The Privacy, Confidentiality and Security Assessment Tool

User manual

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, adopt 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. The findings indicated that very few countries had developed comprehensive guidelines on protecting the confidentiality and security of HIV information *(2)*.

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.

That 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 *The Privacy, Confidentiality and Security Assessment Tool: protecting personal health information (3),* 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, *The Confidentiality and Security Assessment Tool: user manual* (user manual) has been produced. This 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

Aim of the user manual

The aim of this user manual is to provide 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.

This user manual provides guidance on how to administer the questionnaires. The actual questions are in *The Privacy, Confidentiality and Security Assessment Tool: protecting personal health information.* The user manual complements the assessment tool and vice versa, and both should be used in conjunction with each other.

Concepts relevant to protecting 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 storage, transfer and use to prevent unauthorized disclosure of that information. Confidentiality policies and procedures should include discussion of the appropriate use and

dissemination of health data, systematically considering the 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 of the information collected. Security discussions should include identifying potential threats to the systems and data and must address both protection of data from inadvertent or malicious inappropriate disclosure and the non-availability of data because of system failure and user errors.

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

- **Personally identifiable health information.** This is individual-level information that includes personal identifiers such as names and addresses, generally obtained at the point of service delivery. This also includes national identification numbers, such as the social security number in the United States of America.
- **Pseudo-anonymized or de-identified health information.** This individual-level information 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 the record with the person's record maintained at a service facility.
- **Anonymized or non-identified health information.** This has been stripped of all identifiers and, since no keys are kept, these data can no longer be linked to the person's record maintained at a service facility.
- **Aggregated health information.** Such data are based on aggregating individual-level information into an indicator and may be obtained from communities, health facilities or data warehouses. These data are usually managed at the level of regional or national databases and are also collected by many international organizations.
- **Non-personal health information.** All levels need to deal with information on facilities, geographical data, information on medicines and medicine supplies and other logistical information.

Background to the assessment tool

With the scaling up of HIV and other health services in middle- and low-income countries, increasing 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 by adopting and implementing relevant privacy laws.

A UNAIDS/PEPFAR workshop with multi-stakeholder input held in Geneva in 2006 developed country guidelines to protect the confidentiality and security of HIV information. The interim guidelines on protecting the confidentiality and security of HIV information was one of the products of that meeting and can be used by countries to adapt, adopt and implement their own guidelines *(1)*.

In 2008, 96 low- and middle-income countries were surveyed to determine whether they had developed and implemented their own guidelines. The findings indicated that very few countries had developed comprehensive guidelines on protecting the confidentiality and security of HIV information *(2)*.

Based on the interim guidelines, an assessment tool was drafted in 2011 to 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, respectively.

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 penultimate draft was field-tested in Kingston, Jamaica, in September 2014. The feedback from this field test was included in the assessment tool. This assessment tool was developed to enable countries to assess the extent to which the confidentiality and security of identifiable and de-identified personal health information are being protected through the existence and implementation of relevant privacy laws, policies and practices *(3)*.

Administering the assessment tool

This section of the user manual provides specific guidance for administering the assessment tool at the three different levels: health facility, data warehouse and national policy levels. For each of the three questionnaires a set of questions are housed 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 have several subheadings and relevant questions, as can be seen in the example of governance and policy:

- Policy.
- Governance structure.
- Review of security practices.
- Responsibilities and training.
- Monitoring, detecting and responding to security breaches.
- Conducting risk assessment.
- Connectivity to other networks.

It is recommended, when possible, that the assessment be approved and led by the health ministry, with the approval of all relevant officials, including the permanent secretary of health, and managed by the director of health informatics, if such a position exists in the country. An external professional—the assessor—should implement the assessment tool in detail by working with the relevant members of the health ministry, especially the informatics department or records department.

At the outset, a draft workplan should be developed based on discussions between the assessor, members of the health ministry and key stakeholders. The workplan outlines the process for administering the assessment tool and should list relevant officials of the health ministry, 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 for the assessment: specifically, to agree on the process and the logistics of administering the assessment tool. Again, the relevant and senior officials of the health ministry should lead this. Formal letters should be sent out as the official invitations for the entry meeting. Further, it is advisable that a small steering committee be created that the assessor and health ministry can tap into for advice and to update on progress or setbacks.

Once the data collection begins, the primary method is small-group interviews to discuss the answer to each question of the assessment tool. In addition, copies of existing policies or procedures should be collected when possible. The assessment tool requires site visits to the national data warehouse and the national offices of the health ministry to administer the data warehouse and policy components of the questionnaires.

Visits to the primary, secondary and tertiary care facilities that have been identified are more logistically challenging. It is recommended to separate the meetings between management and technical staff. Splitting them into two groups can reveal, for instance, that although management says that a policy or procedure is in place, the technical staff may not be administering the policy or procedure or may be unaware of their existence.

Representatives of the health informatics or records department of the health ministry should always accompany the assessor when visiting sites. However, they may or may not attend the actual meetings depending on local circumstances, since informants should not be inhibited in expressing their opinions. The focal person at the facility level and the person responsible for organizing the meetings should be a member of the facility records department. The length of a meeting can range from one to two hours. Table 1 provides a checklist for initiating and administering the assessment tool.

In summary, countries need to protect the confidentiality and security of identifiable and de-identified personal health information since health-care systems in many countries are now collecting and storing increasing quantities of personal health information. Very few countries have developed let alone implemented comprehensive guidelines on protecting the confidentiality and security of HIV information.

The assessment tool was produced so that health professionals in countries can assess the extent to which such policies have been developed and implemented. It was field-tested in Kingston, Jamaica, in September 2014. The feedback from this field-test resulted in the production of the assessment tool. This user manual provides guidance for countries to facilitate the use of the assessment tool in assessing how secure the collection, storage and use of personal health information is in a country while maintaining confidentiality.

Following the use of the assessment tool and the production of a report based on the confidentiality and security assessment performed in a country, it is hoped that this will inform where the country needs to strengthen the protection of the confidentiality and security of personal health information. The interim guidelines on protecting the confidentiality and security of HIV information *(1)* provides additional guidance on how countries can adapt, adopt and implement their own guidelines.

To provide guidance on which issues to raise, several statements and guiding questions have been developed that include general opening statements on the overall purpose of the assessment and use of the assessment tool as well as more detailed questions to guide informants through the more specific questions.

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.

Use of the assessment tool at the health facility level

This module of the assessment tool is to be implemented at the health facility level, including primary, secondary, tertiary or quaternary sites. The participants for the interview include both management and technicians, preferably in two separate meetings; if possible, begin with management and then the technical personnel. This enables follow-up on any questions with the technical staff where management indicated that policies and procedures are in place. The technicians are the ones that should be implementing these policies and guidelines, but they may indicate that they are not aware of any such policies or guidelines.

The representatives of the records department and health information system should attend every health facility visit.

The following introductory statement can be adapted or used as is to provide guidance for this health facility section: "This questionnaire sets out to determine the existing policies and guidelines for the confidentiality and security of patient data at the facility level and to determine the physical precautions in place for data collection, backup and storage; the terms and conditions of data release; the use of routers, firewalls and antivirus software; and the retirement and disposal of data."

Conversations and discussions on this topic with officials can be energetic and lengthy, so two hours should be set aside. Once the introductory statement is delivered and hard copy questionnaires are distributed to the participants, the assessment tool can be administered.

At the outset of each section, such as the governance and policy section, provide an overview to give the respondents an idea of what the section is about. Once this is done, go through the questions in the assessment tool in order.

The following introduction is a general statement that can be adapted or used as is. This section is entitled governance and policy and has 30 questions that cover: legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessment and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessment and networking.

A number of questions and purpose statements for each of the sections have been provided (Table 2). Each section has subsections, which will also require a short introduction. When discussing this with informants, including the number of questions per subsection and reading the purpose statement are also useful.

The following introduction is a statement that can be adapted or used as is for the policy subsection: "This subsection is entitled policy and has six questions. The purpose of this section is 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." Each subsection can be introduced in the same manner (Table 2).

Table 2

Sections, subsections and purpose statements of the health facility

1. Governance and policy

This section is entitled governance and policy and has 36 questions that cover legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessment and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessment and networking.

1.1 Policy (6 questions)
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 Governance structure (4 questions)
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 Review of security practices (2 questions)
Purpose—to determine the security practices and review as documented in the policy.
1.4 Responsibilities and training (18 questions)
Purpose—to determine the responsibilities and training as documented in the policy.
1.5 Monitoring, identifying and responding to security breaches (4 questions)
Purpose—to determine the ability to identify and manage security breaches as documented in the policy.
1.6 Conducting risk assessment (3 questions)
Purpose—to determine the presence and scheduling of risk assessment documented in the policy.
1.7 Connectivity to other networks (3 questions)
Purpose—to determine whether the policy sufficiently details connectivity to other networks.

2. Data collection

This section is entitled data collection and has 13 questions that cover data collection. The purpose of this section is to determine what guidelines exist on data collection.

2.1 Data collection mechanisms (12 questions)
Purpose—to determine data collection methods, content and quality related to personally identifiable health data.
2.2 Physical security measures on site (2 questions)
Purpose—to determine the physical precautions taken to secure personally identifiable health data.

3. Data storage

This section is entitled data storage and has 15 questions that cover data archiving and migration of data. The purpose of this section is to determine what guidelines exist on data archiving and migration of data.

3.1 Policy (2 questions)
Purpose—to determine whether the policy has clear guidelines on data archiving.
3.2 Physical security storage measures (10 questions)
Purpose—to determine the physical precautions taken to secure personally identifiable health data in storage.
3.3 Inventory management (3 questions)
Purpose—to determine whether the policy has clear guidance on the migration of data to newer technologies.

4. Data backup

This section is entitled data backup and has 23 questions that cover backup and storage. The purpose of this section is to determine what guidelines exist on backup and storage of data.

4.1 Computers and laptops (8 questions)
Purpose—to determine the physical precautions taken to back up personally identifiable health data on computers.
4.2 Servers (5 questions)
Purpose—to determine the physical precautions taken to secure personally identifiable health data in storage on servers.
4.3 Audit logs (10 questions)
Purpose—to determine the use, review and backup of audit logs.

5. Authorization and access control
This section is entitled authorization and access control and has 20 questions that cover access to data. The purpose of this section is to determine what guidelines and procedures exist on security controls and levels of access to data.

5.1 Policy (2 questions)
Purpose—to determine whether the policy clearly defines access to data and whether security controls are independently validated.
5.2 User access (1 question)
Purpose—to determine whether levels of access are specified for using data for different purposes.
5.3 Passwords (17 questions)
Purpose—to determine whether the policy requires user sessions to be locked after certain periods of inactivity.

6. Data release
This section is entitled data release and has 15 questions covering the policies and terms and conditions related to the release of data. The purpose of this section is to determine the extent of a policy on data release and to what extent it covers the requirements and conditions on the release of data.
6.1 Policy (2 questions)
Purpose—to determine whether the policy contains a detailed release section.
6.2 Mandatory requirements for data release (13 questions)
Purpose—to determine the extent to which the policy covers the requirements and conditions on the release of data.

7. Transmission security
This section is entitled transmission security and has 27 questions that cover routers, firewalls and antivirus software. The purpose of this section is to determine what policies exist in terms of router usage, firewalls and antivirus software.

7.1 Routers (4 questions)
Purpose—to determine the extent to which the policy covers router usage.
7.2 Firewalls (5 questions)
Purpose—to determine the extent to which the policy covers procedures for protecting data using firewalls.
7.3 Antivirus on computers (5 questions)
Purpose—to determine the extent to which the policy requires electronic systems containing personally identifiable health data to use antivirus software.
7.4 Antivirus on servers (5 questions)
Purpose—to determine the extent to which the policy requires servers containing personally identifiable health data to use antivirus software.
7.5 Transfer of paper data (4 questions)
Purpose—to determine the physical precautions taken to store and secure personally identifiable health data in paper format.
7.6 Transmission of electronic data (4 questions)
Purpose—to determine the physical precautions taken to transfer personally identifiable health data electronically.
7.7 Mail handling (1 question)
Purpose—to determine the procedures used for handling incoming mail at sites involved with personally identifiable health data.

8. Data disposal
This section is entitled data disposal and has six questions that cover the retirement and disposal of data. The purpose is to determine the extent to which the policy covers secure retirement and disposal of paper-based data.

Use of the assessment tool at the data warehouse level

The data warehouse module of the assessment tool is best implemented at the responsible departments within the health ministry or other organization that manages and administers the data warehouse or data repository. The officials to be included for the interview are representatives of management and appropriate technical professionals. Representatives of the records department and health information systems must also attend.

The following introductory statement can be adapted or used as is to provide guidance for the participants in this data warehouse section: "This questionnaire sets out to determine the existing policies and guidelines for the confidentiality and security of patient data at the data warehouse level and to determine the physical precautions in place for data migration, backup and storage; the terms and conditions of data release; the use of routers, firewalls and antivirus software; and the retirement and disposal of data."

Similar to the other two modules, conversations and discussions on this topic with informants can be robust and lengthy, so two hours should be set aside. Once the introductory statement is delivered and a hard copy of the assessment tool is distributed to the participants, it can be administered.

At the beginning of each section, such as the governance and policy section, an overview should be provided to give the respondents an idea of what the section is about. Once this is done, go

through the questions in the assessment tool in order.

The following introduction for the Governance and Policy section is a general statement that can be adapted or used as is: "This section is entitled governance and policy and has 36 questions that cover legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessment and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessments and networking."

The questions and purpose statement for each section are described in Table 3. Each section has subsections, and each requires a brief introduction. Including the number of questions per subsection and reading the purpose statement are also useful.

The following introduction is a statement that can be adapted or used as is for the legislation subsection and each subsection can be introduced in the same manner (Table 3): "This subsection is entitled policy and has six questions. The purpose of this subsection is 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."

Table 3

Sections and subsections and purpose statements of the data warehouse module

1. Governance and policy

This section is entitled governance and policy and has 36 questions that cover legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessment and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessment and networking.

1.1 Policy (6 questions)
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 Governance structure (4 questions)
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 Review of security practices (2 questions)
Purpose—to determine the security practices and review as documented in the policy.
1.4 Responsibilities and training (18 questions)
Purpose—to determine the responsibilities and training as documented in the policy.
1.5 Monitoring, identifying and responding to security breaches (4 questions)
Purpose—to determine the ability to identify and manage security breaches as documented in the policy.
1.6 Conducting risk assessment (3 questions)
Purpose—to determine the presence and scheduling of risk assessment documented in the policy.
1.7 Connectivity to other networks (3 questions)
Purpose—to determine whether the policy sufficiently details connectivity to other networks.

2. Data collection

This section entitled data collection has 13 questions that cover data collection. The purpose of this section is to determine what guidelines exist on data collection.

2.1 Data collection mechanisms (12 questions)
Purpose—to determine data collection methods, content and quality regarding personally identifiable health data.
2.2 Physical security measures on site (1 question)
Purpose—to determine the physical precautions taken to secure personally identifiable health data.

3. Data storage

This section entitled data storage has 15 questions that cover data archiving and migration of data. The purpose of this section is to determine what guidelines exist on data archiving and migration of data.

3.1 Policy (2 questions)
Purpose—to determine whether the policy has clear guidelines on data archiving.
3.2 Physical security storage measures (10 questions)
Purpose—to determine the physical precautions taken to secure personally identifiable health data in storage.
3.3 Inventory management (3 questions)
Purpose—to determine whether the policy has clear guidance on the migration of data to newer technologies.

4. Data backup

This section is entitled data backup and has 23 questions that cover backup and storage. The purpose of this section is to determine what guidelines exist on the backup and storage of data.

4.1 Computers and laptops (8 questions)
Purpose—to determine the physical precautions taken to back up personally identifiable health data on computers.
4.2 Servers (5 questions)
Purpose—to determine the physical precautions taken to secure personally identifiable health data in storage on servers.
4.3 Audit logs (10 questions)
Purpose—to determine the use, review and backup of audit logs.

5. Authorization and access control
This section is entitled authorization and access control and has 20 questions that cover access to data. The purpose of this section is to determine what guidelines and procedures exist on security controls and levels of access to data.

5.1 Policy (2 questions)
Purpose—to determine whether the policy clearly defines access to data and whether security controls are independently validated.
5.2 User access (1 question)
Purpose—to determine whether levels of access are specified for using data for different purposes.
5.3 Passwords (17 questions)
Purpose—to determine whether the policy requires user sessions to be locked after certain periods of inactivity.

6. Data release
This section is entitled data release and has 15 questions that cover the policies and terms and conditions related to the release of data. The purpose of this section is to determine the extent of the policy on data release and to what extent it covers the requirements and conditions of release.

6.1 Policy (2 questions)
Purpose—to determine whether the policy contains a detailed section on the release of data.
6.2 Mandatory requirements for data release (13 questions)
Purpose—to determine the extent to which the policy covers the requirements and conditions related to the release of data.

7. Transmission security
This section is entitled transmission security and has 27 questions that cover routers, firewalls and antivirus software. The purpose of this section is to determine what policies exist on the use of routers, firewalls and antivirus software.

7.1 Routers (4 questions)
Purpose—to determine the extent to which the policy covers router usage.
7.2 Firewalls (5 questions)
Purpose—to determine the extent to which the policy covers procedures for protecting data using firewalls.
7.3 Antivirus on computers (5 questions)
Purpose—to determine the extent to which the policy requires electronic systems containing personally identifiable health data to use antivirus software.
7.4 Antivirus on servers (5 questions)
Purpose—to determine the extent to which the policy requires servers containing personally identifiable health data to use antivirus software.
7.5 Transfer of paper data (4 questions)
Purpose—to determine the physical precautions taken to store and secure personally identifiable health data in paper format.
7.6 Transmission of electronic data (4 questions)
Purpose—to determine the physical precautions taken to transfer personally identifiable health data electronically.

8. Data disposal
This section is entitled data disposal and has six questions that cover the retirement and disposal of data. The purpose is to determine the extent to which the policy covers the secure retirement and disposal of paper-based data.

Use of the assessment tool at the policy level

The policy module of the assessment tool is best implemented at the health ministry headquarters or its equivalent. High-level officials are required for the interview, including the permanent secretary and heads of departments. The ideal group size is 10 but can be expanded to 15. If more than 15 people have to participate, two separate meetings may be best. However, if more than one meeting is required, ensure that some of the same people attend both meetings to ensure continuity. Ideally, representatives of the records department and health information systems should attend all meetings, but others may also be included.

The following introductory statement can be used or adapted to provide guidance for the policy module: "This questionnaire sets out to determine the policies and guidelines that currently exist and directly or indirectly touch on the confidentiality and security of patient data. This can include acts such as an access to information or health records and standards regulations; policies on the security of information technology; staff orders in a human resources manual; guidelines for conducting research on human subjects and many others. Basically, anything that directly or indirectly protects the confidentiality and security of patient data."

Conversations and discussions on this topic with officials can be robust and lengthy, so set aside two hours. Once the introductory statement is delivered and a hard copy of the assessment tool is distributed to the participants, it can be administered. Once consensus is reached for a particular question, move on to the next. Chairing the discussions efficiently is important to keep a

good pace; otherwise, people will start to leave the meeting. However, letting the conversations flow is equally important to not interfere with or bias a particular response.

At the outset of each section, such as the governance and policy section, begin the session with an overview to give the respondents an idea of what the section is about. Once this is done, go through the questions in order. The following introduction is a general statement that can be adapted or used as is: "This section is entitled governance and policy and has 36 questions that cover legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessments and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessment and networking."

The number of questions and purpose statement for each section are described in Table 4. Each section has subsections, and each requires a brief introduction. It is also good to include the number of questions per subsection and to read the purpose statement.

The following statement can be adapted or used as is for the legislation subsection and each subsection can be introduced in a similar manner (Table 4): "This subsection is entitled legislation and has six questions. The purpose of this subsection is 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."

Table 4

Sections and subsections and purpose statements of the policy module

1. Governance and policy

This section has 36 questions that cover legislation, policy, governance structure, security practices, responsibilities and training, security breaches, risk assessment and networks. The purpose of this section is to determine what legislation, policies and governance structures exist and to what extent they cover the use of personally identifiable health data. This section also seeks to identify what security practices are in place, risk assessments and networking.

1.1 Legislation (4 questions)
Purpose—to determine the existence and extent of legislation covering the use of personally identifiable health data for public health practice and research.
1.2 Policy (10 questions)
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.
1.3 Governance structure (5 questions)
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.
1.4 Review of security practices (4 questions)
Purpose—to determine the security practices and review as documented in the policy
1.5 Responsibilities and training (6 questions)
Purpose—to determine the responsibilities and training as documented in the policy.
1.6 Monitoring, identifying and responding to security breaches (2 questions)
Purpose—to determine the ability to identify and manage security breaches as documented in the policy.
1.7 Conducting risk assessment (2 questions)
Purpose—to determine the presence and scheduling of risk assessment documented in the policy.
1.8 Connectivity to other networks (3 questions)
Purpose—to determine the presence of networks and connectivity permissions and methods.

2. Data storage

This section entitled data storage has three questions that cover data archiving and the migration of data. The purpose of this section is to determine what guidelines exist on data archiving and migration of data.

2.1 Policy (2 questions)
Purpose—to determine whether the policy has clear guidelines on data archiving.
2.2 Inventory management (1 question)
Purpose—to determine whether the policy has clear guidance on the migration of data to newer technologies.

3. Authorization and access control

This section is entitled authorization and access control and has four questions that cover access to data. The purpose of this section is to determine what guidelines exist on security controls and levels of access to data.

3.1 Policy (2 questions)
Purpose—to determine whether the policy clearly defines access to data and whether security controls are independently validated.
3.2 User access (1 question)
Purpose—to determine whether levels of access are specified for using data for different purposes.
3.3 Passwords (1 question)
Purpose—to determine whether the policy requires user sessions to be locked after certain periods of inactivity.

4. Data release
This section is entitled data release and has 15 questions that cover the policies and terms and conditions related to the release of data. The purpose of this section is to determine the extent of the policy on data release and to what extent it covers the requirements and conditions of the release of data.

4.1 Policy (2 questions)
Purpose—to determine whether the policy contains a detailed section on the release of data.
4.2 Mandatory requirements for data release (13 questions)
Purpose—to determine the extent to which the policy covers requirements and conditions related to the release of data.

5. Transmission security
This section is entitled transmission security and has four questions that cover routers, firewalls and antivirus software. The purpose of this section is to determine what policies exist on using routers, firewalls and antivirus software.

5.1 Routers (1 question)
Purpose—to determine the extent to which the policy covers router usage.
5.2 Firewalls (1 question)
Purpose—to determine the extent to which the policy covers procedures for protecting data using firewalls.
5.3 Antivirus on computers (1 question)
Purpose—to determine the extent to which the policy requires electronic systems containing personally identifiable health data to use antivirus software.
5.4 Antivirus on servers (1 question)
Purpose—to determine the extent to which the policy requires servers containing personally identifiable health data to use antivirus software.

6. Data disposal
This section is entitled data disposal and has three questions that cover the retirement and disposal of data. The purpose is to determine the extent to which the policy covers the secure retirement and disposal of paper-based data.

Annex

Annex: development of the interim guidelines and the assessment tool

A three-day workshop was held in Geneva, Switzerland, on 15–17 May 2006. It was attended by a multidisciplinary group of health professionals and community members, including people living with HIV *(1)*.

The workshop's aim was to develop draft guidelines on protecting the confidentiality and security of HIV information. It involved plenary sessions and small and large group work. The main conclusions, recommendations and next steps were as follows *(1)*:

- For protecting data, three interrelated concepts influence the development and implementation of protections for sensitive data: privacy, confidentiality and security.
- The public health goal is to safeguard the health of communities by collecting, analysing, disseminating and using health data, which must be carefully balanced with the individual's right to privacy and confidentiality.
- The purpose of defining the principles of the confidentiality and security of health information is to ensure that health data are available and used to improve health and reduce harm for all people, healthy and not healthy.

- The risk of harm following a breach of confidentiality varies with the national or local context according to levels of stigma, lack of comprehensive public health safety nets, legal traditions of respect of privacy, religious perspectives and other local conditions.
- Within countries, privacy and confidentiality laws should be in place, or developed if not already in place, and those involved with the data at all administrative levels must review and know the relevant parameters of privacy or confidentiality laws.
- Countries and organizations at all levels of the health-care system should have a written policy that defines security procedures concerning how data are collected, stored, transferred and released.
- Organizations at all levels of the countries' health-care system and international organizations must identify a confidentiality and security officer to be ultimately responsible for the confidentiality and security of HIV information within that organization.
- The development and review of confidentiality and security laws and procedures should include active participation from relevant stakeholders, including people living with HIV, members of communities affected by HIV, health-care professionals, information technology specialists and legal and ethical experts.
- Funding organizations should comply with these standards and are obligated to make adequate funding available to implement them, sufficient to ensure protection of the data collected and used.
- The different types of HIV information—personal identified, pseudo-anonymized, anonymized, aggregated, and non-personal data—require protection. The procedures for protecting each different type of data must be explicitly described.
- Several organizational procedures need to be followed to ensure safeguards for the collection, transfer, storage, use, dissemination and disposal of personal identified data and other information. The policies and procedures developed must cover both paper-based and electronic systems.
- The greatest threats to electronic information systems are generally not from outside attack but rather from issues inherent in the system design and implementation.

Review of security and confidentiality guidelines in 98 countries

In 2008, a survey was sent to UNAIDS field staff covering 98 middle- and low-income countries. Respondents were asked to complete, in conjunction with relevant country professionals, a questionnaire on whether countries had developed their own guidelines on protecting the confidentiality and security of HIV information and, if so, how detailed the guidelines were (2). The responses were analysed in terms of the countries that claimed to have developed such guidelines (G countries) and those that had not

(NG countries). The responses were scored, aggregated and weighted to produce standard scores for six categories: information governance, country policies, data collection, data storage, data transfer and data access. Associations with national HIV prevalence, gross national income per capita, Organisation for Economic Co-operation and Development (OECD) income category, receiving PEPFAR funding and being a G or NG country were investigated.

Higher information governance scores were observed for G countries compared with NG countries; no differences were observed between country policies or data collection categories. However, for data storage, data transfer and data access, G countries had lower scores than NG countries. No significant associations were observed between country score and HIV prevalence, per capita gross national income, OECD income category and whether countries had received PEPFAR funding.

In conclusion, few countries, including the countries that had claimed that they had developed guidelines, had developed comprehensive guidelines on protecting the confidentiality and security of HIV information. One of the recommendations from this study was that countries should develop their own guidelines, using established frameworks to guide their efforts, but may require assistance in adapting, adopting and implementing them *(2)*.

Developing the assessment tool

After the interim guidelines on protecting the confidentiality and security of HIV information and the 2008 country survey were completed, countries clearly required guidance in assessing the existence and implementation of national guidelines and the extent to which they were being implemented. As a result, an assessment tool began to be developed.

Drafting the assessment tool

The first drafts of the assessment tool to assess the confidentiality and security of personal health information at the facility, data warehouse and national levels were developed by staff members of ICF International/MACRO, UNAIDS and the CDC during 2011 and 2012.

While ICF International/MACRO developed a first draft of the assessment tool, this was done with extensive input from staff from the United States Centers for Disease Control and Prevention (CDC) and UNAIDS. The questions and response choices in the tool were designed to include best or recommended practices to help guide the assessment and improvement of current practices. Use of the assessment tool was intended to provide specific indicators of the extent to which confidentiality and security practices were maintained or whether they needed to be improved and provide a framework for implementing additional confidentiality and security protection measures.

The assessment tool comprises three complementary but independent modules. The three modules were designed to be relevant for organizations that are responsible for developing and implementing national policies and implementation at the data warehouse and facility levels; all modules related back to the interim guidelines. Each section included a reference to the technical requirement summarized in the interim guidelines on protecting the confidentiality and security of HIV information *(1)*. Although these guidelines initially specifically focused on HIV information, all items covered in these guidelines apply to ensuring the confidentiality and security of all personally identifiable health information *(4)*.

The Zambia workshop

The workshop held in Lusaka, Zambia, in 2012 reviewed the draft assessment tool produced by ICF International/MACRO, the CDC and UNAIDS. Multi-stakeholder involvement included relevant officials of the health ministry, clinicians, members of civil society, UNAIDS and the CDC. Key points raised during the meetings included the following:

- During all discussions, everyone recognized the need to develop and implement national guidelines on protecting the confidentiality and security of identifiable health information.
- The assessment tool was extended to cover all personally identifiable health information.
- Several workshop participants considered the tools to be too detailed and thus recommended reducing their size; however, almost all items in the draft were also rated highly in terms of their importance to be included.
- The user-friendliness of the tool was judged insufficient, requiring substantial assistance or tutorial material to administer.
- Community data were missing from the modules.
- The process should target both paper-based and electronic systems collecting health data at all levels.

Each question of the assessment tool was rated based on the following four categories:

- Suitability—the question and its response alternatives are appropriate and necessary.
- Completeness—the question's response alternatives are complete without obvious omissions.
- Validity— the question assesses what is intended and produces actionable responses.
- Clarity—the question is clear and concise, and what is being asked and how to respond are easy to understand.

The priority level of each question was determined according to the following scale:

1 = low, 2 = moderate, 3 = high and 4 = critical.

Points raised during the workshop included that the assessment tool itself was seen to be a key resource in developing country guidelines for the security and confidentiality of patient data. The assessment tool was extended to cover all health information

and not only HIV information. The assessment tool needed to be made more user-friendly; and some informants thought that community data were missing.

The penultimate Assessment Tool

The responses from the Zambia workshop and other relevant input were reviewed during 2013 and 2014. The penultimate draft of the assessment tool was reviewed and questions were agreed on for the health facility, data warehouse and national levels in June 2014.

The final product drew heavily on the draft assessment tool as reviewed in Zambia; it was also compared with the CDC and Prevention data security and confidentiality guidelines for HIV, viral hepatitis, sexually transmitted disease, and tuberculosis programmes *(5)*. In 2011, these guidelines had developed recommended standards to ensure the security, confidentiality and appropriate use, including sharing, of data collected by programmes funded by the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP). The standards are grouped into five topical areas, including: programme policies and responsibilities; data collection and use; data sharing and release; physical security; and electronic data security. Each standard was followed by a set of questions that, when answered, would provide guidance towards programming in policy development and implementation.

Comparison of the NCHHSTP guidelines with the draft assessment tool showed that they were largely comparable, but that the draft assessment tool from the Zambia workshop was more detailed and would therefore provide a more comprehensive assessment tool.

The penultimate draft was reviewed by staff of the CDC, UNAIDS and the consultant who subsequently performed the field test in Jamaica.

Field-testing the assessment tool

The focus of the field-testing was to determine the suitability of the questions of the assessment tool and to provide substantive recommendations regarding suitability. The purpose was not to assess the security and confidentiality of patient data in the country per se but to assess the use of the assessment tool itself and how it performed.

Jamaica was selected as the field-test country because it is an English-speaking country and the assessment tool was developed in English. Jamaica has an established, well-developed health sector and a population size that would enable the assessment tool to be field-tested.

Jamaica is in the process of implementing its National Health Information System Strengthening & e-Health Strategic Plan 2014–2018 *(6)*. The field test was performed in close consultation and collaboration with various sections of Jamaica's Ministry of Health and with support from the Permanent Secretary for Health and the Director of Health Informatics.

A workplan was developed based on discussions between officials of the Ministry of Health, the CDC and UNAIDS. It outlined the process for field-testing

the assessment tool and listed relevant officials of the Ministry of Health, other government officials, health and legal professionals and members of civil society who would participate in the process.

An entry meeting was held at the start of the field test specifically to agree on the process and the logistics of field-testing the assessment tool. The Records Department of the Ministry of Health led this meeting and subsequent process. At the end of the field test, an exit meeting was held at which the results from the field test were discussed with a broader group of stakeholders, including civil society.

The assessment tool was field-tested in two primary, two secondary and two tertiary health-care facilities. In addition, a national data warehouse was identified where the assessment tool was tested, and the tool was also field-tested at the national policy level. The primary method of data collection was through small-group interviews reaching consensus on the purpose and wording of each question of the assessment tool. If policies or procedures had been developed, copies of these were requested.

The field test documented responses to the questions within the context of the existing local or national policies, legislation and technical guidelines, including scope and coverage, to assess the assessment tool and its ability to capture the required data.

In the first two facilities, both management and technical staff were brought together and the assessment tool was reviewed in one large group. However, concern was noted during these meetings that technical staff might have been complying with perceived management desires regarding their responses. It became clear that holding separate meetings for management and technical staff, respectively, worked better, although it took somewhat longer to administer. Although a policy or procedure may be in place according to management, the technical staff members were not complying with the policy or procedure in some cases or unaware of their existence in some cases. This identified the delineation between having policies or procedures and the degree to which they are known or implemented.

A representative of the Records Department of the Ministry of Health always accompanied the consultant when visiting sites. The focal person at the facility level and the person responsible for organizing the meetings were from the facility's records department. The maximum length of a meeting was two hours, though not all took that long.

The questions during the field test were rated based on the same criteria used during the Zambia exercise and assessed the clarity, suitability, completeness and validity of each question. The following criteria were used:

- **Clarity:** did the respondent clearly understand the question? Any additional explaining required?
- **Suitability:** did the question provide the answer sought in the question? Did it provide the answer relating to the question?

- **Completeness:** were the question responses complete without obvious omissions? Were any additions required to the question?
- **Validity:** did the questions assess what was intended and produce actionable responses?

Field-test results

The following is an overview of how the assessment tool was modified based on the feedback received. Details concerning the roll-out of the field-testing, including site and meeting details or particulars on the modifications, have been described elsewhere *(7)*.

Facility level: 168 questions

In general, with relevant professionals and good participants attending the sessions, excellent comments and suggestions were made regarding changes to the questionnaire. Although most of the assessment tool questions were easy to understand, they always brought about rich discussion that prolonged the length of the meetings. However, consensus was always reached on each question. In most instances, there were discussions about how questions would be rolled out, implemented or moved forward in terms of informing policies and procedures. A total of 18 questions out of 168 were modified.

Data warehouse level: 161 questions

Many of the data warehouse questions were identical or slightly modified versions of the facility-level questions, and many of the recommendations for the facility questionnaire applied. Good suggestions were made regarding changes to the questionnaire. Two meetings were held in total, with the first meeting lasting one hour. The participants were unable to finalize the questionnaire because of the rich discussion around the topic of security and confidentiality and not the questions themselves. The second meeting lasted one hour and was required to have a more focused approach on the data warehouse questions from a technical viewpoint and less on the responses to the questions. A total of nine questions out of 161 were adjusted: two were removed and seven amended.

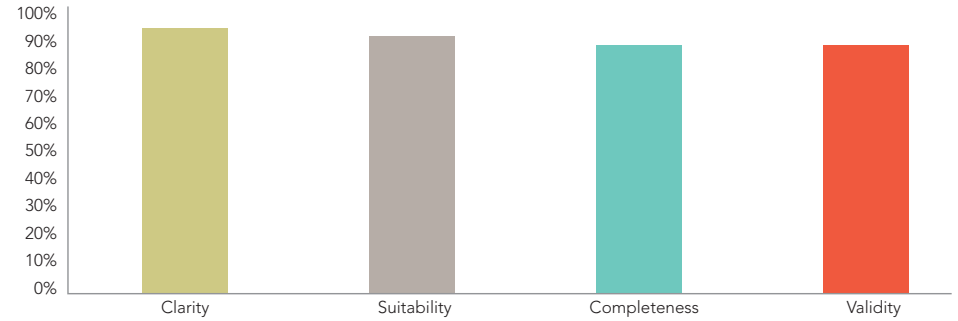
National policy level: 65 questions

Good feedback was also received for the national policy questionnaire. The questionnaire prompted rich discussion regarding policy and legislation that increased the time taken to administer the questionnaire: the time required to administer the questionnaire was one hour. The session included representatives of the System and Information Technology Unit, the Policy, the Planning and Development Division, the Planning and Evaluation Branch, Human Resource Management, the Finance Department and the Legal Department. A total of six questions out of 65 were adjusted.

The overall outcome of assessing all 394 questions and the score obtained for each of the outcome measures is indicated in Figure 1.

Figure 1

The percentage of the 394 questions of the assessment tool that were considered to be 'clear', 'suitable', 'complete' or 'valid' during the field test and that did not have to be altered or removed.



	Clarity (did the respondent clearly understand the question?)	Suitability (did the question provide the answer sought after?)	Completeness (question responses are compete without obvious omissions)	Validity (assesses what is intended; produces actionable responses)
Series 1	97%	96%	94%	94%

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: protecting personal health information. Geneva: UNAIDS; 2016 (http://www.unaids.org/en/resources/documents/2016/confidentiality_security_assessment_tool).

4 Beck EJ, Gill W and De Lay PR. Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of the SDGs and big-data. Global Health Action, 2016 (http://www.globalhealthaction.net/index.php/gha/article/view/32089).

5 Data security and confidentiality guidelines for HIV, viral hepatitis, sexually transmitted disease, and tuberculosis programs: standards to facilitate sharing and use of surveillance data for public health action. Centers for Disease Control and Prevention: Atlanta, United States, 2011.

6 National health information system strengthening and e-health strategic Plan 2014-2018. Ministry of Health, Government of Jamaica: Kingston, Jamaica 2013. (http://moh.gov.jm/wp-content/uploads/2015/07/MOH_NHISeHealth_StrategicPlanFINAL.pdf).

7 Gill W. Confidentiality and security assessment tool for assessing the existence of national country policies on confidentiality and security

JC2840

UNAIDS
Joint United Nations
Programme on HIV/AIDS

20 Avenue Appia
1211 Geneva 27
Switzerland

+41 22 791 3666

unaids.org