidelines for the data release policy? 1. Yes (v) 2. No 6.1.2. Which of the following information is included in the data release policy? (Please select all that apply.) 1. Class of use for which data may be released (e.g. individual health care or public health practice) 2. Specific data elements that may be released 3. Entities and organizations to whom data may be released 4. Requirements for how recipients will protect the confidentiality of received data 5. Specifications for time limitations on use of released data 6. Data quality standards that must be met prior to data release 7. Clearly defined individual(s) who are authorized to release data 8. Clear procedures for handling data requests that are not covered under the data release policy 99. Other (please specify):	IF "2," GO TO QUESTION 114.
6.2 Mandatory requirements for data release Purpose – To determine the extent to which the policy covers requirements and conditions in terms of the release of data.	6.2.1. According to the Data Confidentiality and Security Policy, for what purpose may personally identifiable health data be released? (Please select all that apply.) 1. Not specified in the Data Confidentiality and Security Policy 2. Individual health care(v) 3. Public health practice (including monitoring and evaluation) (v) 4. Human subject research (with consent) (v) 5. Exceptional statutory purposes(v) 6. Public use 99. Other (please specify):	IF "1,"GO TO QUESTION 127. IF "2," GO TO QUESTION 115. IF "3," GO TO QUESTION 118. IF "4," GO TO QUESTION 121. IF "5," GO TO QUESTION 124.

Category	Questions	Instruction
	6.2.2. When is the release of personally identifiable health data for individual health care permitted? (Please select all that apply.) 1. Authorized transfer of patient across facilities(v) 2. Authorized transfer between clinical services(v) 3. Request from patient(v) 4. Not specified 99. Other (please specify):	ANSWER ONLY IF #2 WAS CHOSEN FOR QUESTION 114.
	6.2.3. Which of the following conditions must be met before releasing personally identifiable health data for individual health care? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released(v) 5. Acquisition of formal approval for the data release(v) 6. Not specified 99. Other (please specify):	
	6.2.4. Which of the following conditions must be met by the organization receiving personally identifiable health data in order for data to be release for individual health care? (Please select all that apply.) 1. Signed confidentiality statements by recipient facility staff(v) 2. Documentation of security training of recipient facility staff(v) 3. Evidence of security assessment (eg. review of procedural, electronic and physical security controls) (v) 4. Documentation of internal steering group review and approval(v) 5. Agreement by the recipient to destroy information after the purpose of the data release been fulfilled(v) 6. Assurance that the minimum amount of data needed to satisfy the purpose is being requested(v) 7. Not specified 99. Other (please specify):	
	6.2.5. When is the release of personally identifiable health data for public health practice permitted? (Please select all that apply.) 1. Not specified 2. Regulation of public health policy(v) 3. Public health program planning(v) 4. National reporting(v) 99. Other (please specify):	ANSWER ONLY IF #3 WAS CHOSEN FOR QUESTION 114.
	6.2.6. Which of the following conditions must be met before releasing personally identifiable health data for public health practice? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released(v) 5. Acquisition of formal approval for the data release(v) 6. Not specified 99. Other (please specify):	

Category	Questions	Instruction
	6.2.7. What requirements must be met by the organization receiving personally identifiable health data in order for data release to be authorized for public health practice? (Please select all that apply.) 1. Signed confidentiality statements(v) 2. Documentation of security training(v) 3. Security assessment (review of procedural, electronic and physical security controls) (v) 4. Review and approval by the internal steering group(v) 5. Agreement to destroy information after purpose of data release has been fulfilled(v) 6. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 7. Not specified 99. Other (please specify):	
	6.2.8. When is the release of personally identifiable health data for human subject research (with consent) permitted? (Please select all that apply.) 1. Ethics committee or institutional review board approval (v) 2. Not specified 99. Other (please specify):	ANSWER ONLY IF #4 WAS CHOSEN FOR QUESTION 114.
	6.2.9. Which of the following conditions must be met before releasing personally identifiable health data for human subject research (with consent)? (Please select all that apply.) 1. Verification that patient consent was obtained(v) 2. Confirmation that data have been reviewed for accuracy(v) 3. Removal of direct patient identifiers from released records(v) 4. Acquisition of formal approval for the data release(v) 5. Not specified 99. Other (please specify):	
	6.2.10. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for human subject research (with consent)? (Please select all that apply.) 1. Signed confidentiality statements(v) 2. Documentation of security training(v) 3. Security assessment (review of procedural, electronic and physical security controls) (v) 4. Proof of ethics or institutional review board and approval(v) 5. Review of a scientific protocol by an internal steering group(v) 6. Agreement to destroy information after the purpose of the data release has been fulfilled(v) 7. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 8. Not specified 99. Other (please specify):	

Category	Questions	Instruction
	6.2.11. When is the release of personally identifiable health data for exceptional statutory purposes permitted? (Please select all that apply.) 1. Court order (v) 2. Subpoena(v) 3. Request from law enforcement agency(v) (v) 4. Request from prosecuting attorneys(v) 5. Request from defense attorneys(v) 6. Request from a health-care practitioner providing treatment for a health-care worker or a law enforcement officer because of a medically significant exposure to blood or body fluids(v) 7. Not specified 99. Other (please specify):	ANSWER ONLY IF #5 WAS CHOSEN FOR QUESTION 114.
	6.2.12. Which of the following conditions must be met before releasing personally identifiable health data for exceptional statutory purposes? (Please select all that apply.) 1. Reviews of data for accuracy(v) 2. Removal of direct patient identifiers from released records(v) 3. Acquisition of formal approval for data release(v) 4. Not specified 99. Other (please specify):	
	6.2.13. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for exceptional statutory purposes? (Please select all that apply.) 1. Review and approval of request by legal counsel(v) 2. Review and approval of request by Confidentiality Security Officer (or equivalent official) (v) 3. Review and approval by internal steering group(v) 4. Signed confidentiality statements from persons receiving data(v) 5. Documentation of security training(v) 6. Medical record release signed by patient(v) 7. Medical record release signed by the patient's attorney(v) 8. Security assessment (review of procedural, electronic and physical security controls) (v) 9. Agreement to destroy information after purpose of data release has been fulfilled(v) 10. Request reviewed to verify the minimum amount of data needed to satisfy the purpose(v) 11. Not specified 99. Other (please specify):	

7. Transmission Security		
Category	**Questions**	**Instruction**
7.1 Routers Purpose – to determine the extent to which the policy covers router usage.	7.1.1. Is a router that controls information flow between the local area network and the Internet or other networks installed? 1. Yes 2. No 7.1.2. Which of the following are characteristics of the router configuration? (Please select all that apply.) 1. Enables password protection 2. Limits router access to named users or user groups through command privilege levels 3. Displays banner indicating ownership of the system and that unauthorized access is prohibited 4. Disables unnecessary services 5. Prevents internal IP addresses from being revealed 6. Enables logging of access, including source IP address and the date, time and description of access 7. Accesses lists that contain information to deny or allow traffic by IP address or group8. Turns off incoming IP-directed broadcasts (IP packets that are sent to a particular network or group of networks) 99. Other (please specify): 7.1.3. How often are router logs reviewed? 1. Daily 2. Weekly 3. Monthly 4. Quarterly 5. As needed or requested 6. Never 99. Other (please specify): 7.1.4. Who reviews and provides oversight of the router logs? (Please select all that apply.) 1. Internal IT staff, manually 2. Internal IT staff, using log analysis software 3. Independent auditor 99. Other (please specify):	IF "2," GO TO QUESTION 131.
7.2 Firewalls Purpose – To determine the extent to which the policy covers procedures for protecting data in terms of firewalls	7.2.1. Are firewalls installed on computers, servers and networks? 1. Yes 2. No 7.2.2. Which of the following are characteristics of the installed firewalls? (Please select all that apply.) 1. Apply a security level in accordance with the type of network 2. Block intrusion attempts (from wireless networks (Wi-Fi), hackers, etc.) 3. Specify which software application can access the network or the Internet 4. Block access of specified software applications 5. Offer outbound protection to control information that leaves the computer 6. Others (please specify):	IF "2," GO TO QUESTION 136.

Category	Questions	Instruction
	7.2.3. How often are computers, servers and network firewall logs reviewed? 1. Real-time, continuous(v) 2. Daily(v) 3. Weekly(v) 4. Monthly(v) 5. Quarterly(v) 6. As needed or requested(v) 7. Never 99. Other (please specify): 7.2.4. Who reviews computer, server or network firewall logs? (Please select all that apply.) 1. Internal IT staff, manually 2. Internal IT staff, using log analysis software 3. Independent auditor 4. No one is assigned to review firewall logs 99. Other (please specify): 7.2.5. Which of the following are included in computer, server or network firewall audits? (Please select all that apply.) 1. Review rule sets 2. Review accounts 3. Ensure that logging is enabled and that the logs are reviewed periodically 4. Ensure that the latest patches and updates are tested and installed 5. Ensure that specific IP addresses are blocked 6. Ensure that specific ports are blocked 7. Perform vulnerability and penetration testing 8. No firewall audits are performed 99. Other (please specify):	
7.3 Antivirus on computers Purpose – To determine the extent to which the policy requires electronic systems containing personally identifiable health data, to use antivirus software.	7.3.1. Is antivirus software installed on desktop and laptop computers containing personally identifiable health data? 1. Yes (v) 2. No 7.3.2. How often is antivirus software updated on desktop and laptop computers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. Never 99. Other (please specify): 7.3.3. When are individual files scanned on desktop or laptop computers containing personally identifiable health data? (Please select all that apply.) 1. As scheduled 2. When moved, copied, opened or saved 3. When downloaded 4. Only as part of a scheduled system scan 99. Other (please specify):	

Category	Questions	Instruction
	7.3.4. How often is the operating system scanned by antivirus software on desktop and laptop computers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify): 7.3.5. How often are removable media connected to desktop or laptop computers that contain personally identifiable health data scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	
7.4 Antivirus on servers Purpose – To determine the extent to which the policy requires servers containing personally identifiable health data, to use antivirus software	7.4.1. Is antivirus software installed on servers? 1. Yes(v) 2. No 7.4.2. How often is antivirus software updated on servers containing personally identifiable health data? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify): 7.4.3. When are individual files scanned on servers containing personally identifiable health data? 1. As scheduled 2. When moved, copied, opened or saved 3. When downloaded 4. Only as part of a scheduled system scan 99. Other (please specify): 7.4.4. How often is the operating system on servers containing personally identifiable health data scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	IF "2," GO TO QUESTION 146.

Category	Questions	Instruction
	7.4.5. How often are all drives containing personally identifiable health data and connected to server(s) scanned by antivirus software? 1. Real-time, continuous 2. Daily 3. Weekly 4. As needed or requested 5. At computer start-up 6. Never 99. Other (please specify):	
7.5 Transfer of paper data Purpose – To determine the physical precautions taken to store and secure personally identifiable health data in paper format.	7.5.1. How often are data on paper transferred to an off-site storage facility? 1. Daily 2. Weekly 3. Monthly 4. Quarterly 5. Annually 6. Never 99. Other (please specify):	
	7.5.2. Which of the following security controls are implemented to ensure the security of paper-based data when they are being transferred within a facility or to an off-site storage facility? (Please select all that apply.) 1. A list of approved transport providers (such as site staff, courier services, and government and private postal services) 2. A locked container for transferring or transporting the paper-based data 3. A tamper-proof seal for the container used for transferring or transporting paper-based data 4. A transfer log that identifies the records being transferred, the sender, the recipient, the delivery person, and all relevant dates and times 5. Authentication of the identity of the recipient on delivery 6. Verification of the success of delivery 99. Other (please specify):	
	7.5.3. Does your site store electronic records containing personally identifiable health data? 1. Yes 2. No	IF "2," GO TO QUESTION 150.
	7.5.4. What methods or media are used to transfer electronic data within sites? (Please select all that apply.) 1. Intranet, local area network and/or wide area network 2. E-mail 3. Internet (via web browser) 4. File transfer protocol (FTP) 5. Tape 6. Optical media (CD or DVD) 7. Flash drive and/or memory stick 8. External hard drive 9. Smart card 10. None of the above 99. Other (please specify):	

Category	Questions	Instruction
7.6 Transmission of Electronic Data Purpose: to determine the physical precautions taken to transfer personally identifiable health data electronically.	7.6.1. What controls are implemented to ensure the security of electronic data when they are being moved within a site? (Please select all that apply.) 1. Authentication of the identities of the sender and receiver before information transfer 2. Password-protected data files (with or without encryption) 3. Encryption of the information during transfer 4. Post-transfer verification of the appropriate and successful transfer of information 5. None of the above 99. Other (please specify):	
	7.6.2. What methods or media are used to transfer electronic data between sites? 1. Intranet, local area network or wide area network 2. E-mail 3. Internet (via web browser) 4. File transfer protocol (FTP) 5. Tape 6. Optical media (CD or DVD) 7. Flash drive and/or memory stick 8. External hard drive 9. Smart card 99. Other (please specify):	
	7.6.3. For which of the following transfer methods or media and transfer types is encryption used when data are in transit within the site? (Please select all that apply.) 1. Not used 2. Intranet, local area network or wide-area network 3. E-mail 4. Internet (via web browser) 5. File transfer protocol (FTP) 6. Tape 8. Optical media (CD or DVD) 9. Flash drive and/or data stick 10. External hard drive 11. Smart card 99. Other (please specify):	IF "1," GO TO QUESTION 154.
	7.6.4. When transferring data, which methods are used to authenticate sending and receiving parties? (Please select all that apply.) 1. Sending and receiving parties are not authenticated 2. Two-factor authentication (TFA) 3. Public key infrastructure (PKI) 99. Other (please specify):	

8. Data Disposal		
Category	**Questions**	**Instruction**
8.1 Data Disposal Purpose – to determine the extent to which the policy covers secure retirement and disposal of data	8.1.1. Do you have written guidelines for the secure disposal and destruction of data? 1. Yes (v) 2. No	
	8.1.2. Do you maintain a data retirement schedule for destroying records when they are no longer needed? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 157
	8.1.3 Which types of records are addressed in the data retirement schedule? (Please select all that apply.) 1. Paper records 2. Backup copies of paper records 3. Electronic record 4. Backup copies of electronic records 99. Other (please specify):	
	8.1.4. Which method(s) of destruction or disposal are used? (Please select all that apply.) 1. Burning 2. Demagnetizing 3. Overwriting 4. Pulping 5. Pulverizing, crushing or grinding 6. Reformatting 7. Shredding 99. Other (please specify):	
	8.1.5. Do you maintain documentation of the secure destruction or disposal of the records (such as a certification or verification of destruction)? 1. Yes (v) 2. No	IF "2," THE DATA WAREHOSE ASSESSMENT IS COMPLETE.
	8.1.6. What information are included in the documentation of the secure destruction or disposal of the records? (Please select all that apply.) 1. Organization 2. Organization contact 3. Date of destruction or disposal 4. Name and signature of person who authorized destruction or disposal of data 5. Description of information destroyed or disposed of, including type (paper or electronic) 6. Time period covered by the records to be destroyed 7. Methods of destruction or disposal (e.g. burning, demagnetizing, overwriting, pulping, pulverizing, reformatting or shredding) 8. Name and signature of person who destroyed or disposed of data 9. Name and signature of person who witnessed destruction or disposal of data 10. Copy of contract with outside firm handling the destruction or disposal of data 99. Other (please specify):	

Policy-level assessment tool

The following policy-level questions will help determine the security, confidentiality and appropriate use (including sharing) of data that are collected by health programmes.

The questions are grouped into the following six areas:

- Governance and policy.
- Data storage.
- Authorization and access control.
- Data release.
- Transmission security.
- Data disposal.

A brief purpose statement introduces each section. It is followed by a set of questions to be answered.

Table 4

Recommended policy-level questions

1. Governance and Policy		
Category	**Questions**	**Instruction**
1.1 Legislation Purpose – To determine the existence and extent of legislation covering the use of personally identifiable health data for public health practice and research.	1.1.1. Does legislation exist that covers the use of personally identifiable health data for public health practice? 1. Yes (v) 2. No	IF "2," GO TO QUESTION 3.
	1.1.2. Does this legislation indicate the circumstances under which explicit individual consent is required when using personally identifiable health data for public health practice? 1. Yes(v) 2. No	
	1.1.3. Does legislation exist that covers the use of personally identifiable health data for human subject research? 1. Yes(v) 2. No	IF "2", GO TO QUESTION 5.
	1.1.4. Does this legislation indicate the circumstances under which explicit individual consent is required when using personally identifiable health data for human subject research? 1. Yes(v) 2. No	
1.2 Policy Purpose - To determine the existence, accessibility, distribution, development process and review, of a written policy document ensuring the confidentiality and security of personally identifiable health data.	1.2.1. Does a written policy document regarding the requirements for ensuring the confidentiality and security of personally identifiable health data exist in this country (referred to as the "Data Confidentiality and Security Policy" or "the Policy")? 1. Yes (v) 2. No, but a policy is in the process of development 3. No, but various informal policies exist 4. No, we do not have any policy or written guidelines	IF "2," "3" OR "4," GO TO QUESTION 15.

Category	Questions	Instruction
	1.2.2. What areas of the data life cycle does the Data Confidentiality and Security Policy cover? (Please select all that apply.) 1. Collection(v) 2. Storage(v) 3. Backup(v) 4. Use(v) 5. Transmission(v) 6. Release(v) 7. Disposal(v) 8. Breach investigation(v) 9. Training(v)	
	1.2.3. Does the Data Confidentiality and Security Policy define the roles and access levels of all persons with authorized access to personally identifiable health data? 1. Yes(v) 2. No	
	1.2.4. Does the Data Confidentiality and Security Policy describe which standard procedures or methods will be used when accessing personally identifiable health data? 1. Yes(v) 2. No	
	1.2.5. Is the Data Confidentiality and Security Policy readily accessible to all staff members who have access to confidential individual-level data? (By "readily accessible," we mean that staff can easily access the policy online or in hard copy while at work.) 1. Yes(v) 2. No	
	1.2.6. To which stakeholders or organizations is the Data Confidentiality and Security Policy document distributed? (Please select all that apply.) 1. Ministry to health staff at the national level 2. Health staff at provincial or state facilities 3. District level health facility staff 4. Local health facilities 5. Academic researchers 6. Staff from donor organizations 7. Multilateral institution staff (e.g. The Global Fund to Fight AIDS, Tuberculosis and Malaria, the World Bank or United Nations organizations) 8. Policy document is not distributed 99. Other (please specify):	
	1.2.7. In which of the following formats is the Data Confidentiality and Security Policy document available? 1. Printed(v) 2. Electronic, distributed via e-mail(v) 3. Electronic, distributed via CD or other media(v) 4. Electronic, available on the Internet (please specify the URL): (v) 99. Other (please specify):	

Category	Questions	Instruction
	1.2.8. Which of the following stakeholders were involved in the development of the policy document? (Please select all that apply.) 1. Medical practitioners 2. Nursing practitioners 3. Public health specialists 4. Other health professionals 5. Information technology specialists (e.g. data entry staff, analysts, managers and programmers) 6. Patient advocacy groups 7. Legal expert 8. Human rights advocates 9. Government officials 10. Business representatives 11. Cleaners, security guards and other providers of support services 12. Ethicists 13. Not developed with stakeholders 99. Other (please specify):	
	1.2.9. Does the policy require periodic review of the policy document? 1. Yes 2. No	IF "2," GO TO QUESTION 15.
	1.2.10. How often is the policy document reviewed? 1. Every year 2. Every 1–2 years 3. Every 3–5 years 4. Every 5–10 years 5. Not reviewed at regular intervals 99. Other (please specify):	
1.3 Governance structure Purpose – To determine the governance structure that is in place to provide oversight for the appropriate collection, use, and dissemination of data, including regular review of the policy document and security practices.	1.3.1. Is there is a governance structure (e.g. steering committee or advisory board) in place to provide oversight for the appropriate collection, use and dissemination of data, including the regular review of the policy document and security practices? 1. Yes 2. No 99. Other (please specify):	IF "2," GO TO QUESTION 18.
	1.3.2. The governance structures are present at the following levels (please select all that apply): 1. National level 2. State or provincial level 3. District level 4. Facility level	
	1.3.3. How often does the steering committee or advisory board meet? 1. Monthly 2. Quarterly 3. Every 6 months 4. Annually 5. Every 2 years 6. No regular meeting schedule	

Category	Questions	Instruction
	1.3.4. Which uses of personally identifiable health data are covered by the Data Confidentiality and Security Policy? (Please select all that apply.) 1. Individual health care(v) 2. Public health practice (including monitoring and evaluation) (v) 3. Human subject research (with consent) (v) 4. Exceptional statutory purposes(v) 5. Not specified 99. Other (please specify): 1.3.5. Is information security and its management reviewed at regular intervals? 1. Yes 2. No	
1.4 Review of security practices Purpose – To determine the security practice and review as documented in the policy	1.4.1. Are security practices reviewed by independent auditors? 1. Yes 2. No 1.4.2. How often do independent auditors review security practices? 1. Every year 2. Every 1–2 years 3. Every 2+ years 4. Not specified 99. Other (please specify): 1.4.3. Is the Data Confidentiality and Security Policy regularly updated for technological advancements (such as databases, web servers, e-mail clients, encryption, firewalls, file servers, backup devices and portable storage devices)? 1. Yes 2. No 1.4.4. How often are software and hardware technologies reviewed? 1. Every year 2. Every 1–2 years 3. Every 3–5 years 4. Not reviewed at regular intervals	IF "2," GO TO QUESTION 22. IF "2," GO TO QUESTION 24.
1.5 Responsibilities and training Purpose – To determine the responsibilities and training required as documented in the policy.	1.5.1. Does the Policy state that staff must repeat the review and signing of the confidentiality statement indicating their understanding of the policies and their agreement to implement them? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 26.

Category	Questions	Instruction
	1.5.2. How often does the Policy state that staff must repeat the review and signing of the confidentiality statement? 1. Every year(v) 2. Every 1–2 years(v) 3. Every 2+ years(v) 4. Never 99. Other (please specify):	
	1.5.3. Is it a requirement that the Data Confidentiality and Security Policy (or pertinent parts thereof) be shared with patients in facilities that are collecting personally identifiable data? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 28.
	1.5.4. How is the Data Confidentiality and Security Policy shared with patients? 1. Available on website, but not explicitly shared 2. Provided upon request 3. Provided to all patients as a hard copy or a link to the website as a matter of practice 99. Other (please specify):	
	1.5.5. Does the Policy require organizations to designate an information security manager? 1. Yes 2. No	IF "2," GO TO QUESTION 30.
	1.5.6. Is there a written description of the information security manager's responsibilities? 1. Yes(v) 2. No	
1.6 Monitoring security breaches Purpose – To determine the ability to identify and manage security breaches as documented in the policy.	1.6.1. Does the Data Confidentiality and Security Policy define all guidelines, processes and procedures for identifying and managing security breaches? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 32.
	1.6.2. The following are included in the policy for responding to security breaches (please select all that apply): 1. Purpose and objectives of the policy(v) 2. Definition of a security breach(v) 3. Consequences of a security breach(v) 4. Organizational structure and delineation of roles, responsibilities and levels of authority(v) 5. Requirements for reporting security breaches(v) 6. Prioritization or severity ratings of security breaches(v) 7. Performance measures(v) 8. Reporting and contact forms(v) 99. Other (please specify):	

Category	Questions	Instruction
1.7 Conducting risk assessments Purpose – To determine the presence and scheduling of risk assessments documented in the policy.	1.7.1. Are risk assessments mandated under the Data Confidentiality and Security Policy? 1. Yes(v) 2. No 1.7.2. How often are risk assessments mandated as per the Policy? 1. Every year 2. Every 1–2 years 3. Every 2+ 99. Other (please specify):	IF "2," GO TO QUESTION 34.
1.8 Connectivity to other networks Purpose – To determine the presence of networks and connectivity permissions and methods.	1.8.1. Does the Policy have a position on facility and data aggregation point computers being connected to more than one network? 1. Yes(v) 2. No 1.8.2. Which of the following methods are permitted for connecting computers in facilities and data aggregation and management points to more than one network? (Please select all that apply across all facilities.) 1. Virtual private network (VPN) 2. Remote desktop software that uses virtual network computing (VNC)/ remote frame buffer protocol (RFB) 3. Remote desktop software that uses remote desktop protocol (RDP) 4. Remote desktop software that uses another protocol (AIP, NX, X11 or proprietary) 5. Multiple network interface cards (NIC) 6. Network bridge 99. Other (please specify): 1.8.3. Is built-in encryption mandated by the Data Confidentiality and Security Policy for all methods of connecting to other networks that can be used by facilities and data aggregation and management points? 1. Yes(v) 2. No	IF "2," GO TO QUESTION 37.

2. Data Storage		
Category	**Questions**	**Instruction**
2.1 Policy Purpose – To determine if there are clear guidelines in terms of data archival within the policy.	2.1.1. Does the Data Confidentiality and Security Policy have clear guidelines/SOPs on archiving data? 1. Yes(v) 2. No 2.1.2. Which of the following are included in the guidelines/SOPs on archiving data? (Please select all that apply.) 1. How often data must be archived(v) 2. Approved storage locations of archived data(v) 3. Approved media for archiving data(v) 4. Roles responsible for archiving data(v) 99. Other (please specify):	IF "2," GO TO QUESTION 39.
2.2 Inventory management Purpose – To determine if there is clear guidance within the policy regarding the migration of data to newer technologies	2.2.1. Does the Data Confidentiality and Security Policy require that data be periodically migrated to newer technologies as they become available? 1. Yes 2. No	

3. Authorization and Access Control		
Category	**Questions**	**Instruction**
3.1 Policy Purpose – To determine if access to data is clearly defined within the policy and that if security controls are independently validated.	3.1.1. Access to data have been defined for following staff members (please select all that apply): 1. Staff access not defined 2. Medical practitioners 3. Nursing practitioners 4. Public health specialists 5. Other health professionals 6. Information technology staff (including data clerks, analysts, managers and programmers) 7. Administrative staff 8. Professional service providers 9. Volunteers 10. Academic or other researchers 11. Cleaners, security guards and other providers of support services 12. Bilateral donor staff 13. Multilateral institution staff (e.g. staff from the Global Fund to Fight AIDS, Tuberculosis and Malaria) 99. Other (please specify): 3.1.2. Does the Data Confidentiality and Security Policy require that system security controls be independently validated? 1. Yes(v) 2. No	
3.2 User access Purpose – To determine if levels of access are specified for using data for different purposes	3.2.1. For roles that are defined as having access to data, are levels of access specified for using data for different purposes (e.g. individual health care or public health practice)? 1. Yes(v) 2. No	
3.3 Passwords Purpose – To determine if the policy requires user sessions to be locked after certain periods of inactivity.	3.3.1. Does the Data Confidentiality and Security Policy require user sessions to be locked after a certain specified period of inactivity on software applications that contain personally identifiable health data? 1. Yes(v) 2. No	

4. Data Release		
Category	**Questions**	**Instruction**
This section covers the policies and terms and conditions related to the release of data. **4.1 Policy** Purpose – To determine if the policy contains a detailed release section.	4.1.1. Does your Data Confidentiality and Security Policy contain a data release section? 1. Yes(v) 2. No 4.1.2. Which of the following information is included in the data release section? (Please select all that apply.) 1. Class of use for which data may be released (e.g. individual health care or public health practice) 2. Specific data elements by which data may be released 3. Entities or organization to whom data may be released 4. Requirements for how recipients will protect confidentiality of received data 5. Specifications for time limitations on use of released data 6. Data quality standards that must be met prior to data release 7. Clearly defined individual(s) who are authorized to release data 8. Clear procedures for handling data requests that are not covered under the data release policy 99. Other (please specify):	IF "2," GO TO QUESTION 46.
4.2 Mandatory requirements for data release Purpose – To determine the extent to which the policy covers requirements and conditions in terms of the release of data.	4.2.1. According to the Data Confidentiality and Security Policy, for what purpose may personally identifiable health data be released? (Please select all that apply.) 1. Not specified in the Data Confidentiality and Security Policy 2. Individual health care(v) 3. Public health practice (including monitoring and evaluation) (v) 4. Human subject research (with consent) (v) 5. Exceptional statutory purposes(v) 6. Public use(v) 99. Other (please specify):	IF "1," GO TO QUESTION 59. IF "2," GO TO QUESTION 47. IF "3," GO TO QUESTION 50. IF "4," GO TO QUESTION 53. IF "5," GO TO QUESTION 56.
	4.2.2. When is the release of personally identifiable health data for individual health care permitted? (Please select all that apply). 1. Authorized transfer of patient across facilities 2. Authorized transfer between clinical services 3. Request from patient 4. Not specified 99. Other (please specify):	ANSWER ONLY IF #2 WAS CHOSEN FOR QUESTION 46.
	4.2.3. Which of the following conditions must be met before releasing personally identifiable health data for individual health care? (Please select all that apply.) 1. Verification that patient consent was obtained 2. Confirmation that data have been reviewed for accuracy 3. Removal of direct patient identifiers from released records 4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released 5. Acquisition of formal approval for the data release 6. Not specified 99. Other (please specify):	

Category	Questions	Instruction
	4.2.4. Which of the following conditions must be met by the organization receiving personally identifiable health data in order for data release to be authorized for individual health care? (Please select all that apply.) 1. Signed confidentiality statements from staff at recipient facility 2. Documentation of security training for staff at recipient facility 3. Evidence of security assessment (eg. review of procedural, electronic and physical security controls) 4. Documentation of internal steering group review and approval 5. Agreement by recipient to destroy information after purpose of data release has been fulfilled 6. Undertaking that the minimum amount of data needed to satisfy the purpose is being requested 7. Not specified 99. Other (please specify):	
	4.2.5. Under what circumstances is the release of personally identifiable health data for public health practice permitted? (Please select all that apply.) 1. Not specified 2. Regulation of public health policy 3. Public health program planning 4. National reporting 99. Other (please specify):	ANSWER ONLY IF #3 WAS CHOSEN FOR QUESTION 46.
	4.2.6. Which of the following conditions must be met before releasing personally identifiable health data for public health practice? (Please select all that apply.) 1. Verification that patient consent was obtained 2. Confirmation that data have been reviewed for accuracy 3. Removal of direct patient identifiers from released records 4. Documentation of the review of a request to verify the minimum amount of data needed to satisfy the purpose is being released 5. Acquisition of formal approval for the data release 6. Not specified 99. Other (please specify):	
	4.2.7. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for public health practice? (Please select all that apply.) 1. Signed confidentiality statements 2. Documentation of security training 3. Security assessment (eg. review of procedural, electronic and physical security controls) 4. Review and approval by internal steering committee 5. Agreement to destroy information after purpose for data release has been fulfilled 6. Request reviewed to verify the minimum amount of data needed to satisfy the purpose 7 . Not specified 99. Other (please specify):	

Category	Questions	Instruction
	4.2.8. Under what circumstances is the release of personally identifiable health data for human subject research permitted? (Please select all that apply.) 1. Ethics committee or institutional review board review and approval 2. Not specified 99. Other (please specify):	ANSWER ONLY IF #4 WAS CHOSEN FOR QUESTION 46.
	4.2.9. Which of the following conditions must be met before releasing personally identifiable health data for human subject research? (Please select all that apply.) 1. Verification that patient consent was obtained 2. Confirmation that data have been reviewed for accuracy 3. Removal of direct patient identifiers from released records 4. Acquisition of formal approval for the data release 5. Not specified 99. Other (please specify):	
	4.2.10. What requirements must be met by the organization that is receiving personally identifiable health data in order for data release to be authorized for human subject research? (Please select all that apply.) 1. Signed confidentiality statements 2. Documentation of security training 3. Security assessment (eg. review of procedural, electronic and physical security controls) 4. Proof of ethics or institutional review board research review and approval 5. Review of a scientific protocol by an internal steering group 6. Agreement to destroy information after the purpose for the data release has been fulfilled 7. Review of request to verify the minimum amount of data needed to satisfy the purpose 8. Not specified 99. Other (please specify):	
	4.2.11. When is the release of personally identifiable health data for exceptional statutory purposes permitted? (Please select all that apply.) 1. Court order 2. Subpoena 3. Request from law enforcement agency 4. Request from prosecuting attorneys 5. Request from defense attorneys 6. Request from a health-care practitioner providing treatment for a health-care worker or law enforcement officer because of a medically significant exposure to blood or body fluids 7. Not specified 99. Other (please specify):	ANSWER ONLY IF #5 WAS CHOSEN FOR QUESTION 46.

Category	Questions	Instruction
	4.2.12. Which of the following conditions must be met before releasing personally identifiable health data for exceptional statutory purposes? (Please select all that apply.) 1. Review of data for accuracy 2. Removal of direct patient identifiers from released records 3. Acquisition of formal approval for the data release 4. Not specified 99. Other (please specify):	
	4.2.13. What requirements must be met by the organization that is receiving personally identifiable health the data in order for data release to be authorized for exceptional statutory purposes? (Please select all that apply.) 1. Review and approval of request by legal counsel 2. Review and approval of request by confidentiality and security officer (or equivalent official) 3. Review and approval by internal steering group 4. Signed confidentiality statements from persons receiving data 5. Documentation of security training 6. Medical record release signed by patient 7. Medical record release by patient's attorney 8. Security assessment (eg. review of procedural, electronic and physical security controls) 9. Agreement to destroy information after purpose of data release has been fulfilled 10. Request reviewed to verify the minimum amount of data needed to satisfy the purpose 11. Not specified 99. Other (please specify):	

5. Transmission Security		
Category	**Questions**	**Instruction**
5.1 Routers: Purpose – To determine the extent to which the policy covers router usage.	5.1.1. Does the Data Confidentiality and Security Policy require that facilities and other data compilation and management points install a router that controls the flow of information between the local area network and the Internet or other networks? 1. Yes(v) 2. No	
5.2 Firewalls Purpose – To determine the extent to which the policy covers procedures for protecting data in terms of firewalls.	5.2.1. Does the Data Confidentiality and Security Policy require that systems that are exposed to the Internet have procedures in place for protecting data (firewalls)? 1. Yes(v) 2. No	
5.3 Antivirus on Computers Purpose – To determine the extent to which the policy requires electronic systems containing personally identifiable health data, to use antivirus software.	5.3.1. Does the Data Confidentiality and Security Policy require electronic systems containing personally identifiable health data to use antivirus software? 1. Yes(v) 2. No	
5.4 Antivirus on Servers Purpose – To determine the extent to which the policy requires servers containing personally identifiable health data, to use antivirus software.	5.4.1. Does the Data Confidentiality and Security Policy require servers containing personally identifiable health data to use antivirus software? 1. Yes(v) 2. No	

6. Data Disposal		
Category	**Questions**	**Instruction**
6.1 Data Disposal Purpose - to determine the extent to which the policy covers secure retirement and disposal of data.	6.1.1. Is there a written Policy on the secure disposal and destruction of paper-based and electronic personally identifiable health data? 1. Yes(v) 2. No 6.1.2. Does the Data Confidentiality and Security Policy require that facilities and data compilation and aggregation points maintain a data retirement schedule for destroying records that are no longer needed? 1. Yes(v) 2. No 6.1.3. Does the Data Confidentiality and Security Policy require that documentation (such as a certification or verification of destruction) be produced for the secure destruction or disposal of paper-based and electronic records that contain personally identifiable health data? 1. Yes(v) 2. No	

References

1 Guidelines on protecting the confidentiality and security of HIV information: proceedings from a workshop, Geneva: UNAIDS; 2007 (http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf).

2 Beck EJ, Mandalia S, Harling G, Santas X, Mosure D, Delay P. Protecting HIV-Information in Countries Scaling Up HIV Services, Journal of the International AIDS Society 2011, 14:6 (http://www. biomedcentral.com/content/pdf/1758-2652-14-6.pdf).

3 The Privacy, Confidentiality and Security Assessment Tool: user manual. Geneva: UNAIDS; 2016 (http://www.unaids.org/en/resources/documents/2016/confidentiality_security_tool_user_manual).

UNAIDS/JC2841E

UNAIDS
Joint United Nations
Programme on HIV/AIDS

20 Avenue Appia
1211 Geneva 27
Switzerland

+41 22 791 3666

unaids.org