HIV/STI Surveillance Training Manual

Unit 7

Confidentiality and Data Security

Table of Contents

Overview .......................................................................................................................... 2
Introduction .................................................................................................................... 4
Addressing Ethical Issues ............................................................................................ 4
Case Identifiers ........................................................................................................... 6
Confidentiality and Security Considerations .............................................................. 9
Guiding Principles ...................................................................................................... 9
Programme requirements ............................................................................................ 10
Policies ........................................................................................................................ 11
Responsibilities ......................................................................................................... 15
Training ....................................................................................................................... 17
Physical Security ........................................................................................................ 17
Data Movement ......................................................................................................... 21
Local Access Control ................................................................................................ 25
Unit 7 Summary ......................................................................................................... 34
Bibliography ............................................................................................................... 34
Unit 7 Case Study ....................................................................................................... 37
Annex 7.1. Additional Laptop Security Considerations .............................................. 38
Annex 7.2. Additional Security and Policy Considerations ........................................ 42
Annex 7.3. Sample Employee Confidentiality Agreement/Oath ................................ 47
Annex 7.4. Attachment G: Using Surveillance Data to Document Need and Initiate
Referrals ..................................................................................................................... 48
Introduction

What you will learn

By the end of this unit you should be able to:
- discuss the ethical principles of respect for persons, beneficence, and justice in the context of HIV surveillance
- identify potential harms caused by release of information regarding HIV status and/or risk history/behaviour
- describe issues of confidentiality and how they relate to HIV surveillance
- describe the purpose of a including a patient identifier on HIV surveillance case reports

Addressing Ethical Issues

What are the issues?

People and groups with increased risk for HIV infection are vulnerable to a number of social, legal and physical harms. Because of this vulnerability and the stigma (mark of disgrace or shame) attached to the disease, public health surveillance programmes need to address a unique set of ethical issues.

If people fear information about their behaviour or their HIV status will be used against them, they may avoid accessing HIV testing, care, support and treatment services, or they may provide inaccurate personal information. Successful surveillance depends on assuring population that information about them will be held in strict confidence and used only for designated surveillance purposes.

In concentrated epidemics HIV-related public health efforts focus on identification of high-risk and infected persons. In generalized epidemics, public health efforts focus on both of these at-risk populations as well as the broader population.

Experience has shown that the general public’s reaction to information about HIV infection in high-risk behaviour populations may be to call for restrictive and prohibitive measures. Such measures simply drive risk behaviour further underground, making HIV testing, prevention, and care programmes more difficult, encouraging the spread of the virus.
Table 7.1. Potential harms that may occur as a result of the release of information regarding HIV status or risk behaviour

<table>
<thead>
<tr>
<th>Type of Harm</th>
<th>Result</th>
</tr>
</thead>
</table>
| Physical     | ▪ public attack  
              ▪ spousal/partner abuse  
              ▪ domestic violence |
| Legal        | ▪ arrest  
              ▪ prosecution, (especially with high-risk populations) |
| Social       | ▪ undesired disclosure to family  
              ▪ workplace discrimination  
              ▪ loss of employment  
              ▪ isolation  
              ▪ loss of healthcare services  
              ▪ exclusion from social environment/network |

Discussing the table

Examine Table 7.1 and then answer the following questions:

a. What are two types of social harm that can occur from the accidental release of information on HIV status or risk behaviour?

b. “Arrest” is classified as which type of harm?

Confidentiality and data security

HIV surveillance is the joint responsibility of many participants in the health care system. Among the participants are:
  ▪ national and sub-national surveillance programmes
  ▪ public and private institutions providing clinical, counselling, and laboratory services
  ▪ individual health care providers
  ▪ persons at risk for HIV infection
  ▪ HIV-infected persons.

The ability of surveillance programmes to collect, store, use, and transmit sensitive HIV case information in a secure and confidential manner is central to the programme’s acceptability and success.

The dynamic nature of information technology is a critical consideration in developing security policies and procedures that will be used to meet the requirements and standards described in these guidelines. The HIV
surveillance system was created before the development of technologies such as laptops, portable external storage devices, and the internet, all of which can be potential sources for security breaches. Now, all Ministry of Health in all countries should routinely assess the changing world of computer technology and adjust security policies and procedures to protect against potential new risks.

**Case Identifiers**

**Why case surveillance needs a unique case identifier**

HIV case surveillance is unique among infectious disease surveillance systems for the following reasons:

1. An individual can only acquire HIV once in a lifetime
2. For surveillance purposes, an HIV-infected person is classified as having advanced HIV disease only once\(^1\), i.e. the earliest diagnosis with clinical stage 3 infection or first CD4 count less than 350 cells per uL.
3. For surveillance purposes, an HIV-infected person is classified as having AIDS only once, i.e. the earliest diagnosis with clinical stage 4 infection or first CD4 count less than 200 cells per uL.

For this purpose, surveillance programmes will need to establish longitudinal surveillance data bases. A longitudinal data base can:

- follow reported cases over time
- identify when a patient progresses from HIV clinical stages 1 and 2 to advanced HIV disease through to death
- permit updating a patient record when additional data are obtained from supplemental reports, active surveillance, systems evaluations (See Unit 5), etc.

Given the requirement of the surveillance system for reporting of cases at different disease stages, and given that patients may move and receive care at multiple facilities, cases will be reported multiple times to the HIV surveillance system. Surveillance programmes need an accurate count of

---

\(^1\) Note that for clinical purposes, someone may be at clinical stage 3 but following clinical improvement from treatment meets the criteria for clinical stage 2. By contrast, the surveillance data base monitors disease progression through the stages but does not record clinical improvements to previous disease stages.
persons with HIV infection, advanced HIV disease and AIDS. To have an accurate count of cases, surveillance programmes need a mechanism that can:

1. Identify multiple reports on one case reported from multiple sources and/or at different time points

2. Distinguish between multiple reports on multiple cases with similar case identifiers and demographic features, e.g. multiple males named Devon Harris who reside in Kingston, Jamaica.

Selecting a case identifier

Implementing a case surveillance system requires that countries determine the method by which cases will be identified. They must decide whether or not such systems should employ names or codes. The UNAIDS guidelines for public health and HIV surveillance ask surveillance programmes to consider the following questions:

- Who will be required to report? What clinical information and personal identifiers will they report? To whom will they report?
- How will the proposed system contribute to a more accurate characterisation of the HIV epidemic?
- What is known about the completeness of reporting for other notifiable conditions, including those that bear some stigma? How can such experience be used to anticipate the willingness to cooperate on the part of those who will be required to report?

Surveillance programmes should carefully consider the type of identifier used for case reporting (see Table 7.2). One identifier that possesses most of these features is a person’s name. Use of names also allows linkage of information on the HIV case surveillance database to other data sources, e.g. programme data from tuberculosis control programmes, STI clinics, mortality records, etc.

There are concerns in many countries that the use of names would discourage persons from accessing HIV services. For this reason, surveillance programmes must develop and maintain methods that ensure that surveillance information is kept confidential and secure.

Although patient names are the best method to identify and report cases, countries may choose to develop/use a unique code to use for reporting cases. A ‘good’ coding system should:

- allow for identification of duplicate reports for the same person
- distinguish between different persons with similar names/demographic profile
- allow for obtaining follow-up information from the health care provider from the surveillance programme
- be available without interviewing the patient i.e. should not be created by the patient and should be recorded on patient medical records
- allow evaluation of the performance of the surveillance system (i.e. permits determining the completeness and timeliness of reporting and the validity of the data submitted on case report forms)

Once a coding system is proposed for development/implementation, it should be evaluated in the country in order to assess its performance in terms of the above mentioned features.

**Table 7.2. Ideal features of a unique case identifier.**

<table>
<thead>
<tr>
<th>Feature of the identifier</th>
<th>Example/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must be unique to the individual</td>
<td>E.g. name, unique national identification number (but only if these are assigned to all residents of a country)</td>
</tr>
<tr>
<td>Should not change over time</td>
<td>E.g. date of birth. If it can change over time, e.g. change of name with marriage or divorce, this should easily determined in health facility records</td>
</tr>
<tr>
<td>Easy to identify from a health facility record</td>
<td></td>
</tr>
<tr>
<td>Routinely collected</td>
<td>If a code is developed from other information, this information should be routinely collected at health facilities</td>
</tr>
</tbody>
</table>
Confidentiality and Security Considerations

Why is confidentiality important

Confidentiality protects subjects from adverse consequences that may arise if their personal information (e.g. HIV positive status, sexual preference, sexual history) is known.

If confidentiality about HIV infection is violated, subjects may suffer discrimination, stigma or arrest. Public health officers must maintain the confidentiality of each individual’s records to guard against inadvertent disclosure.

Confidentiality and data security guidelines

The following guidelines on confidentiality and data security have been adapted from: The CDC HIV Surveillance Programme Technical Guidance for HIV/AIDS Surveillance Programmes, Volume III: Security and Confidentiality Guidelines. 2006.

These guidelines should be reviewed by the appropriate personnel within the National HIV/AIDS programme (e.g. manager of public health surveillance systems, national epidemiologists, manager of the national health information systems, etc) who should then determine the requirements for the country’s HIV surveillance system. Surveillance programmes should also consider the country’s laws, policies and regulations that protect patient confidentiality. Public health officials may wish to promote laws that strengthen patient confidentiality for both health care and surveillance purposes.

Guiding Principles

The five guiding principles (GP) listed below are the backbone upon which all programme requirements and security considerations are derived.

GP 1. HIV surveillance information and data will be maintained in a physically secure environment. Refer to sections related to ‘Physical Security’ and ‘Removable and External Storage Devices’.

GP 2. Electronic HIV surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will
be implemented and documented to minimise the number of staff that have access to personal identifiers and to minimise the number of locations where personal identifiers are stored. Refer to sections ‘Policies’, ‘Training’, ‘Data Security’, ‘Access Control’, ‘Laptops and Portable Devices’, and ‘Removable and External Storage Devices’.

**GP 3.** Individual surveillance staff members and persons authorised to access case-specific information will be responsible for protecting confidential HIV surveillance information and data. Refer to sections ‘Responsibilities’, ‘Training’, and ‘Removable and External Storage Devices’.

**GP 4.** Security breaches of HIV surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate. Refer to the section on ‘Security Breaches’.

**GP 5.** Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV surveillance information and data. Refer to the sections on ‘Policies’ and ‘Security and Confidentiality Programme Requirement Checklist’.

**Programme requirements**

This section details the requirements and security considerations that must be put in place to ensure protection of confidential information. Table 7.3 shows the main areas that are covered in this unit.

**Table 7.3. Programme requirements and security considerations to ensure protection of confidential information.**

<table>
<thead>
<tr>
<th>Main topic area</th>
<th>Detailed in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Requirements 1 through 9</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>Requirements 10 through 13</td>
</tr>
<tr>
<td>Training</td>
<td>Requirement 14</td>
</tr>
<tr>
<td>Physical security</td>
<td>Requirements 15 through 18</td>
</tr>
<tr>
<td>Data movement</td>
<td>Requirements 19 through 25</td>
</tr>
<tr>
<td>Local access control</td>
<td>Requirements 26 through 30</td>
</tr>
<tr>
<td>Security breaches</td>
<td>Requirements 31 through 33</td>
</tr>
<tr>
<td>Laptops and portable devices</td>
<td>Requirement 34</td>
</tr>
<tr>
<td>Removable and external storage devices</td>
<td>Requirement 35</td>
</tr>
</tbody>
</table>
Policies

Requirement 1
Policies must be in writing. Requirement 1 relates to Guiding Principle 2 (GP-2).

Requirement 2
A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (GP-2)

The rationale is to increase accountability and help ensure that the individual knows his/her responsibilities as ORP.

Requirement 3
A policy must describe methods for the review of security practices for HIV surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (GP-5)

Requirement 4
Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)

Requirement 5
A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (GP-2)

Data release policies outline the types of data that can be released and who is authorised to receive the data. For example, with regard to matching HIV cases to cases in other data stores (e.g., TB, STD, or vital statistics), the policy should specify what the purpose is, how this is done, who performs the matching, what results are released, how the results should be stored, and who receives the results.

This policy establishes the rules to be implemented to ensure that information is allowed to flow within the information system and across system boundaries only as authorised. Data release, by definition, suggests that information about an HIV-infected individual is available for distribution. A data release policy has to balance the inherent purpose of HIV surveillance data with the confidentiality of any HIV-infected individual reported for surveillance purposes. Therefore, any HIV surveillance data release policy must be written with two questions in mind. First, which data elements can be released about any case patient that would not identify the individual if pieced together? Second, what
purposes are consistent with the reasons for which the data were originally collected?

With regard to the first question, certain information containing patient identifying data elements (including elements such as patient's name, address, and social security number) may never be released for public distribution. Care must also be taken to ensure that information released cannot be linked with other databases containing additional information that can be used to identify someone. However, in developing a data release policy, state and local HIV surveillance programmes should be aware that several data elements that are not inherently identifying could be linked together to identify an individual. For example, when releasing data on a community with relatively few members of a racial/ethnic group, a risk factor group (e.g., persons with haemophilia), or an age group (e.g., >50 years old or specifying the date of birth or death), surveillance staff should be careful that release of aggregate data on the distribution of HIV-infected individuals by these categories could not suggest the identity of an individual. Time periods also need to be considered when developing a data release policy. Output from cases reported cumulatively (since 1981) better hides any individual's identity than output from cases reported within the past 12 months.

Therefore, care should be taken in deciding how both the numerator and the denominator are defined when developing a data release policy.

Care should also be taken in graphic presentation of data. For example, geographic information systems (GIS) allow for relatively accurate dot mapping of observations. Care must be taken that graphic (like numeric) presentation of data cannot permit the identification of any individual by noting pinpoint observations of HIV cases at, for example, the county, district, parish or enumeration district level. Other considerations in developing data release policies include the need for national surveillance programmes to assure that their data release policies are consistent with national confidentiality laws, and to include clear definitions of terms used in the data release policy (e.g., personal identifier, population size, and time period). For a complete discussion covering this issue, refer to Unit 8, Analysis, Interpretation, and Dissemination of HIV Surveillance Data.

The second issue that should guide the development of a data release policy is to consider the purpose for which the data were originally collected. No HIV surveillance information that could be used to identify an individual should be available to anyone for non-public health purposes. Examples include the release of individual-level data to the public, to parties involved in civil, criminal, or administrative litigation, for commercial purposes, or to non-public health agencies of the national government.
Surveillance data are collected to monitor trends in the epidemic on a population-based level. However, some national surveillance programmes may choose to share individual case reports with prevention and care programmes to initiate referrals to services. Additionally, some surveillance programmes use surveillance data to initiate follow-up for supplemental public health research. Programmes that choose to establish these linkages should do so without compromising the quality or security of the surveillance system and should establish principles and procedures for such practices in collaboration with providers and community partners. Programmes that receive surveillance information should be subject to the same penalties for unauthorised disclosure and must maintain the data in a secure and confidential manner consistent with these guidelines.

Additionally, activities deemed to be research should get appropriate human subjects approvals consistent with the country’s Ministry of Health procedures. A discussion on using HIV surveillance data to initiate referrals to prevention or treatment services is available in the document *Integrating HIV and AIDS Surveillance: A Resource Manual for Surveillance Coordinators - Toolkit 5, Using HIV Surveillance Data to Document Need and Initiate Referrals*, found in Attachment G. Attachment G can be found as an annex to this unit (see Annex 7.4). Several other CDC resources and guidance documents are available online to inform local discussions, including *HIV Partner Counseling and Referral Services: Guidance*, *HIV Prevention Case Management: Guidance*, resources on evaluation of HIV prevention programmes, and more at: [http://www.cdc.gov/hiv/pubs/guidelines.htm](http://www.cdc.gov/hiv/pubs/guidelines.htm).

**Requirement 6**

Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at non-central sites. (GP-2)

As security questions arise in the course of surveillance activities, staff must have ready access to the written policies. In most circumstances, having a copy of the written policies located within the surveillance unit would satisfy this requirement. Computer access to an electronic version of the policies also may be acceptable. The key is for staff to have quick access to policies as security and confidentiality questions arise.

**Requirement 7**

A policy must define the roles for all persons who are authorised to access information, and must specify the specific information that they are authorized to access. For those staff outside the surveillance unit, the policy must define standard procedures or methods that will be used when access is determined to be necessary. (GP-2)
Requirement 8

All authorised staff must sign a confidentiality statement annually. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorised. All new employee or newly authorised staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (GP-2)

The policy should establish rules to ensure that only designated individuals, under specified conditions, can:

- access the information system (network log-on, establish connection)
- activate specific system commands (execute specific programmes and procedures; create, view, or modify specific objects, programmes, information system parameters).

The policy should include provisions for periodic review of access authorisations. The policy could limit access to sensitive data to specified hours and days of the week.

It should also state types of access needed, which could be linked to roles defined for those with access. For example, data analysts may have access to data across programmes that do not include identifiers.

Additionally, the policy should cover restrictions on access to the public Internet or email applications while accessing surveillance information. Accidental transmission of data through either of these systems can be avoided if they are never accessed simultaneously. Similarly, intruders can be stymied in attempts to access information if it is not available while that connection is open.

The policy should establish rules that ensure that group authenticators (administrators, super users, etc.) are used for information system access only when explicitly authorised and in conjunction with other authenticators as appropriate. The policy should express similar rules for individual users to ensure that access to identifiable data is allowed only when explicitly authorised and in conjunction with other authenticators as appropriate. The policy should document the process for assigning authorisation and identify those with approval authority. Information technology (IT) authorities granting access must obtain approval from the ORP or designee before adding users, and they should maintain logs.
documenting authorised users. The ORP or a designee should periodically review user logs.

**Requirement 9**

A policy must outline procedures for handling incoming mail to, and outgoing mail from, the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (GP-2)

The local mailing system and private carrier services are commonly used for the movement of paper copies of information. There are many ways that project areas can protect the confidentiality of an HIV-infected individual when using the mail. For example, when surveillance staff and providers are mailing information (e.g., case report forms) to the central office, the policy could require that names and corresponding patient numbers be sent in one envelope, while the remaining information referenced by the corresponding patient number is sent in another envelope. In addition, the terms 'HIV' or 'AIDS' should not necessarily be included in either the mailing address or the return address. Mailing labels or pre-addressed, stamped envelopes may be supplied to field staff and providers to encourage this practice and to ensure the use of the correct mailing address. Whenever confidential information is mailed, double envelopes should be used, with the inside envelope clearly marked as confidential. Because of the potential number of entries on a given paper copy line list, programmes must exercise extreme caution if they find it necessary to mail a paper list. Procedures for mailing lists, including the amount and type of information permitted in any one mailing, must be clearly outlined in the local policy. Two methods that surveillance programmes currently employ to minimise risk when using the mail are to:

- generate lists containing names without references to HIV or AIDS,
- remove the names from the list and mail them separately from the other sensitive information.

**Responsibilities**

**Requirement 10**

The ORP must certify annually that all programme requirements are met. (GP-2)

**Requirement 11**

Each member of the surveillance staff and all persons described in this document who are authorised to access case-specific information must be knowledgeable about the organisation's information security policies and procedures. (GP-3)
Requirement 12
All staff who are authorised to access surveillance data must be responsible for challenging those who are not authorised to access surveillance data. (GP-3)

Many programmes consider the area of personal responsibility as a potential area of concern because the actions of individuals within a surveillance system are much more difficult to prescribe than operational practices. This area represents one of the most important aspects of holding data in a secure and confidential fashion, but the development of objective criteria for assessing the degree of personal responsibility in individual staff members may be difficult.

The programme requirements in this area may be evaluated objectively by using a series of questions supervisors pose during the annual review of security measures with staff. Input from staff can be obtained through such questions as:

- How often do you find the need to reference security policies or standards?
- Do you know who (by job position or name) should have access to the secure surveillance area? How would you approach someone who was entering the secured room whom you believe was not authorised access? Have you had any occasion to challenge such a person?
- To whom should security irregularities be reported? What are some examples of what would constitute an irregularity? What irregularities would not need to be reported, if any?
- Who else needs access to your computer for any reason? For example, do family members or other staff members ever need to use your workstation? Do you ever need to lend your key to a secured area to another member of the health department staff for after-hours access to the building? Who else knows your computer passwords?

Requirement 13
All staff who are authorised to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (GP-3)

Surveillance staff should avoid situations that might allow unauthorised persons to overhear or see confidential surveillance information. For example, staff should never discuss confidential surveillance information in the presence of persons who are not authorised to access the data.
Staff working with personal identifiers should have a workspace that does not allow phone conversations to be overheard or paperwork and computer monitors to be observed by unauthorised personnel. Ideally, only staff with similar roles and authorisations would be permitted in a secure, restricted area.

**Training**

**Requirement 14**

Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (GP-3)

Security training should be required for all new staff and must be repeated annually thereafter, but the nature of this training may vary based on country circumstances. For example, in areas of low HIV prevalence where one surveillance person is on staff, if that person leaves before training a replacement, the policy should indicate that training for data security and confidentiality may be obtained in a neighbouring country with a similar system. In other areas, new staff may be trained by the surveillance coordinator one-on-one. In this instance, the policy should document what types of information must be covered in such a session, and provisions should be made to document that training was completed. In areas of high HIV prevalence with larger numbers of staff, periodic group training sessions may be more appropriate.

**Physical Security**

**Requirement 15**

All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. (GP-1)

**Requirement 16**

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)

**Requirement 17**

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room (GP-3)
Maximum security practice dictates that HIV surveillance data be maintained on a dedicated file server at only one site in each project area where layers of security protections can be provided in a cost-effective manner. This would obviate the need to duplicate expensive security measures at multiple locations throughout the country.

Remote sites that need access to the central surveillance server for surveillance activities could access the server through a secured method (e.g., virtual private network [VPN], or authentication server) set up for authorised users.

Some countries may decide to maintain the reporting system in more than one site. If this is the case, every additional reporting system site in the country must meet the same minimum security measures outlined in all of the programme requirements.

Because the surveillance system can potentially identify any number of persons with HIV infection within a country (or local jurisdiction if surveillance is decentralised), particular attention to the security of surveillance information is critical. The minimum security standard should be to enclose the surveillance information inside a locked room regardless of the method used. Whether the reporting system resides on a server or workstation, the computer containing the electronic surveillance data must be enclosed inside a locked room. Only authorised surveillance personnel should have access to the locked room. However, depending on the numbers of HIV cases reported, the size and role of the surveillance staff, community interest, and department resources, the ORP may decide that other authorised health department staff may need to work inside the surveillance room.

If the surveillance data reside on a server inside a locked room and not on the hard drive of any individual workstation within the department, the individual workstation (when logged off the network) does not pose a great security risk and would not necessarily have to be located behind a locked door to meet the minimum standard. LAN accounts with access to identifying information in the reporting system should be limited only to the workstations of those authorised.

LAN accounts also should be limited by time of day (See Requirement 7). The use of cubicles in many office buildings can also present a challenge to creation of a secure area. Cubicles with low walls make it difficult, even within a secure area, to have a telephone conversation without others hearing parts of the conversation.

Where necessary, higher cubicle walls with additional soundproofing can be used. When cubicles are part of the office structure, cubicles where
sensitive information is viewed, discussed, or is otherwise present should be separated from cubicles where staff without access to this information is located.

When electronic surveillance data with personal identifiers are stored outside of a physically secure area (i.e., a locked room with limited access), or if limited local resources require that surveillance data with personal identifiers stored on a LAN be accessible to non-surveillance staff, real-time encryption software must be employed. The additional encryption software is designed to keep identifying information encrypted. Should an unauthorised individual gain access to the surveillance database, unencrypted identifying information cannot be viewed.

Encryption requirements would also apply to backup storage media, which are frequently located off-site and could be managed by an outside vendor. Paper copy data stores must be maintained in a locked cabinet and inside a locked room. If an area chooses to no longer maintain paper copies in locked file cabinets inside a locked room (e.g., because of age or volume), the programme should destroy the completed forms after ensuring the data are entered into the reporting system and after they are no longer needed for follow-up. Before destroying the forms, a site may opt to digitally scan forms for future reference. Digitised forms should be secured the same as any other surveillance data.

Requirement 15 does not apply to subsets of case report forms, such as those that a surveillance staff member may hold in the course of an investigation, but does apply to paper copy line lists or logbooks that list a large number of reported cases by name in any one jurisdiction. Even if appropriate space is available to properly store all surveillance forms, programme staff should consider developing a records retention policy that would describe the record retention and the scheduling of records for destruction after a designated period. Older records offer only limited value, but continue to pose a security risk. Sites should carefully weigh the benefits and risks of retaining any paper copies of case report forms. Such a decision should be predicated on adherence to these security standards, national regulations, and local practice. Once a decision has been made to destroy a case report form, line list, notes, or any other related paper surveillance document, the document must be destroyed in accordance with Requirement 17.
Requirement 18
Rooms containing surveillance data must not be easily accessible by window. (GP-1)

Window access, for the purposes of this document, is defined as having a window that could allow easy entry into a room containing surveillance data. This does not mean that the room cannot have windows; rather, windows need to be secure. If windows cannot be made secure, surveillance data must be moved to a secure location to meet this requirement.

A window with access, for example, may be one that opens and is on the first floor. To secure such a window, a permanent seal or a security alarm may be installed on the window itself. Even if the window does not open, programme managers may decide to include extra precautions if, for example, the building does not have security patrols or if the building or neighbouring buildings have had breaches. If a project area has a concern about a current or planned physical location, staff can request advice from CAREC.

For the purposes of this document, a remote site is defined as a site that remotely connects to and accesses a centralised electronic database to enter and store surveillance data even though paper forms may be stored locally. The central database is located in a different physical location than the remote site. A satellite location is defined as a site that collects and electronically enters surveillance data in a local database and then sends the electronic data file to a central location. If remote and satellite sites maintain case report forms or other surveillance information with personal identifiers, the central location should not be maintaining duplicate copies of the case report forms. Surveillance staff should discourage providers from maintaining duplicate copies of HIV case reports after they have been reported to the health department.

The national HIV case database should be housed in only one location (excluding electronic backups and replication for disaster recovery); however, for countries with multiple database locations, the number of satellite locations should be kept to a minimum, thereby keeping the data collection and storage as centralised as possible. If the system is decentralised, each remote and satellite site should maintain only cases within that site's jurisdiction, and must meet the same physical security requirements discussed in the section on ‘Physical Security’.

If, after discussing a records retention schedule, programme staff decide to retain the hard copy case report form even after the record is entered into the reporting system, they should consider removing or striking out the name on the report before storage. The patient number or code would still
provide linkage, when necessary, to the name in the reporting system while improving record security. This practice would decrease:

- the number of places where names are stored,
- the amount of time they are held, and
- the number of persons who may have access to them in the future.

Security software that controls the storage, removal, and use of data maintained in the reporting system should be in place at all locations where the electronic surveillance data are maintained. Security software may include such protections as user identifications, passwords, boot protection, encryption algorithms, and digital signatures. Additionally, an area may maintain names outside of the reporting system and use a state ID number to link name and surveillance information when needed.

**Data Movement**

**Requirement 19**

Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)

**Requirement 20**

An analysis dataset must be held securely using protective software (i.e. software that controls the storage, removal, and use of the data). (GP-1)

**Requirement 21**

Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (GP-1)

Electronic files stored for use by authorised surveillance staff should be encrypted until they are actually needed. If these files are needed outside of the secure area, real-time encryption or an equivalent method of protection is required. This requirement also applies in those situations where surveillance data are obtained electronically from external sources (clinical data management systems and laboratories) or as part of a separate collection system. Extracts from those systems need to be protected as if they were extracts from the surveillance data system.

Additionally, those systems within other health facilities need to be held to the same standards as the HIV surveillance systems. External agencies are to be encouraged to review their procedures, and approved data transfer methods need to be used.
Requirement 22
When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting national standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioural information, must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)

The intent of this requirement is to eliminate the possibility that a third party may identify a person as being HIV-infected a member of an HIV risk-group. When trying to locate an HIV-infected person during an investigation or interview, letters, business cards or voice messages left at the person’s residence should not include any terminology that could be associated with HIV, AIDS, or the health department. These precautions need to be taken in case a family member or friend discovers the letter or card or hears the voice message. Similarly, if a third party calls the telephone number listed on a card or letter, that party should not be able to determine by a phone greeting that it is an HIV surveillance unit (or the health department); nor should a third party be able to obtain that information by pretending to be the case patient. This may require the use of some confirmation mechanism to assure that the person calling really is the case patient and not someone pretending to be that person to discover confidential information.

If secure fax or encrypted e-mail transmissions are used at all (a practice that is strongly discouraged), care must be taken to avoid linking HIV or risk factor status with identifiable information about a person. This may include ensuring that the terms HIV or AIDS do not appear in the fine print at the very top of a fax indicating who sent it and that these terms do not appear in more obvious locations in the letterhead and body of the fax. Other important steps include thinking about who else besides the intended recipient may have access to faxes on the receiving end and the possibility of misdialling the fax number or using the incorrect e-mail address.

Requirement 23
When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS. (GP-1)

One purpose of this requirement is to make it difficult to link an individual's name on a line list with HIV/AIDS, should that line list fall into the hands of an unauthorised person. Terms that could be associated
with HIV/AIDS include CD4 count or opportunistic infection (OI). Programmes should consider using less recognisable terms, codes, or abbreviations such as T-lymphocyte count or OI. In some circumstances, just the word “count” may suffice. While risk factor information (e.g., injection drug use or sexual orientation) may not necessarily be associated with HIV/AIDS, it nevertheless is highly sensitive. Wherever possible, risk factor categories must be coded to help minimise the possibility of a breach. If a coding scheme for transmission category is already built into the reporting system, the codes should be used when there is a need to generate line lists with risk factor categories. When surveillance staff record notes, they should make it a habit to use these risk factor codes. For example, instead of using the phrase injection drug user or the readily decipherable abbreviation IDU, a code could be substituted.

This requirement applies to information or data taken from secure areas. It does not refer to data collected from the field and taken to secure areas. While coding of terms associated with HIV/AIDS in the field is encouraged, there may be occasions when it cannot be done, for example, when uncoded terminology must be abstracted from a medical chart during the course of an investigation.

**Requirement 24**

Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)

Under exceptional circumstances, HIV surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation arises that would make returning to the surveillance office impossible or unsafe. For example, if a worker carrying sensitive information were caught in a sudden heavy storm, driving home instead of returning to the office would be permissible provided the worker's supervisor is notified (or an attempt was made to notify the supervisor) of the need to return home with the sensitive information. Precautions should be taken at the worker's home to protect the information under such circumstances. All completed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

Managing field time effectively can be accomplished by using a variety of creative tactics. Field visits should be scheduled in the most efficient way possible. One option is to assign provider sites to workers by geographic area. For example, all providers in the east sector could be covered by the same worker to minimise travel time between sites. Another option might be to schedule visits so that sites located far from the office receive visits early in the day with staff working their way back to the office by the end
of the day. A flex-time schedule is another option that a site may wish to consider.

If returning to the secured area creates significant inefficiencies in case surveillance investigations, alternative methods of securing sensitive surveillance information could be considered when developing the policy that satisfies this requirement.

Investigators could incorporate the use of pre-addressed, stamped envelopes and drop completed case report forms in the mail before returning home for the day. Tampering with the mail is a criminal offence, and case reports are considered better protected in the mail than at a private residence. This possibility should be accounted for when developing the mail policy discussed in Requirement 9.

Some areas do not complete case report forms on-site, but take notes using shorthand that is not easily translated and does not contain HIV-related terms. Notes such as these could be stored in less secure areas because someone seeing the notes would not understand their meaning. When this method is used, blank case report forms or other HIV-related materials should not be stored at the same location as the notes. Staff using this technique may carry the notes around discreetly (e.g., in a purse or notebook) and then complete official forms when they return to the surveillance office. Other methods to disguise the data, de-identify it, or separate sensitive variables from it could be used to eliminate the need to return to the office at the close of business (i.e., if personal identifiers are removed using approved methods, the information is less sensitive and may be secured off-site). Whatever methods are used, the approved method must be described in the local security policy.

**Requirement 25**

Prior approval must be obtained from the surveillance coordinator when planned work-related travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (GP-1)

Policies and procedures for gaining prior approval for not returning surveillance information with personal identifiers to the secured area at the close of each business should be implemented. Refer to the discussion following Requirement 24 for additional considerations.

In some instances, it may be necessary to transfer data between sites, e.g. between parish/district health departments. The sending and receiving sites must agree on the product that will be used for that purpose and identify the method of transfer. Transport by a designated officer should be done in a manner to minimise the risk of the information getting into unofficial hands, i.e. by direct non-stop transfer with handover to the
designated person. There should be written records of the transfer and receipt of the documents. See Requirement 23 for electronic transfer of information and Requirement 9 for mailing of sensitive documents.

**Local Access Control**

**Requirement 26**

Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on all of the following conditions being met:

- a demonstrated need for the names
- documentation of approval the *Institutional Review Board* (IRB) of the country’s Ministry of Health (or designate)
- signing of a confidentiality statement regarding rules of access and final disposition of the information.

Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies. (GP-1)

Most analyses of HIV surveillance data do not require IRB approval; in fact, most such analyses do not require the inclusion of identifying information in the data sets. Occasionally, investigators from other health department units or academia want to conduct supplemental studies using reported case patients as their study population. Additionally, clinic-based researchers may want to obtain additional information on their patients. In these cases, the researcher should submit a request for the data set to the HIV surveillance coordinator. The surveillance coordinator should then refer to the local data release policy to determine if any of these types of data sets can be released. Data containing patients' names are not normally released for research purposes; further, the data release policy should anticipate that even data not containing names could be used to breach an individual's confidentiality if data sets are created or can be created that could indirectly identify any individual (e.g., a data set of all Asian haemophiliacs with HIV infection in a county with a low Asian population and low morbidity).

Under certain circumstances and in accordance with local data release policies, the surveillance coordinator should refer the researcher to the Chair of the IRB. If the Chair determines that an IRB should be convened; both the researcher and surveillance coordinator must abide by the ruling. The IRB may approve the release of an analysis data set. Before a researcher obtains access to a data set, the surveillance coordinator must obtain a signed statement from the researcher certifying that he or she will
comply with standards outlined in the local security policy. Signing this statement should indicate that the researcher:

- understands the penalties for unauthorised disclosure,
- assures that the data will be stored in a secured area, and
- agrees to sanitise or destroy any electronic (or other storage) devices that contained the data set when the research project is completed.

If the researcher is a member of the HIV surveillance unit and already has a signed confidentiality statement on file, there is no need to sign an additional statement.

Analysis databases or data sets that are released to individuals who work outside the secured area must be held securely until the data are approved for release. For example, epidemiologists or statisticians who do not work in the secured area often use analysis databases for routine analysis. The computers used in these circumstances must have protective software (e.g., user ID and password protection) to maintain data securely. Other robust authentication methods also may be used since the examples described are only the minimum required. Encryption software is not required with analysis databases because they are considered much less sensitive than those that contain names or other personal identifiers. Analysis data are still considered sensitive, since it may be possible to identify individuals by using particular combinations of reporting system variables.

For that reason, analysis data should not be taken home, and all the results of all analyses performed by using reporting system variables must be approved for release as outlined in the surveillance unit's data release policy.

**Requirement 27**

Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorised individuals can only be granted during times when authorised surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (GP-1)

If unauthorised personnel (e.g., cleaning or maintenance crews) are allowed access to the secured area during times when surveillance staff are not present, then more stringent security measures must be employed inside the secured area to meet the programme requirements. Under such circumstances, computerised surveillance information and data stored on one or more stand-alone computers or accessible via a LAN-connected workstation must be held securely with access controls in place, such as boot-up passwords that prevent unauthorised access to the computer's hard
drive by booting from a system disk, encryption software, or storing the data on removable devices that can be locked away before allowing unauthorised personnel access. If surveillance information is stored on a LAN server, accounts with authorised access should be restricted by time of day and day of week. See Requirement 7.

Managing keys or keypad codes to a secure area is difficult when personnel who receive the keys or codes are not directly supervised by the surveillance unit. Because of staff turnover in cleaning crews, the number of people who may be given keys or codes to the secure area may multiply over time. The more people with keys and codes, the greater the risk to the system. While tracking who has a key or code in this scenario can be difficult, it is recommended that a method of tracking and logging the issuance of keys or codes be implemented. It is further recommended that if an accurate accounting of all keys or codes to a secure area cannot be made, that the lock or code to that area be changed and issued using the tracking and logging method developed.

While many surveillance programmes do not routinely grant access to the secured area to cleaning crews or maintenance staff, programme requirements can be met even if cleaning crews are granted access without authorised escort, provided added measures (as discussed previously) are employed. The added measures must be named and described in the local security policy.

For example, the policy might state that in lieu of escorting cleaning crews and other maintenance staff inside the secured area after hours, the surveillance unit will implement additional documented security measures to provide for enhanced data protection.

**Requirement 28**

Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorised based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (GP-1)

The primary function of HIV surveillance is the collection and dissemination of accurate and timely epidemiologic data. Areas that elect to establish linkages to other public health programmes for prevention or case management should develop policies and procedures for sharing and using reported data that ensure the quality and security of the surveillance system. These programmes should be developed in consultation with providers and community partners, such as their prevention planning groups. Recipients of surveillance information must be subject to the same
training requirements and penalties for unauthorised disclosure as surveillance personnel.

Before establishing any programme's linkage to confidential surveillance data, public health officials should define the public health objectives of the linkage, propose methods for the exchange of information, specify the type of surveillance data to be used, estimate the number of persons to be served by the linkage based on the availability of resources, outline security and confidentiality procedures, and compare the acceptability and effectiveness of basing the prevention programmes on individual HIV surveillance case reports to other strategies. The ORP must have the final approval of proposed linkages, since the ORP is ultimately responsible for any breach of confidentiality.

Prevention programmes that use individual HIV surveillance case data should evaluate the effectiveness of this public health approach. On an ongoing basis, programmes also should assess confidentiality policies, security practices, and any breaches of confidentiality. Individual HIV case reports should not be shared with programmes that do not have well-defined public health objectives or with programmes that cannot guarantee confidentiality.

**Requirement 29**

Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (GP-2)

Security is compromised if other programmes that lack adequate standards to protect the security and confidentiality of the data are granted access to HIV surveillance data or information and use that access to add HIV data to their systems.

Linking records from the surveillance data with records from other databases semi-annually or annually is encouraged to identify cases not previously reported, such as cases identified through TB surveillance or cancer surveillance. This provides a systematic means to evaluate the performance of health department surveillance and to take action to strengthen weaknesses in systems as they are identified. For example, programmes can plan site visits with those providers who do not comply with the country’s reporting laws to stimulate more timely and complete reporting.

Before the linkage of surveillance data, protocols should be discussed and developed. The protocol should address how the linkage will be performed...
using methods that are secure, who will analyse the results, and how the information will be used to improve the selected surveillance systems.

**Requirement 30**
Access to surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (GP-2)

Some country laws mandate access to HIV surveillance information for purposes other than law enforcement or litigation activities. For example, in the some states in the US require school officials or prospective parents to be notified when they enrol or adopt HIV infected children. However, the surveillance unit is not necessarily required to release the information just because it is requested by law enforcement or other officials. Access should be granted only to the extent required by law of the country and not beyond any such requirement.

Any request for surveillance information for law enforcement purposes should be reviewed by the ORP with the appropriate legal counsel to determine what specific information, if any, must be released from records maintained solely for epidemiologic purposes.

Medical information may be available to the courts from less convenient but more appropriate sources. When information is ordered released as part of a judicial proceeding, any release or discussion of information should occur in closed judicial proceedings, if possible.

**Central and Remote Access Control**
The most secure protection for HIV surveillance data is having only one centralised database in each country. Centralised data stores are those in which all electronic records of HIV cases are stored in only one location within each country.

Centralisation of HIV surveillance data within a country has clear benefits. First, centralised data stores offer greater security. The advantages of having several HIV surveillance databases throughout a country may be outweighed by the risk of a security breach. Centralised data stores add efficiency by improving case matching. With a centralised database, remote surveillance staff may conduct matches against the parish/county/district database, thereby reducing local level duplicates and minimising unnecessary field investigations of cases already reported elsewhere in the country. Centralised systems may cost less to maintain. Finally, a centralised platform may support parallel surveillance systems (e.g., TB and STD). In other words, the hardware used for centralised systems could enhance surveillance activities for other diseases without
increasing access to the HIV database or compromising existing database security in any way.

Technologies such as browser-based applications, the Internet, Wide-Area Networks (WANs), and advances in data encryption technology and firewalls have made centralisation of HIV surveillance data more feasible.

New browser-based applications have numerous technical access controls, including authentication of the individual attempting access, assignment/restriction of access rights at the variable/field level, and assignment/restriction of access to functional components (role-based privileges). Use of a centralised database allows data entry and data analysis directly from the remote location while preventing access to non-authorised uses. Further, the capacity exists to assign access rights and privileges to staff just as is done in a decentralised system. In addition to these access controls, centralised systems can be configured to limit access by allowing only those connections originating from an authorised person using an authorised workstation.

A centralised database can be accessed using a WAN or the Internet, both of which have advantages and disadvantages. A WAN often uses transmission facilities provided by common carriers, such as telephone companies to establish a dedicated, private, and permanent point-to-point connection between satellite or remote offices and the central database, an option that may be cost-prohibitive for some countries. All communications between points must still be password protected, and communications must be encrypted using methods that meet the data encryption standards set forth in this guidance. Use of the Internet does not require dedicated phone lines and establishes temporary point-to-point connections over a public medium. This would be a less expensive alternative but, because the Internet is a public medium, a Virtual Private Network (VPN) must be established to guard against intrusion during communications. In addition to establishing a VPN, these communications must also be encrypted using methods that meet the data encryption standards set forth in this guidance. Additionally, firewalls must be in place to prevent unauthorised access. When properly configured, a centralised system allows each local jurisdiction complete access to their HIV data while prohibiting access by outside jurisdictions. A local jurisdiction can conduct local-level data analyses directly from a central dataset, or they may download a de-identified dataset for analysis.

If centralisation is not yet feasible, each satellite site should maintain only cases within their jurisdiction.
For matching case notifications, sites may consider the utility of maintaining limited data on out-of-jurisdiction cases receiving care and/or reported in their jurisdiction.

**Security Breaches**

**Requirement 31**
All staff who are authorised to access surveillance data must be responsible for reporting suspected security breaches. Training of non-surveillance staff must also include this directive. (GP-3)

**Requirement 32**
A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)

**Requirement 33**
A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Chief Medical Officer of the Ministry of Health. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (GP-4)

A breach may be attempted, in progress, done without negative outcome, or done with negative outcome. Attention should be paid to identifying a breach, responding to it, repairing damage, learning from the event, and if necessary revising or enhancing policies and procedures, revising or instituting training, or enhancing physical or operational security.

By keeping a log of breaches and lessons learned from investigating them, the surveillance unit will be able to detect patterns of breaches, track compliance, and incorporate improvements to the security system.

The ORP should be notified of all breaches of confidentiality (i.e., those breaches that result in the unauthorised disclosure of private information with or without harm to one or more individuals).

**Laptops and Portable Devices**

**Requirement 34**
Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held
securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (GP-1)

With the current rate of advances in technology, laptop computers and other hand-held/portable devices may common tools for HIV surveillance in the Caribbean, and may be key components of centralised surveillance systems. Unfortunately, laptops are vulnerable to theft. Although the likely target of the theft would be the device rather than the data, extreme care must be taken if the device stores HIV surveillance data or information.

If surveillance data are stored on the device's hard drive, hard drives must be removable and stored separately when the device is being transported to and from the secured area.

Alternatively, a security package that uses both software and hardware protection can be used. For example, an acceptable, though not as robust, level of protection can be achieved by using a smart disk procedure. This procedure prevents the device from booting up unless an encoded smart disk is inserted when the device is first turned on and a password is entered. Such a smart disk must not be stored with the device while in transit. The smart disk must be used in conjunction with an encryption package. Using this kind of protection scheme is critical because the device is capable of containing large amounts of sensitive information (e.g., names, addresses, dates of birth). Therefore, if a device has sensitive data on either an external storage device or hard drive, it must be taken back to the secured area at the close of business (unless out of town business travel is approved). Contingency plans should be in place and these should outline protective steps to take in case returning to the secure surveillance area is not possible. See Requirement 24 and Requirement 25. A removable drive is worth using even if data are encrypted and the laptop employs several layers of security.

Another option to consider when using laptops is to store encrypted data on an external storage device. If the device is lost or stolen, the data are protected. Unlike the laptop's hard drive, an external storage device lacks market value and is not as likely to be stolen or reused. Nonetheless, external storage devices containing patient identifiers must be encrypted when taken out of a secure area. For more information about removable and external storage devices, refer to section ‘Removable and External Storage Devices’.

With the inception of Wireless Fidelity (Wi-Fi) products, many devices can now connect wirelessly to the Internet or a LAN. This functionality introduces risks regarding devices used to collect or store surveillance
data. If these devices are not properly configured, data can be transmitted wirelessly over great distances without protection; this can result in the data being exposed to anyone with similar wireless products. Even if data are not being transmitted wirelessly but the device is capable of a wireless connection to the Internet, data stored on the device are susceptible to compromise by exposure to the Internet. For example, surveillance data may be collected in the field and stored on a laptop with Wi-Fi capability. The person collecting the data stops by a store that has a "hot spot" in order to connect to the Internet and check e-mail. The data stored on the laptop have the potential to be compromised.

Any use of Wi-Fi or similar evolving wireless technologies must be given serious consideration when developing local policies. It is strongly recommended that any local policy developed in response to Requirement 34 include explicit language regarding wireless technologies.

**Removable and External Storage Devices**

**Requirement 35**

All removable or external storage devices containing surveillance information that contains personal identifiers must:

- include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,
- be encrypted or stored under lock and key when not in use, and
- with the exception of devices used for backups, devices should be sanitised immediately following a given task.

External storage devices include but are not limited to diskettes, CD-ROMs, USB port flash drives (memory sticks), zip disks, tapes, smart cards, and removable hard drives. Deleting electronic documents does not necessarily make them irretrievable. Documents thought to be deleted often are preserved in other locations on the computer's hard drive and on backup systems. Acceptable methods of sanitising diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetising) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration). Such physical destruction would include the device, not just the plastic case around the device.
Unit 7: Confidentiality and Data Security

Unit 7 Summary

When conducting HIV surveillance, it is critical to be mindful of patient confidentiality. Persons with HIV disease are often subject to physical, legal and social harms.

Information on persons with HIV infection must be properly protected to prevent breaches of security that can result in disclosure of their HIV status. All policies developed and surveillance activities conducted should take into account the five guiding principals of data security. Countries should also work towards achieving the requirements described with regards to policies, training, physical security, data security and security breaches.

Bibliography


Annex 7.1. Additional Laptop Security Considerations

Basic Security

Choose a secure operating system and lock it down
An operating system that is secure and offers a secure logon, file level security, and the ability to encrypt data should be used. A password is considered a single-factor authentication process, but for enhanced security, commercial products can be used that change the access to a two-factor authentication. This can be achieved, for example, by using a password and an external device that must be plugged into the USB port.

Enable a strong BIOS password
The basic input/output system (BIOS) can be password protected. Some laptop manufacturers have stronger BIOS protection schemes than others. In some models, the BIOS password locks the hard drive so it cannot be removed and reinstalled into a similar machine.

Asset tag or engrave the laptop
Permanently marking (or engraving) the outer case of the laptop with a contact name, address, and phone number may greatly increase the likelihood of it being returned if it is recovered by the authorities. A number of metal tamper-resistant commercial asset tags are also available that could help the police return the hardware if it is recovered. Clearly marking the laptops may deter casual thieves.

Register the laptop with the manufacturer
Registering the laptop with the manufacturer will flag it if a thief ever sends the laptop in for maintenance. The laptop’s serial number should be stored in a safe place. In the event the laptop is recovered, the police can contact you if they can trace it back to your office.

Physical Security

Get a cable lock and use it
Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While this may not stop determined hotel thieves with bolt cutters, it will effectively deter casual thieves who may take advantage of users while their attention is diverted. Most of these devices cost between US$30 and US$50 and can be found at office supply stores or online. However, these locks only work if tethered properly to a strong, immovable, and unbreakable object.

Use a docking station
Many laptop thefts occur in the office. A docking station that is permanently affixed to the desktop and has a feature that locks the laptop securely in place can help prevent office theft. If a user is leaving the laptop overnight or for the weekend, a secure filing cabinet in a locked office is recommended.

Lock up the PCMCIA NIC cards
While locking the laptop to a desk with a cable lock may prevent laptop theft, a user can do little to keep someone from stealing the Personal Computer Memory Card International Association (PCMCIA) Network Interface Card (NIC) or modem that is inserted into the side of the machine. These cards can be removed from the laptop bay and locked in a secure location when not in use.

**Use a personal firewall on the laptop**

Once users connect to the Web from home or a hotel room, their data are vulnerable to attack, as firewall protection provided in the office is no longer available. Personal firewalls are an effective and inexpensive layer of security that can be easily installed. It is recommended that a third-party personal firewall be used to secure workstations.

**Consider other devices based on needs**

Since laptop use has become common, as has laptop theft, a variety of security-enhancing devices are now available. Motion detectors and alarms are popular items, as are hard drive locks. Biometric identification systems are also being installed on some laptop models, which allow the fingerprint to be the logon ID instead of a password. Cost, utility, and risk need to be taken into account when considering additional devices.

**Preventing Laptop Theft**

**No place is safe**

Precautions need to be taken with a laptop regardless of location, as no situation is entirely without risk. As discussed previously, the laptop should always be secured by using a cable lock or secure docking station.

**Use a nondescript carrying case**

Persons walking around a public place with a leather laptop case can be a target. A formfitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be safer. If a person is travelling in airports and train stations, small locks on the zippers of the case (especially backpacks) can be used (when not passing through security checkpoints) to prevent a thief from reaching into the bag.

**Beware of distractions**

Business travellers often use cell or pay phones in airports, restaurants, and hotel lobbies. Care needs to be taken that a laptop set down on the floor or a nearby table is not stolen while someone is engrossed in a telephone conversation.

**When travelling by air**

Sophisticated criminals can prey on travellers. When carrying a laptop, travellers need to use caution to safeguard it. When a person sets a laptop bag down for a minute to attend to other things, there may be a risk of theft. Always be aware of your surroundings because a thief could be waiting for that moment of distraction to grab a laptop (or other valuables).
**When travelling by car**
When transporting a laptop, it is safer to rent a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops should never be visible from outside of the car. Even when the laptop is in the trunk, the cable lock can be used to secure the laptop to the trunk lid so it cannot be taken easily.

**While staying in a hotel**
The hazards of leaving valuables in hotel rooms are well documented, and professional thieves know that many business travellers have laptops that can be resold. If a user keeps the laptop in the hotel room, it can be securely anchored to a metal post or fixed object.

**Make security a habit**
People are the weakest link in the security chain. If a person cares about the laptop and the data, a constant awareness of potential risks will help keep it safe. The laptop should always be locked up when it is not being used or is in storage. (A cable lock takes less time to install than it does for the PC to boot.) Use common sense when travelling and maintain physical contact with the laptop at all times. If a person is travelling with trusted friends or business associates, take advantage of the buddy system to watch each other’s equipment.

**Protecting Sensitive Data**

**Use the New Technology File System (NTFS) (proprietary to Windows operating systems)**
Assuming a user has Windows NT/2000/XP on the laptop, use the NTFS to protect the data from laptop thieves who may try to access the data. File Allocation Table (FAT) and FAT32 file systems do not support file-level security and provide hackers with an opening into the system.

**Disable the guest account**
Always double check to make sure the guest account is not enabled. For additional security, assign a complex password to the account and completely restrict logon times. Some operating systems disable the guest account by default.

**Rename the administrator account**
Renaming the administrator account will stop some hackers and will at least slow down the more determined ones. If the account is renamed, the word 'Admin' should not be in the name. Use something innocuous that does not sound like it has rights to anything. Some computer experts argue that renaming the account will not stop everyone, because some persons will use the Security Identifier (SID) to find the name of the account and hack into it. The SID is a machine-generated, non-readable binary string that uniquely identifies the user or group.
Consider creating a dummy administrator account
Another strategy is to create a local account named 'Administrator'; then give that account no privileges and a complicated 10+ digit complex password. If a dummy administrator account is created, enable auditing so a user knows when someone has tampered with it.

Prevent the last logged-in user name from being displayed
When a user presses CTRL+ALT+DEL, a login dialog box may appear that displays the name of the last user who logged into the computer. This can make it easier to discover a user name that can later be used in a password-guessing attack. This action can be disabled by using the security templates provided on the installation CD-ROM or via Group Policy snap-in. For more information, see Microsoft KB Article Q310125.

Enable EFS (Encrypting File System) in Windows operating systems
Some operating systems ship with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing the files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on folders, not just files. All files that are placed in that folder will automatically be encrypted.

Disable the infrared port on a user laptop (if so equipped)
Some laptops transmit data via the infrared port on the laptop. It is possible for a person to browse someone else's files by reading the output from the infrared port without the laptop user knowing it. Disable the infrared port via the BIOS, or, as a temporary solution, simply cover it up with a small piece of black electrical tape.

Back up the data before a user leaves
Many organisations have learned that the data on the computer is more valuable than the hardware. Always back up the data on the laptop before a user does any extended travelling that may put the data at risk. This step does not have to take a lot of time, and a user can use the built-in backup utilities that come with the operating system. If the network does not have the disk space to back up all of the travelling laptop user's data, consider personal backup solutions including external hard drives (flash sticks), CD-Rs, and tape backup—all of which can also be encrypted.

Consider using offline storage for transporting sensitive data
Backing up the hard drive before users leave can help them retrieve the data when they return from a trip, but it does not provide an available backup of the data when they are out in the field. Several vendors offer inexpensive external storage solutions that can hold anywhere from 40 MB to 30 GB of data on a disk small enough to fit easily into the pocket. By having a backup of the files users need, they can work from another PC in the event that their laptop is damaged or missing. Most of these devices support password protection and data encryption, so the files will be safe even if a user misplaces the storage disk. When travelling, users should keep these devices with them, not in the laptop case or checked baggage. For additional security, lock or encrypt the files and have them sent by a courier service to the destination hotel or office.
Annex 7.2. Additional Security and Policy Considerations

Access and Storage Devices
Establish and implement policies and procedures for using and transporting secure access devices (smart card, key FOB, etc.) and external storage devices (diskettes, USB flash drives, CD-ROM, etc.).

Accountability
Maintain a record of the movements of hardware and electronic media and any persons responsible for transporting these devices.

Application and Data Criticality Analysis
Assess the relative criticality of specific applications and data in support of other contingency plan components.

Audit Controls and Logs
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use protected electronic health information. Establish and implement policies and procedures that regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Establish and implement policies and procedures for the backup, archiving, retention, and destruction of audit logs.

Automatic Logoff
Establish and implement policies and procedures that terminate any electronic session after a predetermined period of inactivity.

Browsers
Establish and implement policies and procedures regarding browser configuration for browser-based applications and Internet usage.

Certificates
Establish server and client digital certificate transportation, generation, and use policies.

Communications
Letterhead stationery, business cards, or dedicated phone lines are used among colleagues for professional purposes, and, in these cases, references to HIV/AIDS would not jeopardise the confidentiality of any case patient. In fact, such identification may be an important part of establishing credibility with providers who report cases. Addressing both purposes (protecting confidentiality and establishing credibility) will require careful organisation and perhaps some duplication of communication mechanisms by surveillance units (e.g., one card and phone line for investigation activities and another set for providers) or the use of more generic terminology (e.g., 'Epidemiology Unit' instead of 'HIV/AIDS Surveillance Unit').
Contingency of Operations and Disaster Recovery

Establish and implement policies and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

A contingency planning policy and operations policy should address all critical aspects of contingency planning. Storage of data for backup and disaster recovery purposes should have the same if not more stringent accessibility, accountability, and encryption security requirements as a production system.

Along with the above, the following rules should be followed. They may be included in the policy or listed separately:

- Maintain list of all users and applications with access to the data. The list should include (per user or application) the day of week and the hours of the day that access will be needed. Access should be limited to these days and hours. The list should also identify those with access to identifiers.
- Conduct a monthly audit reflecting all successful/unsuccessful access. The report should include day, time of day, and length of access. It should be verified against authorised users and access requirements.
- Define administrative privileges for IT personnel (should be very limited). IT personnel need to have programme approval before accessing the data.
- Identify some form of double authentication process for accessing the data.
- Keep systems containing the data in a secured area that is clearly labelled for authorised personnel only.
- Implement column and/or row level encryption of data.
- Create a data backup plan that includes procedures to create and maintain exact copies of protected electronic health information.
- Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity (time-outs).

Emergency Access Procedures

Establish and implement policies and procedures for obtaining necessary protected electronic health information during an emergency.

Emergency Mode Operation

Establish and implement policies and procedures to enable continuation of critical business processes for protecting the security of protected electronic health information while operating in emergency mode.

Encryption and Decryption

Implement a mechanism to encrypt and decrypt protected electronic health information.

Integrity Controls

Implement security measures to ensure that electronically transmitted protected electronic health information is not improperly modified without detection until disposed of. Ensure
that any agent, including a contractor or subcontractor to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect the information.

**Internet Connectivity**
If a modem (internal or external), DSL, or cable is used on a workstation to provide access to the Internet, ensure that passwords and logon data used to access the Internet are not stored on the workstation. Most communications software has the capacity to dial a service and connect a user and even to send a password down the line. To prevent this from happening, never programme a password into the workstation. Some modems have the capability to answer the telephone as well as to make calls. Make sure users know how to tell if their modem has been placed in answering mode and how to turn off that mode. External modems normally have an indicator light labelled AA that glows if Auto Answer mode is selected. Internal modems are harder to monitor, but small utility programmes are available that can help. Call-back modems actually call the user back at a prearranged number. External modems are recommended because the ease of turning them off offers programmes the greatest degree of control.

It is highly recommends that workstations holding confidential and sensitive data that are connected to the Internet should be disconnected from the Internet except when the Internet is being used for authorised activities.

If the line is for data only, make sure that the telephone number of the line does not appear in the telephone directory and is not displayed on the telephone itself or on the wall socket.

**Intrusion Detection**
Establish and implement policies and procedures regarding intrusion detection and penetration vulnerabilities.

**Keyboard and Screen Locking**
Establish and implement policies and procedures for screen saving and keyboard locking.

**Logins and Monitoring**
Establish and implement policies and procedures for workstation logins, and designate who can request and authorise changes to a login. Establish and implement policies and procedures for monitoring login attempts and reporting discrepancies.

**Maintenance Records**
Establish and implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

**Media Disposal and Re-use**
Establish and implement policies and procedures to address the final disposition of protected electronic health information, and/or the hardware or electronic media on which
it is stored. Establish and implement policies and procedures for removal of protected electronic health information from electronic media before the media are made available for re-use.

**Networks, LANs, and WANs**
Establish and implement policies and procedures governing all servers on the network. Establish and implement policies and procedures for the documentation of network configurations and architectures. Topics to include are:

- name and location of servers
- netware protocols
- users, groups, and roles that access data and physical server
- authentication protocols
- e-mail hosting
- remote access
- web hosting
- data located on each server
- administrative safeguards

Computers used to maintain HIV surveillance information with personal identifiers should not be connected to other computers or computer systems that are located outside of the secure area until and unless the connection is deemed secure by adding multiple layers of protective measures—including encryption software, restricted access rights, and physical protections for the LAN equipment and wiring—and justifying a public health need to maintain highly sensitive data on a system that has multiple users and multiple locations. This system should operate under a certified LAN administrator, who will attest to the system's effectiveness and assume responsibility for any breach of security directly resulting from the system's failure to protect sensitive data. Internet access devices (e.g., modems and network interface cards) or cables should not be connected to any computer or computer system containing surveillance information and data unless authorised staff need Internet access as a means to enhance surveillance activities. If Internet connectivity is used for surveillance activities, specific rules of use should be provided in writing to authorised users, and they should sign a statement that they understand those rules.

**Password Management**
Establish and implement policies and procedures for creating, changing, and safeguarding passwords.

**Patching and Service Packs**
Establish and implement policies and procedures for security patching and service pack control.

**Protection from Malicious Software**
Establish and implement policies and procedures for guarding against, detecting, and reporting malicious software.
**Risk Analysis**
Establish and implement policies and procedures that require conducting a regular, accurate, and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected electronic health information held by the covered entity.

**Routers and Firewalls**
Establish and implement policies and procedures regarding router and firewall logs to capture packets that violate filter criteria. Establish and implement policies and procedures for firewall and router configuration.

**Software Inventory, Releases, Licensing, and Upgrades**
Establish and implement policies and procedures for the inventory of authorised software (including versions) that can be installed on development, training, testing, staging, and production servers and workstations.

Establish and implement policies and procedures for tracking and verifying software licenses. Establish and implement policies and procedures for pre-release and testing of software.

Establish a methodology to deploy new or upgraded software to all appropriate workstations and servers (configuration management). Establish a method for tracking the software loaded on every workstation and server.

**Testing and Revision of Plans**
Establish and implement policies and procedures for periodic testing and revision of contingency plans.

**Transmission Security**
Implement technical security measures to guard against unauthorised access to protected electronic health information that is being transmitted over an electronic communications network.

**Workstation Use**
Establish and implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access protected electronic health information.
Annex 7.3. Sample Employee Confidentiality Agreement/Oath

<Insert Name of Agency Here>

Confidentiality Agreement
As an HIV/AIDS Programme employee, subcontracted employee, student, or visiting professional, I understand that I will be exposed to some very privileged patient information. Examples of such information are medical conditions, medical treatments, finances, living arrangements, and sexual orientation. The patient's right to privacy is not only a policy of the HIV/AIDS Programme, but is specifically guaranteed by statute and by various governmental regulations.

I understand that intentional or involuntary violation of the confidentiality policies is subject to appropriate disciplinary action(s), which could include being discharged from my position and/or being subject to other penalties. By initialling the following statements I further agree that:

Initial below

_____ I will never discuss patient information with any person outside of the programme who is not directly affiliated with the patient's care.

_____ If in the course of my work I encounter facilities or programmes without strict confidentiality protocols, I will encourage the development of appropriate confidentiality policies and procedures.

_____ I will handle confidential data as discretely as possible and I will never leave confidential information in view of others unrelated to the specific activity. I will keep all confidential information in a locked cabinet when not in use. I will encrypt all computer files with personal identifiers when not in use.

_____ I will shred any document to be disposed of that contains personal identifiers. Electronic files will be permanently deleted, in accordance with current HAP required procedures, when no longer needed.

_____ I will maintain my computer protected by power on and screen saver passwords. I will not disclose my computer passwords to unauthorised persons.

_____ I understand that I am responsible for preventing unauthorised access to or use of my keys, passwords, and alarm codes.

_____ I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.

I agree to abide by the HIV/AIDS Programme Confidentiality Policy. I have received, read, understand, and agree to comply with these guidelines.

Warning: Persons who reveal confidential information may be subject to legal action by the person about whom such information pertains.

___________________________________________________ __________
Signature Date

________________________________________________________
Printed Name

___________________________________________________ __________
Supervisor's Signature Date