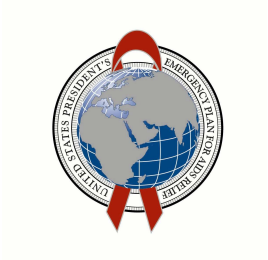


GUIDELINES on PROTECTING the CONFIDENTIALITY and SECURITY of HIV INFORMATION:

Proceedings from a Workshop

15-17 May 2006, Geneva, Switzerland

INTERIM GUIDELINES

15 May 2007

Executive Summary

A three-day Workshop was held in Geneva, Switzerland 15th-17th May 2006, which was attended by a multidisciplinary group of health professionals and community members, including people living with HIV. The Workshop's aim was to develop draft guidelines on protecting the confidentiality and security of HIV information, and to produce a plan to field test them within countries. It involved plenary sessions and small and large group work. The main conclusions, recommendations, and next steps are as follows.

E.1 For protecting data, three interrelated concepts have an impact on the development and implementation of protections for sensitive data. These are privacy, confidentiality, and security. *Privacy* is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information and provides the overall framework within which both confidentiality and security are implemented. *Confidentiality* relates to the right of individuals to protection of their data during storage, transfer, and use, in order to prevent unauthorized disclosure of that information to third parties. *Security* is a collection of technical approaches that address issues covering physical, electronic, and procedural aspects of protecting information collected as part of the scale-up of HIV services.

E.2 The public health goal is to safeguard the health of communities through the collection, analysis, dissemination, and use of health data, which must be carefully balanced with the individual's right to privacy and confidentiality. Guidelines must allow for consideration of relevant cultural norms, which may influence these policies, while ethical principles should guide decision-making regarding the appropriate use and dissemination of data. Overall, guiding principles should be based on human rights principles (section 5.1).

E.3 The purpose of defining health information confidentiality and security principles is to ensure that health data are available and used to serve the improvement of health, as well as the reduction of harm, for all people, healthy and not healthy. Pursuing this goal involves an ongoing process of refining the balance between maximizing of benefits, which can and should come from the wise and fullest use of data, and protection from harm, which can result from either malicious or inadvertent inappropriate release of individually identifiable data. Appropriate policies, procedures, and technical methods must be balanced to protect both individual and public rights.

E.4 The risk of harm following a breach of confidentiality varies with the national or local context according to levels of stigma, lack of comprehensive public health safety nets, legal traditions of respect of privacy, religious perspectives, and other local conditions.

E.5 Within countries, privacy and confidentiality laws should be in place, or developed if not already in place, and relevant parameters of privacy or confidentiality laws must be reviewed and known by those involved with the data at all administrative levels.

E.6 Countries and organizations at all levels of the healthcare system should have a written policy that defines security procedures concerning the way data are collected, stored, transferred, and released. The policies need to be implemented at all relevant levels, and staff must understand the policies and to have signed an agreement stating that they will

implement them as part of their work. This will also require training new staff and updating all staff on the relevant procedures.

E.7 Organizations at all levels of the countries' healthcare system and international organizations must identify a confidentiality and security officer (CSO) to be ultimately responsible for the confidentiality and security of HIV information within that organization.

E.8 Development and review of confidentiality and security laws and procedures should include active participation from relevant stakeholders, including people living with HIV, members of communities affected by HIV, health care professionals, information technology specialists, and legal and ethical experts.

E.9 Funding organizations should comply with these standards and have an obligation to make adequate funding available to implement them, sufficient to ensure protection of the data collected and used. Funding organization must also require that maintaining these standards is a condition for funding of any implementing partners or agencies.

E.10 The different types of HIV information – personal identified, pseudo-anonymized, anonymized, aggregated, and non-personal data – require protection. Procedures for protecting each different type of data must be explicitly described.

E.11 A number of organizational procedures need to be followed to ensure safeguards for the collection, transfer, storage, use, dissemination, and disposal of personal identified data and other information (sections 6.2 – 6.7). Policies and procedures developed must cover both paper-based and electronic systems.

E.12 The greatest threats to electronic information systems are generally not from outside attack, but rather from issues inherent in the system design and implementation. These threats fall into two categories: non-availability of data due to system failure and user errors.

E.13 Proposed next steps for completion of the guidelines include:

E.13.1 Completion of a sample Threat Analyses.

E.13.2 Development of a sample Institutional Policy and Procedure.

E.13.3 Development and piloting of a Self Assessment Program.

E.13.4 Development and application of a questionnaire in UNAIDS and PEPFAR focus countries and PEPFAR implementing partners, to determine the utility and applicability of the guidelines.

E.13.5 Obtain feedback on the interim guidelines from UNAIDS and PEPFAR focus countries and PEPFAR implementing partners, and incorporate this feedback into the final guidelines.

E.13.6 Validate the guidelines by field testing them within countries.

E.13.7 Translate the guidelines into several languages.

E.13.8 Develop strategies for building capacity to support the implementation of confidentiality and security activities in-country.

Index Page

1.0 Aim

The aim of the Workshop was to develop consensus on a draft set of guidelines to ensure the confidentiality and security of HIV related information collected for patient management and monitoring, and program and HIV services monitoring and evaluation as part of scaling-up HIV services in middle- and lower-income countries. Potential methods to implement these guidelines within countries were also discussed.

2.0 Background

As part of scaling-up HIV services in middle-and lower-income countries, increasing emphasis is being placed on the collection of information to improve patient management and monitoring as well as program or service monitoring and evaluation. Such data allow individuals to be tracked over time and between places, and enable the development of longitudinal patient-level information for clinical management. Patient-level information becomes even more important when used for program or service monitoring or evaluation. This will require information systems, whether paper-based or electronic, which ensure patient confidentiality yet allow relatively easy access to the information at both the individual and aggregate level. Implemented systems must also address issues of system availability. For example, procedures must specify the minimally acceptable hours of operation for each day, week, or month. They should also identify and manage predictable risks to data systems such as electricity interruptions, staffing shortages, and natural disasters.

When patient-level data are used for program monitoring or evaluation, guidance must address which type of data can be used and in which format; the storage, use, and dissemination of such data at the different levels of society; and their use by international organizations, while ensuring data confidentiality and security. For the workshop, five different levels of data collection were identified which warranted special attention. These included, first, the provision of both preventive and therapeutic services by non-governmental organizations (NGOs) and community groups. The second level included health and other facilities at which HIV-related information is collected in both public and private sectors. The third level included sub-national (district, regional, provincial, or state) and national administrative institutions where information is collected, stored and analyzed. The fourth level related specifically to national data repositories such as data warehouses, where information from multiple societal sectors can be stored and analyzed, and the fifth level related to information transferred to international agencies (bilateral or multilateral donors, foundations, research institutions, etc.)

When developing approaches to protecting data, a distinction should be made between providing for the physical protection of data to guard against environmental threats, and the protection needed to guard against inappropriate use of sensitive information, whether due to inadvertent or deliberate activities.

There are three interrelated concepts that have an impact on the development and implementation of protections for sensitive data. These are privacy, confidentiality, and security. While interrelated, each is distinct and each is developed and implemented in a different manner.

Privacy is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information and provides the overall framework within which both confidentiality and security are implemented. Privacy protections vary from one jurisdiction to another and are defined by law and regulations. Privacy protections provide the overall framework within which both confidentiality and security are implemented.

Confidentiality relates to the right of individuals to protection of their data during storage, transfer, and use, in order to prevent unauthorized disclosure of that information to third parties. This may have an impact on whether, within countries, informed consent is required from individuals before patient-level information can be used for program monitoring and evaluation, or whether an implicit assumption can be made that anybody using public services agrees that their information can be used to monitor and evaluate such programs in order to improve them for the whole population. If the latter, decisions have to be made whether and under what conditions nominal, anonymized or pseudo-anonymized data can be collected, stored and used. Thus, development of confidentiality policies and procedures should include discussion of the appropriate use and dissemination of health data with systematic consideration of ethical and legal issues as defined by privacy laws and regulations.

Security is a collection of technical approaches that address issues covering physical, electronic, and procedural aspects of protecting information collected as part of the scale-up of HIV services. While there are many common requirements to ensure the confidentiality and security at the various levels of healthcare provision, different levels may have specific security requirements. At each level, security discussions should include identification of potential threats to the systems and data, the likelihood of harm from any of these threats to security, development of strategies to manage each of the identified threats, and a cost and risk trade-off analysis which attempts to practically balance the risks to security and resulting harm with the resources needed to manage the risk. Security must address both protection of data from inadvertent or malicious inappropriate disclosure, and non-availability of data due to system failure and user errors.

2.1 Physical security

Episodic or longitudinal biomedical information collected as part of clinical management, be that in paper or electronic format, needs to be physically secured, such as by being stored in a locked cabinet, within a locked room, and within a secured building. Data transfer of paper-based information may include transport in locked briefcases, transmission by fax (within some additional procedural protections) or using mail services within the organization (internal-mail) or between organizations (external-mail). Electronic infrastructures which are too geographically dispersed to be physically protected, such as a wide area networks (WAN), need to be secured via commercially-available or public domain encryption and password schemas.

2.2 Electronic security

2.2.1 Data at rest: Depending on the location of where the data are stored, for instance at health facility level, the data may be in nominal or de-identified format. The latter may range from totally anonymized – where all personal identifiers and other identifying information have been stripped and data can no longer be linked to the original source of the information – to pseudo-anonymized, in which the data are stored stripped from identifiers but through a key can be traced back to the original source. The key for this may be held where the data are stored, at the site where the data originate from, or even on a portable device such as a smart card, which the patient carries.

Access to personal computers, laptops, and servers all need to be made secure through the use of passwords, key fobs, smartcards or other means of securing access to the stored information. The data may be stored in an encrypted format and contain other access controls such as passwords and user identifications. Data stored on local or wide area networks with large numbers of computers or internet access will require the use of technologies such as firewalls and routers to limit access to those entitled to the data. Different levels of access may be created depending on different purposes for the information, which is known as "role-based" access.

2.2.2 Data transfer: For electronic data, this includes the use of diskettes, CD-ROMs, memory sticks, smart cards, personal digital assistants (PDAs), telephone conversation, encrypted email, secured file transfer protocol (ftp), or secured web services. Security measures required in these situations include encryption and the use of public-private key pairs, virtual private networks (VPNs) and other relevant measures.

2.3 Procedural Security

As part of these security requirements, a written policy of security procedures needs to be produced that covers the way the data are collected, stored, transferred and released. These policies need to be accessible to and known by those involved with the data at all levels. The policies need to be implemented at the relevant levels, and staff need to sign that they have understood the policies and will implement them as part of their work. This will also involve training new staff and updating all staff on the relevant procedures. Data release policies should define the release of information for different purposes, ranging from the release of clinical information to health professionals, relatives or friends, to the release of information held in medical records or electronic databases for program monitoring and evaluation, for reporting or research.

2.4 Legal and ethical considerations

Data security and release policies must also address legal and ethical issues when determining the appropriate use and dissemination of data. To do so, relevant parameters of existing privacy or confidentiality laws must be reviewed and known by those involved with the data at all administrative levels. These include laws and regulations that authorize public health powers; privacy laws that govern the acquisition, use, storage, and disclosure of personally identifiable information; and laws addressing research on human subjects. Although models from higher-income countries may provide useful frameworks to enhance legal protections, development

of guidelines must consider the broad range or absence of applicable laws within middle- and lower-income areas.

The public health goal to safeguard the health of communities through the collection and dissemination of health data must be carefully balanced with the individual's right to privacy. Guidelines must allow for consideration of relevant cultural norms, which may influence these policies. Ethical principles should guide decision-making regarding the appropriate use and dissemination of data. Although there will likely be diverse opinions regarding acceptability of data uses, consideration of issues within the bounds of relevant ethical principles will facilitate discussions.

2.5 Published guidelines

Published material on confidentiality and security, including legislation and regulation, exists in many countries. The background material presented to workshop participants was drawn from material published in the United States, United Kingdom, and Australia. Institutional guidelines include the U.S. Centers for Disease Control and Prevention's *Technical Guidance of HIV/AIDS Surveillance Programs* and the U.S. National Institute of Standards Technology's 800 series on protecting information; the International Standards Organization (ISO); non-governmental organizations within the health-care sector, such as the North American Association of Central Cancer Registries; peer-reviewed journal articles; documentation from information technology vendors, academic publications, and publications from independent security experts.

The published guidelines cover confidentiality and security from a variety of perspectives: legal, ethical, procedural, electronic, physical, and data dissemination, and cover topics as diverse as firewall configuration and good password construction, how to protect portable electronic devices such as laptop computers, what kind of training hospitals must provide for their workers, model legislation for protecting the privacy of individuals, how to de-identify data sets so they can be safely analyzed, and whether fax machines should be used for transmitting confidential information. Most were produced within higher-income countries, and may need tailoring for adaptation within middle- and lower-income countries.

Workshop participants were provided copies of published guidelines before and during the workshop, and in many cases were contributing authors to the various publications. These proceedings largely reflect a distillation and synthesis of previously published, English-language material (Appendix 4).

3.0 Objectives

To review and critique existing material, largely developed within higher-income countries, and distil these into guidelines which can be adapted and implemented in middle- and lower-income countries to ensure confidentiality and security of patient-level information at the level of:

3.1) communities, non-governmental organizations (NGOs);
3.2) health and other facilities;
3.3) sub-national (district/regional/provincial/state) and national levels;

3.4) national data-repositories or data-warehouses;
3.5) international organizations.

4.0 Methods

A multidisciplinary group of health professionals and community members was invited to attend a 2.5-day workshop. This included country program managers; country-based information technology (IT) people; IT experts specializing in relevant areas; users of data including clinicians, statisticians or epidemiologists; ethicists; legal experts and people living with HIV from a wide variety of countries (Appendix 1).

After an introductory session on the first day (Appendix 2), the invitees were split into 5 workgroups, each focussing on a specific level of the healthcare system (sections 3.1-3.5). Having deliberated within each of the 5 groups and reported back to the other groups, a summary integrated plenary session was held on the final day, which also delineated future steps.

5.0 HIV Confidentiality and Security Principles

The purpose of defining the health information confidentiality and security principles is to ensure that health data are used to serve the improvement of health, as well as the reduction of harm, for all people, healthy and not healthy.

Pursuing this goal involves an ongoing process of refining the balance between:

a) maximizing of benefits – benefits that can and should come from the wise and fullest use of data, and
b) protection from harm – harm that can result from either malicious or inadvertent inappropriate release of individually identifiable data.[1]

These potential benefits and harms may accrue to individuals, groups, or institutions. The tremendous potential 'wealth for health' in longitudinal electronic patient health data repositories, as well as the potential for increased risk of confidentiality breach inherent in consolidated and centrally accessible data, motivates this statement of principles, which, independent of context, may help inform this balance.

One aim of government is to ensure that the best information is used to provide healthcare to the public. However, in some contexts, confidential individual health information has been used in ways harmful to the individuals concerned, and so they must be protected as well. Security against access is not an unqualified objective; legitimate access to essential data must also be secured. Appropriate policy, procedures, and technical methods must be balanced to secure both individual and public protections.

[1] The term "identifiable data" refers both to directly and indirectly identifiable data, e.g., data can be indirectly identifiable when the merging of two independent data sources leads to creation of characteristics which, when combined, have a high probability of belonging to only one individual.

The risk of harm following a breach varies with the national or local context according to levels of stigma, lack of comprehensive public health safety nets, legal traditions of respect of privacy, religious perspectives, and other local conditions.

For a society to reap a greater health benefit while minimizing risk of harm, it must improve and maintain the protection of individuals and their data. Such protection is not only improved by having established principles, laws, and policies, but is based on the mores and values of each society. It is also dependent on people living with HIV being aware of the laws and policies that exist, and of the implementation of these laws and policies. In the end, it is a universally held attitude of respectful consideration for all persons, healthy or not, that would permit the fullest disclosure without ensuing harm, and thereby renders accessible, the greatest health information for public benefit.

5.1 Guiding principles on the Confidentiality and Security of HIV information

5.1.1. The procedures that yield HIV data must conform to international ethical and legal standards. Fundamental ethical and legal standards for protecting privacy and confidentiality exist in relevant human rights instruments. The *Right to Privacy* is cited in Article 12 of the Universal Declaration on Human Rights; Article 17 of the International Covenant on Civil and Political Rights; and Article 37 of the Convention on the Rights of the Child. The HIV-related action is to ensure that HIV test results are confidential and to guarantee the right of non-disclosure to third parties.[2] The Declaration of Commitment on HIV/AIDS (UNGASS 2001) states that "the full realization of human rights for all is an essential element in a global response to HIV/AIDS" (paragraph 16). In particular, governments committed themselves to enforce legislation, regulations and other measures to ensure all the rights of people living with HIV, including privacy and confidentiality (paragraph. 58).[3]

Another source of international standards is the UNESCO *Universal Declaration on Bioethics and Human Rights.*[4] Article 9 of the Declaration, entitled Privacy and Confidentiality, states: "The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law."

Data collection that fails to conform to these standards should not be used for the program activity. Funding organizations should comply with these standards and have an obligation to make adequate funding available to implement them, sufficient to ensure protection of the data collected and used. Funding organization must also require that maintaining these standards is a condition for funding of any implementing partners or agencies.

---

[2] UNAIDS. *Report on the Global HIV/AIDS Epidemic* July 2002, p. 63.

[3] UNAIDS. *Keeping the Promise: Summary of the Declaration of Commitment on HIV/AIDS,* United Nations General Assembly Special Session on HIV/AIDS, 25-27 June, 2001, New York, p. 13.

[4] United Nations Educational, Scientific and Cultural Organization. *Universal Declaration on Bioethics and Human Rights*. Adopted by acclamation on 19 October 2005 by the 33rd session of the General Conference of UNESCO.

5.1.2 Organizations, institutions, and individuals have a duty to respect the rights of those whose identifiable data may be collected or stored. These rights include but are not limited to:

a. The right to refuse to answer questions posed by those collecting the data;
b. The right to have free a copy of their health record;
c. The right to access, review, and correct identified data that can be verified to be erroneous;
d. The right to voluntary informed consent when appropriate;
e. The right to seek redress for a perceived breach of confidentiality without negative consequences.

5.1.3 Organizations, institutions, and individuals having access to the data have an obligation to ensure that that confidentiality and security protections for identifiable information are in place.

a. Confidentiality and security protections are needed to ensure the quality of prevention, treatment, and care programs.
b. Local ownership and proper steps to ensure confidentiality and security help to provide good data for reporting upstream.
c. Measures for confidentiality and security protection should go hand in hand with community and advocacy efforts to reduce HIV-related stigma, including stigma experienced by populations most at risk.

5.1.4 HIV-related information and data collected for patient management and monitoring should be maintained in a technically and physically secure environment.

5.1.5 Individuals authorized to access HIV-related information should receive appropriate training and should be responsible for protecting confidentiality.

5.1.6 Security breaches and loss of confidentiality should be thoroughly investigated and appropriate sanctions imposed.

5.1.7 Security strategies and related laws and policies should be continuously reviewed, independently assessed, and changed when required.

5.1.8 Data may be shared between or among organizations or institutions provided that:

a. The recipient will be using the data for a legitimate health purpose;
b. The nature and amount of data shared is contingent on the reason for the data transfer, but should always be the minimum amount of data required to successfully complete the task. For example, personal identifiers should never be transmitted when a pseudo-anonymized record can complete the task;
c. The confidentiality and security measures of the receiving organization are equivalent to those of the organization which collected the data and were agreed to when the data were collected.

5.1.9 Organizations and institutions should collect only information that fulfills the clearly stated purpose(s) of the activity.

5.1.10 Organizations, institutions, and individuals have an obligation to ensure that all policies and procedures related to confidentiality and security of identifiable information should be transparent and available. This includes potential future use of routinely collected patient information, including on deceased individuals.

5.1.11 Organizations, institutions, and individuals who fail to adequately protect the confidentiality and security of identifiable information should be held accountable and appropriate remedies imposed.

5.1.12 Individual level information should not be shared with those charged with law enforcement, immigration control, management of the public welfare system, or other non-health functions without consent from the individual to whom the information relates, except in circumstances involving the threat of imminent danger of grave physical harm to individuals or populations.

5.1.13 The development and implementation of policies and procedures should be consistent with these principals, should involve persons living with HIV and other stakeholders throughout the process, and be integrated into national HIV care and treatment plans.

6.0 Technical guidelines

6.1 Types of data

While all data collected, stored and used as part of scaling-up HIV services in countries have confidentiality and security requirements, it is important to recognize the different types of data, since there are important differences in their sensitivity and in the impact on patients if confidentiality is breached. Four main different types of information can be identified:

6.1.1 *Personal Identified Data*: individual level information that, most significantly, includes personal identifiers such as names and addresses. These data are generally obtained at the point of care, where services are delivered to individuals. They are managed at community and health facilities whether sponsored by the public sector, NGOs, the private sector or international organizations. However, in some cases such data are stored in regional or national databases. This category of data also includes national identification numbers, which can be directly linked to individual patients across different databases across various social sectors, e.g., the social security number in the United States.

6.1.2 *Pseudo-anonymized Data*: this individual level information has been stripped of certain identifiers – like names, addresses, etc. In many cases, this identifying information will have been replaced with a randomized identifier or key value that can be used, if necessary, to link the record with the person's medical record maintained at an individual health care facility. Data of this type are obtained from communities, health facilities, vital statistics or other data sources. They may be transferred and managed within a data warehouse, which could be at regional or national level.

6.1.3 *Aggregated Data*: such data are based on aggregating individual level information, obtained from communities, health facilities, or data warehouses, into an indicator. They are

usually managed at the level of regional or national databases. This is also the type of information which many international organizations collect.

6.1.4 *Non-Personal Data*: all levels need to deal with information on facilities, geographic data, information on drugs and drug supplies, and other logistic information.

Some of the information through which a person's identity can be identified is listed in Box 1. Most of the guidelines described below are applicable to these different types of data, unless otherwise specified.

Box 1: A list of information through which persons could be identified in their own right or in combination.

- Name: first, middle and last name;
- Address;
- Full postal code;
- Telephone number;
- Fax number;
- Email address;
- Age or date of birth;
- Sex;
- Ethnicity;
- Social security number, welfare number or equivalent;
- Occupation;
- Employer information;
- Photographs;
- Biometric identifiers;
- Payment information (credit card number, bank account, etc.);
- Latitude and longitude of residence.

6.2 Organization and Procedures

6.2.1 Within each country, institutions must develop guidelines to ensure confidentiality and security of HIV-related information, covering all levels operative within that country's or institution's healthcare system, and the different types of data collected, stored and used. Such a policy document must be in writing and widely distributed, available both in paper and electronic formats. The policy document must specify which data can be collected for which purposes, for which data individual consent is required, as well as defining the roles of individuals or groups given access to HIV data and the type of data they have access to. Such a policy document should be developed with the collaboration of relevant stakeholders in the country, including people living with HIV.

6.2.2 This policy document must also describe the methods for the regular review of security practices for individual and program-related HIV data, including review by independent security auditors. Included in the policy should be a requirement for an ongoing review of evolving technologies to ensure that data remain secure when collected, stored, transferred, disseminated, or used through these new technologies.

6.2.3 The policy document must be readily accessible by any staff having access to medical records or confidential HIV program information at all sites where data are gathered or stored. Patients should also be informed of the existence of such policies, and should have access to them.

6.2.4 All authorized persons involved with dealing with the data, should be responsible for ensuring data confidentiality and security and for reporting suspected security breaches.

6.2.5 All authorized staff must be provided with the policy document and must receive training in maintaining the appropriate confidentiality and security measures. Once training is completed, they should annually sign a confidentiality statement indicating their understanding of the policies and their agreement to implement the policies. Newly hired staff must be trained and must sign a confidentiality statement, before access to confidential HIV data is authorized. This must be a precondition to access and use of confidential data.

6.2.6 To ensure that all authorized individuals remain knowledgeable about the security policies, every individual with access to confidential HIV data must attend data security training at regular intervals.

6.2.7 Organizations at all levels of the healthcare system must identify a professional to be ultimately responsible for the confidentiality and security of HIV information within that organization. Such Confidentiality and Security Officers (CSOs) are required for

Box 2: Summary tasks for Confidentiality and Security Officers

1.1) Identify and review all applicable guidelines. Ensure that information confidentiality and security goals are identified, meet organizational requirements, and are integrated in relevant processes;
1.2) formulate, review, and approve the guidelines adapted within the facility or organization for which they are responsible;
1.3) test, review, and validate the effectiveness of the implementation of the information confidentiality and security policy;
1.4) provide clear direction and visible management support for confidentiality and security initiatives;
1.5) advocate for the resources needed for information confidentiality and security;
1.6) approve assignment of specific roles and responsibilities for information confidentiality and security across the organization;
1.7) initiate plans and programs to maintain information confidentiality and security awareness;
1.8) ensure that the implementation of information confidentiality and security controls is coordinated across the organization.

community organizations, health facilities, regional or national databases or warehouses as well as international organizations. The potential tasks of the CSO are described in Box 2.

6.2.8 A security breach or breach of confidentiality should be reported to the proper party, including the CSO. Breaches in procedure which do not result in exposure of any confidential data to any unauthorized persons can be addressed within the facility where the breach occurred. Breaches in confidentiality, however, must be reported to the top management level of the sponsoring organization. Each breach should be investigated immediately to assess the cause and to implement remedies and prevent future breaches.

6.2.9 Policies must specify penalties for breaches in security. These should include both personnel policies within organizations for breaches resulting from any staff member's action or inaction, up to and including dismissal. This may also include legal sanctions for more serious breaches, especially in circumstances where the breach was intentional.

6.2.10 Staff access to information, whether for data collection, use, dissemination, or disposal, must be based on the role assigned to the staff member (Box 3). For example, clinical staff would need full access to individual records within their facilities, but not, usually, across facilities; district supervisors need access to data from across their districts, but not necessarily to personally identifying data, except under special circumstances such as focussed evaluations or investigation of breaches; data analysts will typically not need access to personally identifiable data.

6.2.11 Staff access to equipment and hardware used for collecting, storing, or disposing of HIV related information must be based on the role assigned to the staff member (Box 3).

6.2.12 Systems used for the authentication of staff accessing HIV related data must be robust and secure and must include procedures for withdrawing access rights when staff is no longer employed at the site.

6.2.13 Sessions on electronic systems must be set to time-out after a defined period of user inactivity.

6.2.14 All components of the system ensuring confidentiality and security need to be independently validated and tested.

6.2.15 Secure codes used as passwords for the purpose of identifying staff to a computer application need to be generated using up-to-date software engineering standards, methods and practices.

6.2.16. Access to and uses of information from medical records or HIV program information by non-members of staff must only take place within the context of a policy defining proper uses and management of the data. Such a policy will address rules for access, use, dissemination and disposal of data.

Box 3: Role based access control

The information systems developed to support HIV services involve different personnel performing a range of roles which require different functions within the information systems. These roles include those of doctors, nurses, data entry clerks, systems managers and others. It is appropriate to identify the different roles that are important for making the system work, and to identify the responsibilities and data access needs of each. While this approach has substantial benefits in defining needs for training, and for customizing system access, its primary importance in this context is that it allows for access to confidential data to be independently defined for each role, based on the needs of people in the role.

This approach restricts access to data and a system's functions to appropriately authorized users. The approach can be applied to paper and electronic systems by defining 'roles' within the system and defining for each 'role' which types of data or functions can be exercised or accessed.

It is important to note that individual users are assigned specific roles but access to a system must be authenticated using their personal identification codes. Thus, even though a person's access rights are indicated by their 'role,' it is essential to also record the user's identity when that person interacts with the data. This is needed for auditing and staff management. The data included in the activity logs are essential to investigating a breach in confidentiality.

Roles can be hierarchical so that sets of permissions can be inherited. For example, the role "medical staff" can be created for a care facility's electronic medical record system. All users who have the role "medical staff" can see the patient list. The role "physician" can be created so that only a physician can see a detailed medical record. If the role "physician" is determined from a physician being a member of "medical," then physicians are automatically allowed to view the patient list, but all medical staff cannot automatically see individual patient records.

Role based access control identifies the functions and data objects which must be controlled within a system, it defines the permissions which can be made available on these functions and objects, the roles to which the permissions are granted, and the agents to whom the roles will be assigned.

Permissions can include:

1) "view" allowing a role to see that a record exists,
2) "read" allowing a role to see the content of the object,
3) "write" to edit the content,
4) "create" to create a new object,
5) "delete" to destroy the object,
6) "execute" allowing a role to perform some system function.

Agents are generally individual users, but could also be groups of users, or external applications or software programs. Role based access control policies implement local privacy and confidentiality laws and principles. Generally speaking, they restrict access to users and roles that have direct and justifiable need for the functions and data which the access control policy protects. The access assigned to a role is generally limited to the minimum level required in order for the role to carry out its official function. The information protected is not limited to private patient information. It can also include aggregate data and de-identified or pseudo-anonymized data. Solid security methods and protocols are critical in the implementation of good access control. However, good confidentiality and privacy protection is defined by the policies which are used to implement the access control parameters themselves.

6.2.17 Risk analyses need to be performed to assess the potential security risks for security breeches at all levels including data collection, storage, analyses and dissemination and to determine the appropriate preventive measures to be taken if breeches occur. Box 4 contains an illustrative example of such risk assessments. It addresses risks to data during transmissions. A fuller discussion of potential risks and threat analyses, including potential ways to deal with these will be described in and added as an additional appendix in the final version of the Guidelines.

6.3 Collection of Personal Identified Data

6.3.1 These data are predominantly collected in community or health facility settings. When such data are collected, decisions regarding which personal data are to be collected and stored must be based on the medical needs of the patient, the requirements of public health, and the requirements of program monitoring and evaluation. Data collection from persons using community or health facility services is primarily aimed at enabling good quality treatment and care over time and between sites. The use of individual data for program monitoring and evaluation or research must be covered by culturally appropriate statutory legislation with explicit individual consent, statutory sanctioned measures to use individual data without explicit patient consent, or a combination.

6.3.2 Personal identifiable data should be collected only by people who have already signed a confidentiality agreement.

6.3.3 Confidentiality and security guidelines must protect against the disclosure of data during the data collection process, in addition to protecting data during the storage, analyses and feedback phases. For instance the conversation between patients and the personnel in charge of the collection must be done in a way that unauthorized people cannot hear the personal data shared.

6.3.4 The collection of personal data should be kept at a minimum.

6.3.5 The tool chosen for the collection must guarantee the accuracy of the data stored.

6.4 Storage of Confidential Data

6.4.1 The amount of personal data to be stored should be based on the medical needs of the patient and the requirements to adequately monitor and evaluate special programs or routine healthcare, and should not be stored longer than necessary.

6.4.2 Procedures should be in place to monitor the use of the system where the data are stored in order to detect potential or actual security breaches.

6.4.3 Threat or disaster analyses need to be performed to assess all potential events which could increase the risk of inadvertent release of data or the destruction of these data at sites housing HIV data, such as acts of vandalism, fires, earthquakes, or typhoons. Appropriate preventive measures need to be taken.

Box 4: Assessment of threats to data in transit

This describes some basic threat types related to the encoding and transport of information. It does not assume any specifics regarding technology or use of cryptographic methods and applies both to paper-based and electronic systems. The attacks described here only cover the communication itself, they do not cover attacks against the applications, the host computers, the workflows, and staff associated with their use. The consequences of security breach in data transmission can result in:

- Falsified patient information being written to the system receiving the transmission (the destination system);
- Loss of patient information at the destination system;
- Incorrect care delivery causing potential harm to the patient;
- In appropriate identification of a patient (i.e., a breach of confidentiality);
- Creation of non-existent patients;
- Abuse of the local health care system, such as illegitimate access to drugs or services;
- Disruption of institutional operations, such as loss of electronic communications.

1. Standard eavesdropping / data interception: an attacker attempts to read patient data being transported over a communications channel. This attack is effectively impossible to detect as it will have no observable effect on the communication itself. Intercepting a raw communication stream is technically easy. If data are encrypted, this attack causes no damage to individual records; however, extended monitoring of a communication channel can be used to reveal flaws in the security implementation and thus allow vulnerabilities to be discovered, which can lead to decryption of data, authentication spoofing, etc.
2. Patient record modification: an attacker attempts to modify patient information while it is in transit over a channel of communication. This attack can be detected if mechanisms are in place to validate data integrity. The level of complexity depends on encoding and transport protocols. This attack can go from easy to hard to implement.
3. Patient record block: an attacker attempts to block the transmission of a patient record, effectively preventing the destination system from receiving anything. This attack can be detected using transport protocols. This attack is generally very easy since all it involves is interrupting the communication channel.
4. Patient Record Insertion: a patient record of non-existent patient is sent to a destination system when there is no matching patient transfer. A variation on this attack is a patient record replay attack where a legitimate patient record transfer is resent by an attacker. This attack can be detected. The level of complexity depends on encoding and transport protocols. A replay attack is generally simpler to detect than a new record insertion.
5. Patient Record Request: this attack assumes that the transport protocols or the workflows support a request from a destination system for an existing patient record from a source system. The attack is essentially requesting an existing patient record when no matching patient record takes place. A variation of this is a request replay attack where a valid patient record request is replayed against a source system. Depending on the transport protocols, this attack can be easy or hard to perform. As usual, a straight replay is easier than constructing a new request. This attack is detectable.
6. Authentication Spoofing: an attacker masquerades as an authorized system in order to request or receive patient information. This attack can be detected. The complexity depends on the transport protocols, channels, and overall workflows.
7. Patient re-identification from anonymized data: an attacker uses statistical techniques to find the identity of an anonymized patient record produced for reporting or analysis purposes. This attack is effectively impossible to detect unless overt action is taken against the compromised party.

6.4.4 Rooms containing individual medical records or HIV program data, whether stored as paper documents or electronically, must be properly secured to limit unauthorized access.

6.4.5 Data being moved within sites or from site to site, whether on paper or on removable data storage equipment, need to be properly secured.

6.4.6 All removable or portable equipment need to be properly secured within facilities – room or cabinets – which are locked and appropriately monitored.

6.4.7 Fixed computers and other hardware need to be properly secured using locks and alarms.

6.4.8 Identification tags must be applied to fixed and portable equipment, so as to facilitate the creation and maintenance of an inventory and to allow detection of equipment losses. Furthermore, it is necessary to have an up-to-date inventory of all fixed and portable equipment.

6.4.9 In general, all data stored need to be backed up, usually at physically separate facilities, to prevent loss or damage to the stored data, and to enable data recovery in the event of natural disaster or other data loss. Therefore, backup policies for patient data need to ensure that backed up data are maintained with the same level of security as the original data being used for patient management.

6.4.10 Data storage must anticipate changes to storage technology over the anticipated life span of the data system. As HIV therapy is expected to be a life-long activity for infected patients, stored data (including backups) must be periodically migrated to newer storage media.

6.4.11 All additions, deletions, and modifications to electronically stored data must be recorded at all times in a separate file or log. Logs generated during this process must be secured, regularly reviewed, and safely stored.

6.4.12 Rigorous and frequent evaluation of network security is required, which should include ensuring the presence of effective firewalls or other controls where required. All computers need up-to-date anti-virus and intrusion-detection software.

6.4.13 Linking computers to different networks needs to be done within the context of preserving network security.

6.5 Use of Data

6.5.1 When data are to be used in a pseudo-anonymized form, they should be stripped of personal identifiers as soon and as close as possible to the actual source of the raw information.

6.5.2 When key values, which allow tracing back to the original medical records, are provided with the pseudo-anonymized data, such key values should be treated with the same precautions as identified data. To lower the risk of breeches of confidentiality and security, it is best that the link between the key values and personal identifiers is kept at the site where the data were originally generated, typically at the community or health facility level, with one or only a few people having access to the key.

6.5.3 Only those data shall be analyzed which have been collected and stored according to the guidelines which govern the data collection process. This can be sanctioned through individual consent or statutory regulations.

6.5.4 All staff authorized to access and use information from medical records or HIV program data must be individually held responsible for protecting the systems used to access and use the data, as well as the information itself.

6.5.5 Access for unauthorized persons to secured systems or data, for example cleaning crews, should only be granted under the strict supervision of authorized persons and only when the data are protected by adequate security measures.

6.5.6 A written policy should define the roles of individuals given access to HIV data and their level of access.

6.5.7 A written policy should outline procedures for handling mail at sites involved with HIV data and in transferring data from one site to another.

6.5.8 Workspace for individuals with access to medical records or HIV program information must also be situated within a secure area.

6.5.9 When data are transferred electronically, sending and receiving parties will need to be authenticated using public key infrastructure or two-factor authentication.

6.5.10 When data are transferred electronically, data in transit need to be encrypted using appropriate protocols. This may include message encryption, use of secured sessions, secured internet lines, or two-factor authentication.

6.6 Dissemination of Information

6.6.1 Whenever possible, release of HIV-related data should be kept to a minimum.

6.6.2 A written data release policy should exist and be reviewed at regular intervals. This needs to define the purpose and uses of HIV data, outline which data elements can be released and for which purpose, and must include provisions to protect small denominator population.

6.6.3 With increased use of mapping tools for geographic display of data analyses, data release policies must take special care not to indirectly identify individuals via too precise location on geographical displays, i.e., they must incorporate available geographic masking techniques for display of confidential information.

6.6.4 The provision of HIV program information for purposes beyond the needs of public health, or of monitoring and evaluation of services, must be contingent on an appropriate scientific protocol addressing a demonstrable need, signing of relevant confidentiality statements, and subject to ethics committee or institutional review board (IRB) approval.

6.6.5 Personal identifiable data are most likely to be sent only for clinical management issues and should be sent only by and to people who have signed the relevant confidentiality agreements.

6.6.6 Access to HIV information for non-public health purposes, for instance for legal issues, should be granted only in circumstances involving the threat of imminent danger of grave physical harm to individuals or populations.

6.6.7 Transfer of HIV data to those who maintain other disease databases or a national Health Management Information System, should be limited only to those organizations, which can demonstrate equivalent security standards.

6.7 Disposal of Information

6.7.1 If old records are going to be kept, they will need to be stored ensuring full confidentiality and security of HIV information.

6.7.2 If records are to be destroyed, both paper and electronic records should be destroyed, including all data backups.

6.7.3 If modified datasets have been provided to healthcare professionals from outside the institution, upon completion of the authorized work datasets will have to be destroyed by the professionals who analyzed them. Such parties must make a written declaration indicating that this has been done.

6.7.4 A written data archival policy should be produced.

7.0 Conclusions and Recommendations

7.1 For protecting data, three interrelated concepts have an impact on the development and implementation of protections for sensitive data. These are privacy, confidentiality, and security. *Privacy* is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information and provides the overall framework within which both confidentiality and security are implemented. *Confidentiality* relates to the right of individuals to protection of their data during storage, transfer, and use, in order to prevent unauthorized disclosure of that information to third parties. *Security* is a collection of technical approaches that address issues covering physical, electronic, and procedural aspects of protecting information collected as part of the scale-up of HIV services.

7.2 The public health goal is to safeguard the health of communities through the collection, analysis, dissemination, and use of health data, which must be carefully balanced with the

individual's right to privacy and confidentiality. Guidelines must allow for consideration of relevant cultural norms, which may influence these policies, while ethical principles should guide decision-making regarding the appropriate use and dissemination of data. Overall, guiding principles should be based on human rights principles (section 5.1).

7.3 The purpose of defining health information confidentiality and security principles is to ensure that health data are available and used to serve the improvement of health, as well as the reduction of harm, for all people, healthy and not healthy. Pursuing this goal involves an ongoing process of refining the balance between maximizing of benefits, which can and should come from the wise and fullest use of data, and protection from harm, which can result from either malicious or inadvertent inappropriate release of individually identifiable data. Appropriate policies, procedures, and technical methods must be balanced to protect both individual and public rights.

7.4 The risk of harm following a breach of confidentiality varies with the national or local context according to levels of stigma, lack of comprehensive public health safety nets, legal traditions of respect of privacy, religious perspectives, and other local conditions.

7.5 Within countries, privacy and confidentiality laws should be in place, or developed if not already in place, and relevant parameters of privacy or confidentiality laws must be reviewed and known by those involved with the data at all administrative levels.

7.6 Countries and organizations at all levels of the healthcare system should have a written policy that defines security procedures concerning the way data are collected, stored, transferred, and released. The policies need to be implemented at all relevant levels, and staff must understand the policies and to have signed an agreement stating that they will implement them as part of their work. This will also require training new staff and updating all staff on the relevant procedures.

7.7 Organizations at all levels of the countries' healthcare system and international organizations must identify a Confidentiality and Security Officer (CSO) to be ultimately responsible for the confidentiality and security of HIV information within that organization.

7.8 Development and review of confidentiality and security laws and procedures should include active participation from relevant stakeholders, including people living with HIV, members of communities affected by HIV, health care professionals, information technology specialists, and legal and ethical experts.

7.9 Funding organizations should comply with these standards and have an obligation to make adequate funding available to implement them, sufficient to ensure protection of the data collected and used. Funding organization must also require that maintaining these standards is a condition for funding of any implementing partners or agencies.

7.10 The different types of HIV information – personal identified, pseudo-anonymized, anonymized, aggregated, and non-personal data – require protection. Procedures for protecting each different type of data must be explicitly described.

7.11 A number of organizational procedures need to be followed to ensure safeguards for the collection, transfer, storage, use, dissemination, and disposal of personal identified data and other information (sections 6.2 – 6.7). Policies and procedures developed must cover both paper-based and electronic systems.

7.12 The greatest threats to electronic information systems are generally not from outside attack, but rather from issues inherent in the system design and implementation. These threats fall into two categories: non-availability of data due to system failure and user errors.

8.0 Next steps for completion of the guidelines

8.1 Completion of the sample Threat Analyses.
8.2 Development of a sample Institutional Policy and Procedure.
8.3 Development and piloting of a Self Assessment Program.
8.4 Development and application of a questionnaire in UNAIDS and PEPFAR focus countries and PEPFAR implementing partners, to determine the utility and applicability of the guidelines.
8.5 Obtain feedback on the interim guidelines from UNAIDS and PEPFAR focus countries and PEPFAR implementing partners, and incorporate this feedback into the final guidelines.
8.6 Validate the guidelines by field testing them within countries.
8.7 Translate the guidelines into several languages.
8.8 Develop strategies for building capacity to support the implementation of confidentiality and security activities in-country.

APPENDIX 1 List of Participants

Christopher BAILEY
Coordinator
EIP/KMS/KCS
WHO
20 Avenue Appia
Geneva 27, CH-1211, Switzerland
Telephone: 41 22 791 1451
Email: baileych@who.int

Eddy BECK
Senior Technical Officer
Office of Monitoring and Evaluation
UNAIDS
20 Avenue Appia
Geneva 27, CH-1211, Switzerland
Telephone: 41 22 791 5521
Facsimile: 41 22 791 4798
Email: becke@unaids.org

Philip BOUCHER
Web Development Officer
ËIP/KMS
WHO
20 Avenue Appia
Geneva 27, CH – 1211
Telephone: 41 22 791 3688
Email: boucherp@who.int

Omprakash CHANDNA
Principal IT and Information Officer
Ministry of Health
Pvt Bag 0038, Gaborone, Botswana
Telephone: 267 3170585 extn 2096/ 267 3974720
Email: ochandna@gov.bw

Shabani CISHAHAYO
Head
IT and Applied Statistics Unit
C/o Treatment and Research AIDS Center (TRAC)
Boulevard de la Révolution
B.P 2717 Kigali, Rwanda
Telephone: +250578472
Facsimile: + 250 578473
Mobile No. +250 08503379
Email: cishahayos@tracrwanda.org /cishabani@yahoo.fr

Evan COLLINS
Hassle Free Clinic
#304-833 King Street West
Toronto, Ontario, Canada M5V 1N9
Telephone: 1 416 603 6027
Facsimile: 1 416 922 2018
Email: ecollins@interlog.com

Nicolas DE KERORGEN
Global AIDS Program
Centers for Disease Control and Prevention
Corporate Boulevard – Atlanta
GA 30329 U.S.A.
Tel 1 404 639 8651
Fax 1 404 639 8114
Email: fju9@cdc.gov

Paul DE LAY
Director, Monitoring and Evaluation
UNAIDS
20 Avenue Appia
Geneva 27, CH-1211, Switzerland
Telephone: 41 22 791 4534
Facsimile: 41 22 791 4798
Email: delayp@unaids.org

Lance GABLE
Senior Fellow
Center for Law and the Public's Health Georgetown University Law Center
600 New Jersey Avenue, NW Washington, DC 20001
Tel: (202) 662-9281
Email: gable1@law.georgetown.edu

Gisèle GATARIKI
Legal Adviser, CNLS
P.O.Box 7162, Kigali, Rwanda
Mobile No. +250 0851 517434
Email: ggatariki@yahoo.com

Maria Lorena DI GIANO
Lawyer, Human Rights and HIV/AIDS
Argentinian Network of Women Living with HIV/AIDS
Bartolomé Mitre 2815
Piso 4, oficina 404, Capital Federal
Buenos Aires, Argentina
Telephone: 54 223 4711822 & 54 223 4761804
Mobile: 54 223 154233278
Email: loredigiano@hotmail.com ; lorenadigiano@copetel.com.ar

Cledy Eliana DOS SANTOS
National AIDS Program
SEPN 511 – Bloco C
70.750-543 Brasilia, Brazil
Telephone: +55 61 448 884-06
Fax: +55 61 448 8224
Email: eliana@ads.gov.br

Nathan HEARD
Public Health Geospatial Analyst
Humanitarian Information Unit
Bureau of Intelligence and Research
US Department of State
SA-44, room 602
301 4th Street SW
Washington DC 20547, USA
Tel: +1 202 203 7788
Email: HeardNJ@state.gov

Chika HAYASHI
Department of HIV/AIDS
WHO
20 Avenue Appia
Geneva 27, CH-1211, Switzerland
Telephone: 41 22 791 3910
Email: hayashic@who.int

Beri HULL
Global Advocacy Officer
Access to Care, Treatment and Support
International Community of Women Living with HIV/AIDS
1345 Emerald Street
20002 NE Washington, D.C.
United States of America
Telephone/Facsimile: 1 202 397 8488
Email: beri@icw.org

Natalya IVANASHEVA
Federal Institute for Organization and
IT'S Development of Health Services of
The Federal Agency for Health and
Social Development
Moscow, Russia
Telephone: 007 495 618 11 09
Facsimile: 007 495 218 32 68
Email: infoservice@svitonline.com ; ivanna@mednet.ru

Kevin KINSELLA
Special Assistant
International Programs Center
Washington Plaza 2, Room 312
U.S. Census Bureau
Washington, DC 20233, USA
Tel: +1 301 763 1457
Facsimile: +1 301 457 3034
Email: kevin.g.kinsella@census.gov

Svilen KONOV
HIV i-Base
3rd Fllor East
Thrale House
44-46 Southwark Street
Bankside, London SE1 1UN, UK
Telephone: 020 7407 8488
Facsimile: 020 7407 8489
Email: svilen.konov@i-base.org.uk

Anna KOROTKOVA
Head of the M&E Center of the Federal
Research Institute of Health Care Organization and IT Development
Russian Federation
Telephone:007 495 68 11 11 09
Mobile: 007 916 808 5709
Fascimile: +7 495 618 11 09
Email: korotkova_anna@mednet.ru

Ruth MACKLIN
Department of Epidemiology and Social Medicine
Albert Einstein College of Medicine 1300 Morris Park Avenue
10461 Bronx, New York, United States of America
Telephone: 1 718 430 3574
Facsimile: 1 718 430 8780
Email: Macklin@aecom.yu.edu

Olena G. MALYGINA
Senior Commercial Officer
SEC « Infroservice »
Moskow Av. 21, Office 419
Kyiv, Ukraine 04073
Tel : +38 044 490 3556
Email : iso@nbi.com.ua

Rosemary MCKAIG
Epidemiologist
NIAID/DAIDS/BSP Epidemiology Branch, NIH

6700B Rockledge Dr
Mailstop 7626, Room 4216
Bethesda, MD 20892
Telephone: 1 301 594 6620
Facsimile: 1 301 402 3211
Email: rmckaig@niaid.nih.gov

Debra MOSURE
Deputy Associate Director for Science
Global AIDS Program
Centers for Disease Control and Prevention
1600 Clfton Rd. MS E41, Atlanta, GA 30333
Tel: +1 404 639 1857
Fax: +1 404 639 4268
Email: djm1@cdc.gov/ DMosure@cdc.gov

Lydia MUNGHERERA
Programme Officer/Training
TASO Headquarters Mulago
Kampala
P.O. Box 10443, Uganda
Telephone: 256 41 532580
Facsimile: 256 41 541288
Mobile: 256 77 448102
Email: mungherera@tasouganda.org & lydiamng@yahoo.co.uk

Dennis NASH
Columbia University, Mailman School of Public Health
Associate Professor of Epidemiology - Department of Epidemiology
Directory, Monitoring, Evaluation and Research- International Centre for AIDS Care and Treatment Programs
722 W. 168th St, Room 706
New York, NY USA 100312
Tel : +1 212 342 2912
Email : dn2145@columbia.edu

Rachel ONG
Asia Pacific Network of People Living with HIV/AIDS
Hua Cheng Apartments No. 16 Sizhaosi Road Block number 3, Unit 4 (Jiahuazuo), Room 602, Chongwen District
100600 Beijing, China
Telephone: 662 254 6090/1
Facsimile: +86 10 632 96911
Mobile: +86 138 013 72 759
Email: Rachel.ong.pcb@gmail.com

John PUVIMANASINGHE
Monitoring and Evaluation Specialist
Department of HIV/AIDS Prevention and Care

Ministry of Health
Private Bag 0038
Gaborone
Botswana
Telephone: 267 3973380 and 267 3903553
Email: puvimana@yahoo.com

Xen SANTAS
Centers for Disease Control and Prevention
Global AIDS Program
Mailstop E-30 1600 Clifton Road MSE41
30333 Atlanta, Georgia
United States of America
Telephone: 1 404 639 2036
Email: xms1@cdc.gov

José Américo SERAFIM
Secretary of Health (Bahia) DATASUS
Ministry of Health
Av.Luiz Viana 2306 –Lt.4-Qd.B-
Rio das Pedras-Imbui 41,730-066
Salvador, Brazil
Email: jaserafim@gmail.com

Catherine SCHENCK-YGLESIAS
Senior Health Informatics Advisor
Office of HIV/AIDS
U.S. Agency for International Development
1300 Pennsylvania Ave., N.W.
Washington, D.C. 20523
Telephone: (202) 712-1006
Fax: (202) 216-3409
E-mail: cschenck@usaid.gov

Mark SHIELDS
Centers for Disease Control and Prevention
Information System, M&E, CDC/GAP
American Embassy
Lusaka, Zambia
Telephone: 260 1 250 955
Email: mark@healthyafrica.net; shields@zamnet.zm

Patricia SWEENEY HARDY
Centers for Disease Control and Prevention
HICSB/DHAP/NCHSTP
1600 Clifton Road MS-E47
Tel: 1 404 639 2047
Atlanta, GA 30341
Email: pas3@cdc.gov

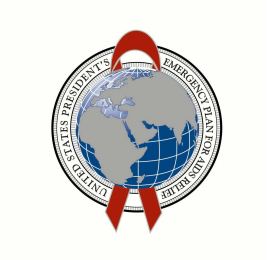
Igor TOSKIN
Monitoring and Evaluation Adviser
Office of Monitoring and Evaluation (EVA)
UNAIDS
20 Avenue Appia
Geneva 27, CH1211
Switzerland
Telephone: 41 22 791 5096
Facsimile: 41 22 791 4798
Email: toskini@unaids.org

Mead WALKER
Consultant
Mead Walker Consulting
1199 Hopewell Road
Downingtown, PA 19335
United States of America
Tel: 610 518 6259
Email: dmead@comcast.net

Francoise WELTER
GNP +
PO Box 11726
1001 GS Amsterdam
Telephone: + 31 20 423 4114
Facsimile: + 31 20 423 4224
Email: fwelter@gnpplus.net

Patrick WHITAKER
Programme Development Adviser
Country Response Information System
UNAIDS
20 Avenue Appia
Geneva 27, CH-1211
Switzerland
Telephone: 41 22 791 1372
Facsimile: 41 22 791 4798
Email: whitakerp@unaids.org

Steven YOON
Epidemiologist
Global AIDS Program
Centers for Disease Control and Prevention
Mailstop E-30 1600 Clifton Road MSE41
30333 Atlanta, Georgia
United States of America
Phone: 404-639-8331
Email: say7@cdc.gov; syoon@cdc.gov



APPENDIX 2: PROTECTING the CONFIDENTIALITY and SECURITY of HIV INFORMATION WORKSHOP AGENDA 15-17 May 2006, Geneva, Switzerland

Day One: Moderator – Steve Yoon

8.30 – 9.00 Registration
9.00 – 9.15 Welcome: Paul De Lay (UNAIDS), Xen Santas (PEPFAR)
9.15 – 9.45 Objectives of Workshop: Eddy Beck
Description of Framework: Xen Santas
9.45 – 10.30 Country presentations :
Botswana: John Puvimanasinghe/ Omprakash Chandra
Brasil: Cledy Eliana Dos Santos/ José Américo Serafim
Russia: Anna Korotkova/ Natalya Ivanasheva
10.30 – 10.45 Provider and user of services issues: Lydia Mungherera
10.45 – 11.15 Coffee
11.15 – 11.45 Ethical issues: Ruth Macklin.
11.45 – 12.15 Legal issues: Lance Gable.
12.15 - 12.50 Discussion
12.50 – 13.00 Working group logistics: Eddy Beck/Xen Santas
13.00 – 14.00 Lunch
14.00 – 17.00 Working groups (5) work
18.30 Reception

Day Two: Moderator - Eddy Beck

9.00 – 13.00 Working groups (continued)
13.00 – 14.00 Lunch
14.00 – 18.30 Report back of individual Working groups
14.00 – 16.00 Working groups 1-3 and discussion
16.00 – 16.30 Coffee
16.30 – 18.30 Working groups 4& 5 and discussion

Day Three: Moderator - Xen Santas

9.00 – 11.00 Similarities and differences at different levels: Mark Shields
11.00-11.30 Coffee
11.30- 13.00 Next steps and time-lines.
13.00 Closure: Paul De Lay

APPENDIX 3 GLOSSARY

Access The ability or the means necessary to read, write, modify, or communicate data/information. To gain entry to a data system in order to read or write data. The entrance to the Internet or other online service or network.

Access control A cohesive set of procedures (including management, technical, physical, and personnel procedures) that are designed to assure to a given level of reliability that an individual:

- is the person he or she claims to be (authentication),
- has a verified need to have access to the information system,
- has been authorized to perform the action or access the data, and
- is doing so from an authorized place using an authorized process.

AES (Advanced Encryption Standard) In cryptography, the Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the U.S. government. It is expected to be used worldwide and analyzed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001 after a 5-year standardization process.

The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

Aggregated data Information, usually summary statistics, which may be compiled from personal information, but is grouped in a manner to preclude the identification of individual cases. An example of properly aggregated data might be, “Whiteacre County reported 1,234 cases of AIDS during 1997 among Hispanics.” An example of improperly aggregated data might be, “Blackacre County reported 1,234 cases of AIDS during 1997 among Hispanics and 1 case among American Indians.”

Analysis data, datasets, or database A dataset created by removing personal data (e.g., names, addresses, postal codes, and telephone numbers) so the record or records cannot be linked to an individual, but still allow the remaining data to be analyzed.

Antivirus program A software program designed to protect a computer and/or network against computer viruses. When a virus is detected, the computer will generally prompt the user that a virus has been detected and recommend an action such as deleting the virus.

Audit An independent examination of information systems and processes to detect unauthorized activities.

Audit log A chronological listing of access to information resources. Items that are typically logged include: user ID, time of access, resources that were accessed, device used to access the information and modifications that were made.

Authentication Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message. Authentication depends on four classes of data, generally summarized as 'what you know,' 'what you have,' 'what you are,' and 'what you do.'

Authorized access As determined by the CSO or a designee, the permission granted to individuals to see confidential data that potentially could be identifying or linked to an individual. The CSO or designee should make these determinations according to role-based or need-to-know responsibilities.

Authorized personnel Those individuals employed by the program who, in order to carry out their assigned duties, have been granted access to confidential information. Authorized personnel must have a current, signed, approved, and binding nondisclosure agreement on file.

Availability The accessibility of a system resource in a timely manner; for example, the measurement of a system's uptime or accessibility via existing communications infrastructure. Availability is one of the six fundamental components of information security.

Biometrics The biological identification of a person, which includes characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges, and the dynamics of handwritten signatures. Biometrics is a more secure form of authentication than typing passwords or smart cards, which can be stolen; however, some forms have relatively high failure rates. Biometric authentication is often a secondary mechanism in two-factor authentication (the first being a password)

BIOS (basic input/output system) The built-in software that determines what a computer can do without accessing programs from a disk. On personal computers, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. Passwords can be added to the BIOS.

The BIOS is typically placed in a Read-Only Memory (ROM) chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by disk failures. It also makes it possible for a computer to boot itself. Because Random-Access Memory (RAM) is faster than ROM, many computer manufacturers design systems so that the BIOS is copied from ROM to RAM each time the computer is booted. This is known as shadowing. Many modern PCs have flash BIOS, which means that the BIOS has been recorded on a flash memory chip, which can be updated if necessary. Access to a computer’s BIOS can often bypass other security controls on that computer.

Breach A breach is a condition of departure from established policies or procedures. A breach can only be understood in view of a written reference point that describes the desired condition and the link between that condition and the objectives associated with maintaining the condition. A breach is an infraction or violation of a standard, obligation, or law. A breach in data security would include any unauthorized use of data, including de-identified data. A breach, in its broadest sense, may be caused by an act of God, a person, or an application/system and may be malicious in nature or purely unintended. An example of a malicious breach would be if staff intentionally, but without authorization, released patient names to the public. An example of an unintended breach would be if patient records were inadvertently left in a public area to which unauthorized persons have access. A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor infraction, like forgetting to lock a file drawer containing sensitive information (even if inside a secure area), constitutes a breach of security protocol as compared with a breach of confidentiality.

Other examples of possible breaches:

- A hacker gains access to an internal machine via the Internet or a dial-up connection.
- A trusted programmer introduces a program into the production environment that does not behave within expected limits.
- A technician creates a backdoor into the operation of a system, even for positive and beneficial reasons, that alters the information protection provided.
- After having been entered into a computerized file, confidential forms are left for removal in the standard paper waste process in an openly accessible location.

Breach of confidentiality A security infraction that results in the release of private information with or without harm to one or more individuals.

Certificate See Digital certificate.

CDC the U.S. Centers for Disease Control and Prevention

Certification authority or certificate authority An organization that issues digital certificates (digital IDs) and makes its public key widely available to its intended audience.

Checksum A value used to ensure data are stored or transmitted without error. It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data. When the data are retrieved from memory or received at the other end of a network, a new checksum is computed and matched against the existing checksum. A non-match indicates an error. Just as a check digit tests the accuracy of a single number, a checksum tests a block of data. Checksums detect single bit errors and some multiple bit errors, but are not as effective as the Classes, Responsibilities, and Collaborations (CRC) design method. Checksums are also used by antivirus software to determine if a file has changed since the last time it was scanned for a virus.

Cipher text Data that have been coded (enciphered, encrypted, encoded) for security purposes. Contrast with *plain text* and *clear text*.

CISSP The Certified Information Systems Security Professional (CISSP) exam is designed to ensure that someone handling computer security for an organization or client has mastered a standardized body of knowledge. The certification was developed and is maintained by the International Information Systems Security Certification Consortium (ISC^2). The exam certifies security professionals in 10 different areas:

1. Access control systems and methodology
2. Application and systems development security
3. Business continuity planning & disaster recovery planning
4. Cryptography
5. Law, investigation, and ethics
6. Operations security
7. Physical security
8. Security architecture and models
9. Security management practices
10. Telecommunications and networking security

Clear text Same as *plain text*.

Collection The process of gathering or obtaining personal health information. Information can be obtained directly - for example, from a client's authorized legal representative or another care provider.

Confidential information Any information about an identifiable person or establishment, when the person or establishment providing the data or described in it has not given consent to make that information public and was assured that such data would not be made public when the information was collected.

Confidential record A record containing private information about an individual or establishment.

Confidentiality The ethical principle or legal right that a physician or other health professional will hold secret all information related to a patient, unless the patient gives consent permitting disclosure.

Confidentiality and Security Officer (CSO) The official who accepts overall responsibility for implementing and enforcing these security standards and who may be liable for breach of confidentiality. The CSO should be a high-ranking official, for example, a division director or department chief over HIV/AIDS monitoring and evaluation. This official should have the authority to make decisions about program operations and should serve as one of the contacts for public health and medical professionals as well as the HIV-affected community on policies and practices associated with HIV/AIDS data collection activities. The CSO is responsible for protecting data as they are collected, transmitted, stored, analyzed, and released and must certify annually

that all security program requirements are being met. The organization's security policy must indicate the CSO by name.

Consent Voluntary agreement with what is being done or proposed (expressed or implied) by another.

Cookies Data created by a web server that are stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the web site to identify users and keep track of their preferences. They are commonly used to maintain the state of the session. The cookies contain a range of Uniform Resource Locators (URLs, or addresses) for which they are valid. When the web browser or other Hypertext Transfer Protocol (HTTP) application sends a request to a web server with those URLs again, it also sends along the related cookies. For example, if the user ID and password are stored in a cookie, it saves the user from typing in the same information all over again when accessing that service the next time. By retaining user history, cookies allow the web site to tailor the pages and create a custom experience for that individual. A lot of personal data reside in the cookie files on the computer. As a result, this storehouse of private information is sometimes the object of attack. A browser can be configured to prevent cookies, but turning them off entirely can limit the web features. Browser settings typically default to allowing first party cookies, which are generally safe because they are only sent back to the web site that created them. Third party cookies are risky because they are sent back to sites other than the one that created them. To change settings, look for the cookie options in the Options or Preferences menu within the browser.

Cookie poisoning The modification of or theft of a cookie in a user's machine by an attacker in order to release personal information. Cookies that log onto password-protected web sites automatically send username and password. Thieves can thus use their own computers and confiscated cookies to enter victims' accounts.

Cryptography The conversion of data into a secret code for transmission over a public network. The original text or plain text is converted into a coded equivalent called cipher text via an encryption algorithm. The cipher text is decoded (decrypted) at the receiving end and turned back into plain text. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 256 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and thus the longer it would take to break the code. The data are encrypted or locked by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to unlock the code and restore the original data.

Cryptographic key A numeric code that is used to encrypt text for security purposes.

Data stewards Refers to individuals responsible for the creation of the data used or stored in organizational computer systems. The data steward determines the appropriate sensitivity and classification level and reviews that level regularly for appropriateness. The data stewards have final responsibility for protecting the information assets and are responsible for ensuring the information assets under their control adhere to local policies. The data steward is one or more of the following:

- The creator of the information
- The manager of the creator of the information
- The receiver of external information
- The manager of the receiver of the external information

De-identification Data records are de-identified when these record are stripped of individual data elements which are directly related to an individual or the individual's relatives, employers, or household members. This includes both the obvious identifiers and those that might not be so apparent. Examples include removing reference to geographic subdivisions smaller than a state (street address, city, county, precinct, etc.), including postal codes; removal from dates directly related to the individual, all elements of dates except the year (date of birth, admission date, discharge date, date of death, etc.); deletion of national identifiers such as the U.S. social security numbers; medical record numbers; health plan numbers; vehicle identification/serial numbers, including license plate numbers; and any other unique identifying number, characteristic, or code. De-identification can be accomplished either by removing entirely a specific list of data elements, or alternatively via aggregating some of these variables (e.g., aggregating dates into years, or geographic locations into states) such that the number of persons in each aggregated unit is sufficiently large (e.g., above 20,000 persons).

Denial of service (DoS) A DoS attack is a form of attacking another computer or organization by sending millions or more requests, e.g. login requests, every second, causing the network to slow down, cause errors, or shut down. Because it is difficult for a single individual to generate a DoS attack, these forms of attacks are often created by another organization and/or worms that run surreptitiously on third-party computers to create a DoS attack.

DES (Data Encryption Standard) An algorithm that encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits). It takes a 64-bit block of plain text as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher. DES is less secure than the newer AES (Advance Encryption Standard), which uses a longer key length (at least 128 bits) and different encryption algorithm.

DHHS the U.S. Department of Health and Human Services.

Digital certificate The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called digital IDs, digital certificates are issued by a trusted third party known as a certification authority or certificate authority (CA).The CA verifies that a public key belongs to a specific organization or individual, and the certification process varies depending on the level of certification and the CA itself, but should include some method of non-online verification of identity, such as the visual inspection of a driver's license, notarization, or fingerprints. The digital certificate typically uses the X.509 file format and contains CA and user information, including the user's public key. The CA signs the certificate by creating a digest, or hash, of all the fields in the certificate and encrypting the hash value with its private key. The signature is placed in the certificate. The process of verifying the signed certificate is done by the

recipient's software such as a web browser or e-mail program. The software uses the widely known public key of the CA to decrypt the signature back into the hash value. If the decryption is successful, the identity of the user is verified. The software then recomputes the hash from the raw data (clear text) in the certificate and matches it against the decrypted hash. If they match, the integrity of the certificate is verified. A signed certificate is typically combined with a signed message, in which case the signature in the certificate verifies the identity of the user while the signature in the message verifies the integrity of the message content. The fact that the message is encrypted ensures privacy of the content. The CA keeps its private key very secure, because if it were ever discovered, false certificates could be created.

Digital signature A digital guarantee that a file has not been altered, as if it were carried in an electronically sealed envelope. The signature is an encrypted digest (one-way hash function) of the text message, executable or other file. The recipient decrypts the digest that was sent and recomputes the digest from the received file. If the digest matches the file, it is proven to be intact and tamper free as received from the sender.

Disaster recovery A plan for duplicating computer operations after a catastrophe occurs, such as a fire, flood, earthquake, or vandalism. It includes routine off-site backup as well as a procedure for activating necessary information systems in a new location.

Disclosure The release of personal health information to a third party for specific and defined purposes.

Distributed denial of service On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker (or cracker) begins a DDoS attack by exploiting vulnerabilities in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple (sometimes thousands of) compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack including the final target and the systems controlled by the intruder.

EMR (electronic medical record) An electronic patient record that resides in a system specifically designed to support users by providing accessibility to complete and accurate data, alerts, reminders, clinical decision support systems, links to medical knowledge, and other aid

Encryption The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information, and the most commonly available systems involve public key and symmetric key cryptography. A public key system uses a mathematically paired set of keys, a public key and a private

key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual. A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. Under both systems, the larger the key, the more robust the protection.

Encrypting File System (EFS) A feature of the Windows 2000 operating system (and later) that lets any file or folder be stored in encrypted form and decrypted only by an individual user and an authorized recovery agent. EFS is especially useful for mobile computer users, whose computer (and files) are subject to physical theft, and for storing highly sensitive data.

Evaluation An activity or activities intended to determine the significance, worth, or condition of, usually by careful appraisal and study

FAT32 (file allocation table) The method that the operating systems use to keep track of files and to help the computer locate them on the disk. Even if a file is fragmented (split up into various areas on the disk), the file allocation table still can keep track of it. FAT32 is an improvement to the original FAT system, since it uses more bits to identify each cluster on the disk. This helps the computer locate files easier and allows for smaller clusters, which improves the efficiency of the hard disk. FAT32 supports up to two terabytes of hard disk storage.

Firewall A method for implementing security policies designed to keep a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate an organization's public web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise. In practice, many firewalls have default settings that provide little or no security unless specific policies are implemented by trained personnel. Firewalls installed to protect entire networks are typically implemented in hardware; however, software firewalls are also available to protect individual workstations from attack. While much effort has been made towards excluding unwanted input to the internal network, less attention has been paid to monitoring what goes out. Spyware is an application that keeps track of a user's Internet browsing habits and sends those statistics to a web site.

The following are some of the techniques used in combination to provide firewall protection:

1. Network Address Translation (NAT) Allows one Internet Protocol (IP) address, which is shown to the outside world, to refer to many IP addresses internally, one on

each client station. This service performs the translation back and forth. NAT is found in routers and is built into Windows Internet Connection Sharing (ICS).
2. Packet Filter: Blocks traffic based on a specific web address (IP address) or type of application (e-mail, File Transfer Protocol [FTP], web, etc.), which is specified by port number. Packet filtering is typically done in a router, which is known as a screening router.
3. Proxy Server: Serves as a relay between two networks, breaking the connection between the two. Also typically caches web pages.
4. Stateful Inspection: Tracks the transaction to ensure that inbound packets were requested by the user. Generally these can examine multiple layers of the protocol stack, including the data, if required, so blocking can be made at any layer or depth.

Geographic masking techniques Techniques which allow the performance of meaningful analysis of geographic information, while protecting the patient's privacy and confidentiality. Several countries, including the U.S. have passed legislation which requires certain data to be masked (i.e., removed) from publicly available data sets in order to protect confidentiality.

HIPAA Health Insurance Portability and Accountability Act of 1996. A law enacted by the U.S. Congress which aims to protect health insurance coverage for workers and their families when they change or lose their jobs. The Act's "Administrative Simplification" (AS) provisions require the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers with the United States. These provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

HIS (Health Information System) The resources, devices, and methods required to optimize the acquisition, storage, retrieval, transmission, and use of information within the health care sector at a national level.

Identifiable data see Personal Identifiable data

Identity Whatever makes an individual recognizable and distinguishable from all others

Individual "Individual," in relation to personal health information, means the individual, whether living or deceased, with respect to whom the information was or is being collected or created

IETF (Internet Engineering Task Force) The body that defines standard Internet operating protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP). The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFC).

Information integrity The information is accurate, reliable and suitable for its purpose.

Information security Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

IPSec (internet protocol security) A security protocol from the IETF that provides authentication and encryption over the Internet. Unlike Secure Sockets Layer (SSL), which secures communications between two applications, IPSec secures everything in the network. Also unlike SSL, which is typically built into the web browser, IPSec requires a client installation. IPSec can access both web and non-web applications, whereas SSL requires a work around for non-web access such as file sharing and backup. Since IPSec was designed for the IP protocol, it has wide industry support and has become the standard for virtual private networks (VPNs) on the Internet.

ISO (**International Organization for Standardization)** An international standard-setting body composed of representatives from national standards bodies. Founded on February 23, 1947, the organization produces world-wide industrial and commercial standards, the so-called ISO standards. It is the world's largest developer of standards (mainly technical): more than 16,000 international norms in total.
Participants include several major corporations and at least one standards body from each member country. ISO is not an acronym; it comes from the Greek word *ίσος* (*isos*), meaning "equal".

IT (information technology) A broad subject concerned with the use of technology in managing and processing information, especially in large organizations.
In particular, IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information. For that reason, computer professionals are often called IT specialists or business process consultants, and the division of a company or university that deals with software technology is often called the IT department. Other names for the latter are information services (IS) or management information services (MIS), managed service providers (MSP)

Kerberos A security system developed at the Massachusetts Institute of Technology that authenticates users. It does not provide authorization to services or databases; it establishes identity at logon, which is used throughout the session.

Key See Cryptographic key.

Key fob An electronic device that provides one part of a three-part match to log in over an non-secure network connection to a secure network. The device may have a keypad on which the user must also enter a secret personal identification number (PIN) in order retrieve an access code, or it could be a display-only device such as a VPN token that algorithmically generates security codes as part of a challenge/response authentication system. The most well-known example of the latter type is RSA's SecurID token.

Keystroke logger A program or hardware device that captures every key depression on the computer. Also known as keystroke cops, they are used to monitor an employee's

activities by recording every keystroke the user makes, including typos, backspacing, and retyping.

LAN (local area network) Any computer network technology that operates at high speed over short distances (up to a few thousand meters). A LAN may refer to a network in a given department or within a given firm or campus. It differs from computer networks that cross wider geographic spaces such as those networks on a wide area network (WAN). A LAN does not use the public arteries of the Internet like intranets and virtual private networks.

Management controls Controls that include policies for operating information systems and for authorizing the capture, processing, storage, and transmission of various types of information. They also include training of staff, oversight, and appropriate and vigorous response to infractions.

Monitoring and evaluation A management tool that is built around a formal process for evaluating performance and impact using indicators that help measure progress toward achieving intermediate targets or ultimate goals of a project implementation. Monitoring systems comprise procedural arrangements for regular, systematic data collection, analysis, and reporting. An evaluation typically analyzes information in order to assess value, worth, or impact of the project. Additionally it looks at the dynamics of developmental interventions and identifies the reasons for both success and failure, and how one can learn from both.

Need-to-know access Under exceptional circumstances that are not stipulated in program policies, the case-by-case granting or denying of authorized access to case-specific information. This type of access is not routine; but rather it is for unusual situations and occurs only after careful deliberation by the CSO in concurrence with other public health professionals.

NIST (National Institute of Standards and Technology) Located in Washington, DC, it is the standards-defining agency of the U.S. government; formerly, the National Bureau of Standards. See http://www.nist.gov.

NTFS (NT File System) One of the file systems for the Windows NT operating system (and later). Windows NT also supports the FAT file system. NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files. NTFS files are not accessible from other operating systems such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

OMB U.S. Office of Management and Budget.

Patch management The installation of patches from a software vendor onto an organization's computers. Patching thousands of PCs and servers is a major issue. A patch should be applied to test machines first before deployment, and the testing

environments must represent all the users' PCs with their unique mix of installed software.

PEPFAR The U.S. President's Emergency Plan for AIDS Relief, a 5-year, $15 billion initiative enacted to provide HIV care, treatment, and prevention services to 2, 7, and 10 million persons, respectively, who are affected by HIV in countries in Africa, Asia, and the Caribbean.

Personal data Information about the characteristics or activities of an identifiable person, including information about individuals who may not be explicitly identified. It differs from a *personal identifiable data* by the fact that not every personal data may be used to determine the identity of the person, for example the age of the individual.

Personal identifiable data Information about the characteristics or activities of an identifiable natural person, including information about individuals who may not be explicitly identified, but whose identity could be inferred from elements of the data.

Personal identifier A datum, or collection of data, that allows the possessor to determine the identity of a single individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a given database. Bits of study data, when taken together, may be used to identify an individual. Therefore, when assembling or releasing databases, it is important to be clear which fields, either alone or in combination, could be used to such ends, and which controls provide an acceptable level of security.

Personnel controls Staff member controls such as training, separation of duties, background checks of individuals, etc. Compare to physical and technical access controls.

Physical access controls Controls involving barriers, such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc. Compare to personnel and technical access controls.

PKI (public key infrastructure) A secure method for exchanging information within an organization, an industry, a nation, or worldwide. A PKI uses the asymmetric encryption method (also known as the public/private key method) for encrypting identifiers, documents, or messages. Also, see *Cryptography*. It starts with the certificate authority (CA), which issues digital certificates (digital IDs) that authenticate the identity of people and organizations over a public system such as the Internet. The PKI can also be implemented by an enterprise for internal use to authenticate users that handle sensitive information. In this case, the enterprise is its own CA. The PKI also establishes the encryption algorithms, levels of security, and distribution policy to users. It not only deals with signed certificates for identity authentication, but also with signed messages, which ensures the integrity of the message so the recipient knows it has not been tampered with. The PKI also embraces all the software (browsers, e-mail programs, etc.) that supports the process by examining and validating the certificates and signed messages.

Plaintext Normal text that has not been encrypted and is readable by text editors and word processors. Contrast with cipher text.

Privacy The legal protection that has been accorded to an individual to control both access to and use of personal information. Privacy protections vary from one jurisdiction to another and are defined by law and regulations. Privacy protections provide the overall framework within which both confidentiality and security are implemented.

Private key The private part of a two part, public key cryptography system. The private key is kept secret and never transmitted over a network.

Pseudo-anonymized Individual level information which has been stripped of certain identifiers - like names, addresses, etc. In many cases, this identifying information will have been replaced with a randomized identifier or key value that can be used, if necessary, to link the record with the person's medical record maintained at an individual health care facility. Data of this type are obtained from communities, health facilities, vital statistics or other data sources. They may be transferred and managed within a data warehouse, which could be at regional or national level.

Public key The published part of a two part, public key cryptography system -- in contrast to the private key, which is known only to the owner.

RAM (random-access memory) A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM, dynamic RAM (DRAM) and static RAM (SRAM).

The two types differ in the technology they use to hold data, dynamic RAM being the more common type. Dynamic RAM needs to be refreshed thousands of times per second. Static RAM does not need to be refreshed, which makes it faster; but it is also more expensive than dynamic RAM. Both types of RAM are volatile, meaning that they lose their contents when the power is turned off.

Records retention policy Assigning a length of time and date to paper or electronic records to establish when they should be archived or destroyed.

Risk In the context of system security, the likelihood that a specific threat will exploit certain vulnerabilities and the resulting effect of that event. A thorough and accurate risk analysis would consider all relevant losses that might be expected if security measures were not in place. Relevant losses can include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. One common risk is that an authorized user could inadvertently or purposely make a change to data which could affect patient care. Another risk is that data may be lost or modified in transmission. Software bugs, viruses and worms, hardware malfunctions, acts of vandalism, and natural disasters such as fire or flood also can compromise data integrity or system availability.

Risk management The optimal allocation of resources to arrive at a cost-effective investment in defensive measures for minimizing both risk and costs in a particular organization.

Role-based access Access to specific information or data granted or denied by the CSO depending on the user's job status or authority. Roles typically group users by their work function. This control mechanism protects data and system integrity by preventing access to unauthorized applications. In addition, defining access based on roles within an organization, rather than by individual users, simplifies an organization's security policy and procedures. Compare to need-to-know access.

ROM (read-only memory) Computer memory on which data have been pre-recorded. Once data have been written onto a ROM chip, they cannot be removed and can only be read. Unlike main memory (RAM), ROM retains its contents even when the computer is turned off. ROM is referred to as being nonvolatile, whereas RAM is volatile.

Most personal computers contain a small amount of ROM that stores critical programs such as the program that boots the computer. In addition, ROM is used extensively in calculators and peripheral devices such as laser printers, whose fonts are often stored in ROM. A variation of a ROM is a PROM (programmable read-only memory). PROMs are manufactured as blank chips on which data can be written with a special device called a PROM programmer.

RSA (Rivest-Shamir-Adleman) A highly secure cryptography method by RSA Security, Inc., Bedford, MA (www.rsa.com). It uses a two-part key. The private key is kept by the owner; the public key is published.

Data are encrypted by using the recipient's public key, which can only be decrypted by the recipient's private key. RSA is very computation intensive; thus it is often used to create a digital envelope, which holds an RSA-encrypted DES key and DES-encrypted data. This method encrypts the secret DES key so that it can be transmitted over the network, but encrypts and decrypts the actual message using the much faster DES algorithm.

RSA is also used for authentication by creating a digital signature. In this case, the sender's private key is used for encryption, and the sender's public key is used for decryption. See Digital signature.

The RSA algorithm is also implemented in hardware. As RSA chips get faster, RSA encoding and decoding add less overhead to the operation.

Sanitize Also known as disk wiping, sanitizing is the act of destroying the deleted information on a hard disk or floppy disk to ensure that all traces of the deleted files are unrecoverable. Software programs that can successfully sanitize a diskette are available.

Script kiddie A person who uses scripts and programs developed by others for the purpose of compromising computer accounts and files, and launching attacks on whole computer systems; in general, these persons do not have the ability to write said programs on their own. Normally, this person is someone who is not technologically sophisticated and who randomly seeks out a specific weakness over the Internet to gain root access to a system without really understanding what is being exploited because the weakness was discovered by someone else. A script kiddie is not looking to target specific information

or a specific organization, but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.

Secret key cryptography Also referred to as symmetric cryptography. It is the more traditional form of cryptography, in which a single key can be used to encrypt and decrypt a message. Secret-key cryptography not only deals with encryption, but it also deals with authentication. The main problem with secret-key cryptography is getting the sender and receiver to agree on the secret key without anyone else finding out. This requires a method by which the two parties can communicate without fear of eavesdropping. However, the advantage of secret-key cryptography is that it is generally faster than public-key cryptography. The most common techniques in secret-key cryptography are block ciphers, stream ciphers, and message authentication codes.

Secured area The physical confinement limiting where confidential data are available. Only authorized staff have access to this area. The secured area usually is defined by hard, floor-to-ceiling walls with a locking door and may include other security measures (e.g., alarms, security personnel).

Security The collection of technical approaches that address issues covering physical, electronic, and procedural aspects of information protection. Security includes the prevention of unauthorized release of identifying information (e.g., preventing a breach of confidentiality), as well as protecting the integrity of the data by preventing accidental data loss or system unavailability. Security measures include methods to detect, document, and counter threats to the confidentiality or integrity of the systems.

SLA (service level agreement) That part of a service contract in which a certain level of service is agreed to between the customer and the provider of the service. In addition to the specified level of service, an SLA should contain support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.

Smart cards A credit card sized card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer. It is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. As a financial transaction card, it can be loaded with digital money and used like a travelers check, except that variable amounts of money can be spent until the balance is zero. Within health care, the card can contain patient identifying information, a complete medical history, or both.

Spyware Software that sends information about an individual’s web surfing habits to its web site. Often quickly installed on a computer in combination with a free download purposefully selected from the web, spyware (also known as parasite software or scumware) transmits information in the background as a user moves around the web.

The license agreement may or may not clearly indicate what the software does. It may state that the program performs anonymous profiling, which means that a user's browsing

habits are being recorded. Such software is used to create marketing profiles. For example, a person who accesses web site A, often accesses web site B and so on. Spyware can be clever enough to deliver competing products in real time. For example, if a user accesses a web page to look for a minivan, an advertisement for a competitor's minivan might pop up.

Spyware organizations argue that as long as they are not recording names and personal data, but treat the user as a numbered individual who has certain preferences, they are not violating a person's right to privacy. Nevertheless, many feel their privacy has been violated. The bottom line is that once users detect a spyware program in their computer, it can be eliminated, albeit sometimes with much difficulty. The downside is that people can become suspect of every piece of software they install.

SSL (secure sockets layer) The leading security protocol on the Internet. When an SSL session is started, the server sends its public key to the browser, which the browser uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session. Developed by Netscape, SSL has been merged with other protocols and authentication methods by the IETF into a new protocol known as Transport Layer Security (TLS).

Super user Someone with the highest level of user privilege who can allow unlimited access to a system's file and setup. Usually, super user is the highest level of privilege for applications, as opposed to operating or network systems. A super user could destroy the organization's systems maliciously or simply by accident.

Symmetric encryption Same as *secret key cryptography*.

Technical access controls Controls involving technology, such as requirements for password use and change, audit of the electronic environment, access to data controlled through known software tools, and control over introduction of changes to the information technology environment (hardware, software, utilities, etc.). Compare to personnel and physical access controls.

Threat An unwanted (deliberate or accidental) expression of intent to execute action that may result in harm to an asset.

Threat analysis An analysis which identifies threats and defines a cost-effective risk mitigation policy for a specific architecture, functionality, and configuration. It involves the mapping of assets, modeling of threats, and building of a mitigation plan that lowers system risk to an acceptable level. The mitigation plan is composed of countermeasures which are considered to be effective against the identified threats.

Trojan horse A program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information, make the system more vulnerable to future entry, or simply destroy programs or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility.

Two-factor authentication The use of two independent mechanisms for authentication; for example, requiring a smart card and a password. The combination is less likely to allow abuse than either component alone.

UNAIDS Joint United Nations Programme on HIV/AIDS. The aim of UNAIDS is to help mount and support an expanded response to the HIV/AIDS pandemic – one that engages the efforts of many sectors and partners from government and civil society. Established in 1994 by a resolution of the U.N. Economic and Social Council and launched in January 1996, UNAIDS is guided by a Programme Coordinating Board with representatives of 22 governments from all geographic regions, the UNAIDS Cosponsors (including UNHCR, UNICEF, WFP, UNDP, UNFPA, UNODC, ILO, UNESCO, WHO and the World Bank), and five representatives of nongovernmental organizations (NGOs), including associations of people living with HIV/AIDS.

USAID (**U.S. Agency for International Development)** The U.S. agency that provides economic, development and humanitarian assistance around the world in support of the foreign policy goals of the United States.

Virus A self-replicating computer program written to alter the way a computer operates, without the permission or knowledge of the user. Though the term is commonly used to refer to a range of malware, a true virus must replicate itself, and must execute itself. The latter criterion is often met by a virus which replaces existing executable files with a virus-infected copy. While viruses can be intentionally destructive -- destroying data, for example -- some viruses are benign or merely annoying.

VPN (Virtual Private Networks) A network that is connected to the Internet, but uses encryption to scramble all the data sent through the Internet so the entire network is "virtually" private.

Vulnerability A security exposure in an operating system or other system software or application software component. Security firms maintain databases of vulnerabilities based on version number of the software. Any vulnerability can potentially compromise the system or network if exploited. For a database of common vulnerabilities and exposures, visit http://icat.nist.gov/icat.cfm

WAN (wide area network) A network of computers that can span hundreds or thousands of miles. Unlike intranets and virtual private networks, a WAN does not use public internet arteries and is isolated from the public domain.

WHO (**World Health Organization)** The United Nations specialized agency for health. It was established on 7 April 1948. WHO's objective, as set out in its Constitution, is the attainment by all peoples of the highest possible level of health. Health is defined in WHO's Constitution as a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity.

Worm a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic

and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

APPENDIX 4 BIBLIOGRAPHY

1. Recommended Readings

Overall

1. CDC / HIV Incidence and Case Surveillance Branch "**Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Confidentiality and Security Guidelines,"** 2006, 86 p.
   http://www.cdc.gov/hiv/topics/surveillance/resources/guidelines/guidance/index.htm
   Contains guidelines about confidentiality and security of U.S. domestic HIV/AIDS Surveillance. It reflects CDC's recommendation as best practices for protecting HIV/AIDS surveillance data and information. It details program requirements and security recommendations. These requirements, recommendations, and practices are based on discussions with HIV/AIDS surveillance coordinators, CDC's Divisions of STD Prevention and TB Elimination, and security and computer staff in other Centers and Offices within CDC, and on reviews by state and local surveillance programs. The document describes 5 principles, and explains issues and solutions for meeting 35 program requirements.

2. UK Depart. of Health "**Report on the review of patient identifiable information,"** *Caldicott report* 1997
   http://www.dh.gov.uk/assetRoot/04/06/84/04/04068404.pdf
   Following the "The Protection and Use of Patient Information*" (UK Dep. Of Health, 1996), the Caldicott Committee had to review the transfer of patient-identifiable information from National Heath Service organizations to other NHS and non-NHS organizations. The Committee puts forward 16 recommendations and suggests 6 principles which can be applied to current flows and any flows proposed in the future.*

3. Paul Douglas Fisher, PhD, James G.McDaniel, PhD (Canadian Society for International Health)
   "**Health Information Systems for low-Income Countries: an Overview,**" 2005, 106 p.
   http://www.csih.org/what/schip/mgraph_en.pdf
   An overview of health information systems (HIS) in general and HIS in low-Income countries in particular. Note: this is not focused on security/confidentiality nor on HIV.

4. The Information for Development Program (*info*Dev) "**Improving health, connecting people: the role of Information and Communication Technologies in the health sector of developing countries,"** 2006, 58 p.
   http://www.asksource.info/pdf/framework.pdf
   The paper describes the major constraints and challenges faced in using information and communications technology (ICT) effectively in the health sector of developing countries. It draws out good practice for using ICT in the health sector, identifies

major players and stakeholders and highlights priority needs and issues of relevance to policy makers.

5. North American Association of Central Cancer Registries "**Data security and confidentiality,"** 2002, 56 p.
   http://www.naaccr.org/filesystem/pdf/Data%20Confidentiality%20Workshop%20Summary.pdf
   A report on data confidentiality and security, from the U.S., based on experience and concrete cases, and containing rules and best practices. Includes:
   -"Data and system security, monitoring and auditing" p.10 describes the 7 layers of security: physical, data links, network, transport, session, presentation and application, from the ISO norms), as well as ways to secure and monitor the system
   - "Data security and confidentiality from a business perspective," p.20 provides a concrete example for implementation
   - "Some practical ways to safeguard confidentiality," p.22 and "Protection of confidentiality initiative", p.24 are other examples of concrete implementations. Appendix A is a check-list of best practices

6. National Cancer Institute "**Confidentiality, Data Security, and Cancer Research: Perspectives from the NCI,"** 1999
   http://www3.cancer.gov/confidentiality.html
   This paper explores the tension in cancer research between the need to protect the confidentiality of individuals and the need for access to information. It proposes a process and a series of measures that would move toward satisfactorily reconciling these needs. The measures include creation of barriers to unimpeded information flow in order to prevent the inappropriate identification of individuals, coupled with a sensible consent policy allowing prospective participants in studies to make informed choices.

Data release policy

7. CDC and Agency for Toxic Substances and Disease Registry "**CDC/ATSDR Policy on Releasing and Sharing Data,"** 2003
   http://www.cdc.gov/od/foia/policies/sharing.htm
   The document contains policy on data release and sharing that balances the desire to disseminate data as broadly as possible with the need to maintain high standards for protection of sensitive information. The policy also ensures that CDC is in full compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA),(where applicable) the Freedom of Information Act [FOIA], and the Office of Management and Budget Circular A110, and the Information Quality Guidelines.

8. CDC and Agency for Toxic Substances and Disease Registry "**CDC - CSTE Intergovernmental Data Release Guidelines Working Group (DRGWG),"** 2005, 86 p.
   http://www.cdc.gov/od/foia/policies/drgwg.pdf or
   http://www.cdc.gov/nchs/about/policy/policy.htm

This report contains16 guidelines and 6 procedures for implementing the "CDC/ATSDR Policy on Releasing and Sharing Data." Most guidelines (each represents a minimum standard for CDC programs) and procedures are accompanied by a best practice statement. Not HIV specific.

9. Canada – Alberta government "**Freedom of Information and Protection of Privacy (FOIP) Act,"** 2005, 66p.
   http://foip.gov.ab.ca/legislation/act/ (the entire Act)
   http://foip.gov.ab.ca/resources/guidelinespractices/chapter7.cfm (Rules and practices)
   Provides a comprehensive source of reference on the application of the FOIP legislation by public bodies in Alberta. It interprets the Act and Regulation with reference to rulings by the Information and Privacy Commissioner. It also sets out roles and responsibilities and offers guidance on approaches and procedures that are intended to assist in the effective administration of the Act. Chapter 7 is dedicated to protection of privacy.

Legal, ethical

10. Lawrence O. Gostin, James G. Hodge "**Model State Public Health Privacy Act,**" 1999, 59 p.
    http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf or
    http://www.critpath.org/msphpa/modellaw5.htm
    This act is a model state privacy law pertaining to the use of public Health Information. The act is broken down into 6 specific articles:1 Acquisition of protected Health Information (HI), 2 Uses of public HI, 3 Disclosures of protected HI, 4 Security safeguards and record retention, 5 Fair information practices, 6 Criminal sanction and civil remedies.

11. Lawrence O. Gostin, Zita Lazzarini, Kathleen M. Flaherty "**Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization,"**
    http://www.epic.org/privacy/medical/cdc_survey.html
    Examines current U.S. state and federal laws protecting the confidentiality of health information. It focuses on four specific areas: public health information held by government, privately held health care information, HIV and AIDS-related information, and immunization information.

12. Lawrence O. Gostin "**Public Health Law and Ethics: A Reader,"** 2003
    http://www.publichealthlaw.net/reader/index.html
    Provides a discussion and analysis of critical problems at the interface of law, ethics, and public health. It is intended as a stand-alone text and offers a detailed commentary that defines a public health problem in each chapter, frames the relevant questions, and introduces the selected readings. The commentary also provides additional resources, many of which are included on the web site, for readers interested in further pursuing the subject matter in the chapter. See especially chapter 7 "Public health and the protection of individual rights" and chapter 10 "Surveillance and public health research: privacy and the 'right to know.'"

13. Pat Sweeney, CDC "**Draft: Ethical Principles and Guidelines for the Use of Identifiable Public Health Data with a Focus on HIV/AIDS,"** 2006
    This document is written for the "UNAIDS HIV-Information Confidentiality and Security Workshop, 15-17 May 2006, Geneva" for discussion purposes.

14. Amy L. Fairchild, Lance Gable, Lawrence O. Gostin, Ronald Bayer, Patricia Sweeney, Robert S. Janssen "**Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information,"** 2007 *Public Health Reports* 2007 Supplement 1, Vol. 122
    A concise history and discussion on the use of personal identifiable information for public health purposes.

15. CDC "**HIPAA privacy rule and public health, guidance from CDC and the U.S. DHHS,"** 2003, 24 p.
    http://www.cdc.gov/mmwr/pdf/other/m2e411.pdf
    The U.S. DHHS issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this report is to help public health agencies and others understand and interpret their responsibilities under the HIPAA Privacy Rule. Elsewhere, comprehensive DHHS guidance is located at the HIPAA website of the Office for Civil Rights.

Electronic security

16. Bruce Schneier "**Secrets and Lies: Digital Security in a Networked World,"** 2004 John Wiley and Sons, ISBN**:** 0471453803
    Describes, using concise everyday analogies, the strategies hackers use to compromise electronic data systems.

17. W. R. Cheswick, S. M. Bellovin, and A. D. Rubin "**Firewalls and Internet Security: Repelling the Wily Hacker,"** 2003, 464 p.
    Addison-Wesley Professional Computing Series http://www.wilyhacker.com/
    This technical book is written primarily for the network administrator who must protect an organization from unhindered exposure to the Internet. It contains the following sections: Security review, Threats, Safer tools and Services, Firewalls and VPNs, Protecting an organization, Lessons Learned, Appendix on Cryptography.

18. International Organization for Standardization "**ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management,"** 2005
    http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html (access requires payment)
    ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; compliance

19. National Institute of Standards and Technology "**Guideline on network security testing,"** 2003, 92 p.
http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf
This detailed overview contains names of many tools, for example, a list of firewall product names. Not HIV or health specific.

20. National Institute of Standards and Technology "**Guidelines on Firewalls and Firewall Policy,"** 2002, 74 p.
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
This document provides introductory information about firewalls and firewall policy primarily to assist those responsible for network security. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewalls environments. Not HIV or health specific.

21. National Institute of Standards and Technology "**Security Self-Assessment Guide for Information Technology Systems, revised2005,"** 2005
http://csrc.nist.gov/publications/nistpubs/800-26/Mapping-of-800-53v1.doc
This technical document provides a comprehensive security self assessment questionnaire. It includes more than 200 controls: management controls, operational controls, and technical controls. Not HIV or health specific.

22. National Institute of Standards and Technology "**An introductory Resource Guide for Implementing the HIPAA Security rule,"** 2005, 137 p.
http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf
The guide identifies resources relevant to the specific security standards included in the HIPAA security rule and provides implementation examples for each. It focuses on the safeguarding of electronic protected health information.

2. Additional Material

Overall

23. Canadian Society for Health Information "**Health Information Glossary,"**
http://www.cihi.ca/cihiweb/en/partner_glossary_e.html
A 400 term-glossary related to this topic.

24. The UK Academy of Medical Sciences "**Personal data for public good: using health information in medical research,"**
http://www.acmedsci.ac.uk/images/project/Personal.pdf
The document outlines AMS concerns, and makes recommendations for what they see as possible improvements to research practices. Reform is needed, according to the

AMS, because data protection and other related legislation has often been interpreted by regulatory bodies in contradictory and confusing ways. Because of the resulting uncertainty, researchers are often advised that personal medical data cannot be used in their research studies unless there is consent from the individual or the data has been anonymised. See especially, "Chapter 3: Confidentiality, security of data and anonymisation."

25. Dr Peter Drury, eHealth International "**eHealth: a model for developing countries,"** 8 p.
http://www.ehealthinternational.org/vol2num2/Vol2Num2p19.pdf
This paper proposes a model or framework for analysis, to inform the development of eHealth in developing countries. The framework has five components – the 5Cs: context of poverty, content of health information provided to health workers, connectivity within and between health facilities, building workforce capacity, supporting community development.

26. Sarah B. Mcfarlane "**Harmonizing HIS with information systems in other social and economic sectors,"** 2005, 7 p.
http://www.scielosp.org/pdf/bwho/v83n8/v83n8a12.pdf
A WHO bulletin about the needs of a better cross-coordination among social and economic sectors in order to optimize the HIS in low- and middle-income countries.

27. Anderson RJ, University of Cambridge "**Security in clinical information systems,"** 1996
http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html
Describes threats to confidentiality, integrity, and availability of personal health information in the light of experience in the UK and overseas, and proposes a clinical information security policy that enables the principle of patient consent to be enforced in the kind of heterogeneous distributed system currently under construction in the UK. An information security policy says who may access what information; access includes such activities as reading, writing, appending, and deleting data.

28. State of Texas Department of Information Resources "**Privacy Issues Involved in Electronic Government,"** 2000 http://www.dir.state.tx.us/taskforce/report/privacy.doc
Privacy and information held in e-governments: Overview, comparison among other countries, and recommendations for Texas.

Legal, ethical

29. Australian government "'**Federal Privacy Act, 1988, 2000,"**
http://www.privacy.gov.au/act/privacyact/index.html
"**Guidelines on Privacy in the Private Health Sector, 2001,"**
http://www.privacy.gov.au/health/guidelines/index.html#1
"**Information Technology and Internet Issues,"**
http://www.privacy.gov.au/internet/index.html
"**Guidelines Under Section 95 of the Privacy Act 1988, 2000,"**
http://www.privacy.gov.au/publications/e26.pdf

Highly readable but somewhat briefer coverage of the topics covered under "Recommended Readings, above.

30. U.S. Public Law 104-191 "**Health Insurance Portability and Accountability Act of 1996,"**
http://www.cms.hhs.gov/HIPAAGenInfo/
The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

31. U.S. Government "**The E-Government Act of 2002,"**
http://www.whitehouse.gov/omb/egov/g-4-act.html
The Act, which has been made for governmental internet web-sites, contains these 2 chapters:
TITLE III: Information Security
TITLE V: Confidential Information Protection and Statistical Efficiency.

32. Joshua B. Bolten "**OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,"** 2003 http://www.whitehouse.gov/omb/memoranda/m03-22.html
Provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002

33. USAID "**USAID Compliance With the E-Government Act of 2002,"**
http://www.usaid.gov/policy/egov/
Outlines how USAID's public website complies with Federal information resource management law and policy as detailed in OMB Memorandum M-05-04.

34. U.K. Government "**Data Protection Act 1998,"** ISBN 0 10 542998 8
http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm
This Act gives individuals the right to access information held about them by organizations. The act governs how organizations can use the personal information that they hold - including how they acquire, store, share or dispose of it. The act is administered and enforced by the Information Commissioner - an independent authority who is appointed by the Queen and reports directly to parliament. Data protection is an international issue which results from European legislation (Directive 95/46/EC, see R10)

35. Protection and Advocacy System of New Mexico "**HIV and Your Legal Rights,"** 1996
http://www.aegis.com/law/journals/1996/LEGLBOOK.html
This booklet covers the inclusion of HIV/AIDS as a disability for the purposes of disability discrimination law; confidentiality; HIV testing and consent; insurance benefits; discrimination in housing, employment, medical care, and public accommodations; end-of-life planning; and disability and other public benefits. A

frequently asked questions part includes answers to questions such as: "Can I be Denied Insurance Because I Have HIV?" or "Can I be Fired Or Not Hired Because I Have HIV/AIDS?"

36. WHO "**The Role of Ethics Review Committees in Public Health Surveillance,"** Consultative meeting, 1st October, 2004

37. Kathleen M. MacQueen and James W. Buehler "**Ethics, Practice, and Research in Public Health,"** 2004
American Journal of Public Health June 2004, Vol 94, No. 6 | 928-931
http://www.ajph.org/cgi/content/abstract/94/6/928 *(accessible only by members)*
Ethical issues that can arise in distinguishing public health research from practice are highlighted in 2 case studies: 1) an investigation of a tuberculosis outbreak in a prison and 2) an evaluation of a program for improving HIV prevention services.

38. Amy L. Fairchild and Ronald Bayer "**Ethics and the Conduct of Public Health Surveillance,"** 2004 *Science* 30 January 2004:Vol. 303. no. 5658, pp. 631 – 632
http://www.sciencemag.org/cgi/content/summary/303/5658/631 *(accessible only by members)*
Efforts to distinguish between public health surveillance and epidemiological research are burdened by history. The authors of this policy forum say the moment is right to reframe the policy discussion and to recognize the imperative of ethical review of surveillance as well as research.

39. Lawrence O. Gostin, James G. Hodge - Council of State and Territorial Epidemiologists (CSTE)
"**CSTE Public Health Practice v. Research: Making Distinctions for Public Health Practitioners,"** 2004
http://www.publichealthlaw.net/Research/Affprojects.htm#CSTE
Provides guidance on the distinctions between public health practice and human subjects research for public health officials, researchers, institutional review board (IRB) members and their staffs.

Data Release Policies

40. P. Doyle, J. Lane, J. Theeuwes, L. Zayatz "**Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies,"** 2002
ELSEVIER 2, 462 pages, ISBN: 0-444-50761
Provides a review of new research in the area of confidentiality and statistical disclosure techniques. A major section of the book provides an overview of new advances in the field of both economic and demographic data in measuring disclosure risk and information loss. It also presents new information on the different approaches taken by statistical agencies in disseminating data -- ranging from licensing agreements to secure access – and provides a new survey of which statistical disclosure techniques are used by statistical agencies around the world. This is complimented by a series of chapters on public perceptions of statistical

agency actions, including the results of a new survey on business perceptions. The book

41. Federal Committee on Statistical Methodology "**Confidentiality and Data Access Committee (CDAC),"** 1999
http://www.fcsm.gov/committees/cdac/index.html
CDAC is sponsored by the Federal Committee on Statistical Methodology to provide a forum for staff members of federal statistical agencies who work on confidentiality and data access topics to communicate among themselves, exchange ideas, etc. This site also contains the brochure, "Confidentiality and Data Access Issues Among Federal Agencies."

42. Goss, Jon, Department of Geography University of Hawai'i " '**We Know Who You Are and We Know Where You Live': The Instrumental Rationality of Geodemographic Systems,"** 1995 *Economic Geography* Vol. 71, No. 2., pp. 171-198
This paper provides a critique of geodemographic systems, sophisticated marketing tools that combine massive electronic data bases on consumer characteristics and behavior, segmentation schemes, and Geographic Information Systems (GIS).

43. Armstrong, Marc P.; Rushton, Gerard; Zimmerman, Dale L. "**Geographically Masking Health Data to Preserve Confidentiality,"** 1999
http://www.uiowa.edu/~geog/faculty/armstrong/Masking.pdf *Statistics in Medicine* 18, 497-525
This document describes methods of geographically masking individual-level data.

44. Onsrud, H.J. "**Identifying Unethical Conduct in the Use of GIS,"** Cartography and Geographic Information Systems, 1995, 22(1), 90-97
http://www.spatial.maine.edu/~onsrud/pubs/ethics18.pdf
Describes and discusses various "grey areas" in the use of GIS and in determining what constitutes a beneficial versus a detrimental consequence, and how these often depend on the perspectives of those affected by the use of information systems.

45. Federal Geographic Data Committee "**FGDC Policy on Access to Public Information and the Protection of Personal Information Privacy in Federal Geospatial Databases,"** 1998
http://www.fgdc.gov/library/factsheets/factsheets-biblio/privacy-factsheet
This policy articulates the FGDC's endorsement of public access to information and appropriate protections for the privacy and confidentiality of personal information in federal geospatial databases. The Federal Geographic Data Committee (FGDC) is an interagency committee that promotes the coordinated development, use, sharing, and dissemination of geospatial data on a national basis. The Office of Management and Budget (OMB) established the FGDC in 1990.

46. Leah K. VanWey, Ronald R. Rindfuss, Myron P. Gutmann, Barbara Entwisle, and Deborah L. Balk. "**Spatial Demography Special Feature: Confidentiality and spatially explicit data: Concerns and challenges,"** 2005 PNAS 2005 102: 15337-15342
http://www.pnas.org/cgi/reprint/102/43/153377

Recent theoretical, methodological, and technological advances in the spatial sciences create an opportunity for social scientists to address questions about the reciprocal relationship between context (spatial organization, environment, etc.) and individual behavior. This emerging research community has yet to adequately address the new threats to the confidentiality of respondent data in spatially explicit social survey or census data files, however. This paper presents four sometimes conflicting principles for the conduct of ethical and high-quality science using such data: protection of confidentiality, the social-spatial linkage, data sharing, and data preservation.

Electronic security

47. Oracle corporation "**Privacy Protections in Oracle Database 10G"** 2004, 36 p.
http://www.oracle.com/technology/deploy/security/db_security/pdf/privacy10g.pdf
Includes sections on authentication, authorization, access control, identity management, encryption, monitoring, and accountability. The document shows that this version of Oracle is "privacy oriented" and compatible with our guidelines: authentication, role-base access, encryption (AES…), notion of Virtual Private Databases, etc. Concludes with a chapter on the challenges of technology to data protection

48. International Telecommunication Union "**Security in Telecommunication and Information technology,"** 2003, 98 p.
http://www.itu.int/itudoc/itu-t/85097.pdf
Provides an overview s issues and deployment of the organization' existing recommendations for secure telecommunications.

49. Uyless D. Black "**Internet Security Protocols: Protecting IP Traffic,"** 2000
Prentice Hall PTR; ISBN**:** 0130142492
A book-length, technical explorations of the issues associated with security internet traffic.

50. Sidnie Feit, McGraw-Hill "**TCP/IP: Architecture, Protocol, and Implementation with IPv6 and IP Security,"** 1999
McGraw-Hill Computer Communications SeriesISBN**:** 0070213895
Additional information on securing information systems which are deployed over the internet. This book is also intended for technical audiences.

51. Stephen A. Thomas "**SSL and TLS Essentials: Securing the Web,"** 2000
John Wiley and Sons, ISBN**:** 0471383546
A book-length, technical explanation of how secure sockets layer (SSL) encryption works.

52. Richard E. Smith "**Internet Cryptography,"** 1997, Addison-Wesley, ISBN**:** 0201924803

Describes the mathematics behind computer encryption schemas, as well as the overall strategy behind public-private and other strategies for authorized decryption of information.

53. US DHHS/ National Committee on Vital and Health Statistics "**Cryptography-based Patient Identifier,"** http://ncvhs.hhs.gov/app7-4.htm
    A short article on the role of encryption in electronic security.

Web links

CDC and HIV/AIDS: http://www.cdc.gov/hiv/
UNAIDS: http://www.unaids.org/en/
USAID and HIV/AIDS: http://www.usaid.gov/our_work/global_health/aids/
WHO and HIV/AIDS: http://www.who.int/hiv/en/
UK Department of Health: http://www.dh.gov.uk