COMMUNITY IMMUNIZATION REGISTRIES MANUAL

CHAPTER II: CONFIDENTIALITY*

Prepared by

All Kids Count Program of The Task Force for Child Survival and Development

The National Immunization Program of the Centers for Disease Control and Prevention

The National Vaccine Advisory Committee

January 28, 1997

---

* Principal contributor: Brian Willis, J.D., MPH, National Immunization Program, Centers for Disease Control and Prevention.

CONTENTS

INTRODUCTION TO CHAPTER II

One of the strategies to reach and sustain the goal of immunizing 90% of the nation's children who are under 2 years old by the year 2000 is to develop immunization information systems, referred to as "immunization registries." These registries permit health departments and providers to maintain a computerized immunization record on children within a community. There are three primary purposes for the development of registries: (1) Registries may serve as a "reminder and recall" system for parents. Immunization registries can use the telephone or mail to automatically remind parents when their child is due for a vaccination, or contact the parents when the child has missed an appointment, or is overdue for an immunization. (2) Registries may serve as a clinical assessment and monitoring tool for providers. In this capacity immunization registries can assist providers to identify their patients who require an immunization in a timely manner. The registries can also assist providers by forecasting which immunization(s) a child may require by incorporating the most current immunization schedule into the registry. In addition, a function that benefits the child, parent, and provider, immunization registries permit providers to exchange information on the immunization status of a child. This may be necessary when the child receives medical services from several providers, is away from the medial home, or is seen in an emergency department. This will also ensure that immunization records are complete when a child receives immunizations from more than one provider. (3) Finally, from a public health perspective, registries may assist communities to assess immunization coverage and identify pockets of need.[**]

An increasing number of state health departments and local health departments currently operate immunization registries. Other health departments are in the process of developing their registries.[***, ****] A major concern for all of these registries has been the **confidentiality** of the information they contain. In order to address this concern, recommendations addressing confidentiality issues of immunization registries have been developed by CDC, the All Kids Count program, and the National Vaccine Advisory Committee.

An individual's medical and demographic information is both personal and confidential. Protection of confidentiality and the individual's right to privacy in these areas are so critically important that the editors believe a separate chapter on the subject is demanded. These questions pose significant and urgent challenges to immunization registries as they are developed and operate on a daily basis. Media attention and recent legislation has further accentuated public sensitivity in this area. Officials in all fields are increasingly called upon

---

** Orenstein, et al. Letter to the Editor. JAMA. May 1, 1996 vol 275, no. 17, 1312-1313.

*** National Vaccine Advisory Committee, Subcommittee on Vaccination Registries. Developing a National Childhood Immunization Information System: Registries, Reminders, and Recall, DHHS, 1994.

**** Gostin, L.O., Lazzarini, Z. "Childhood Immunization Registries," JAMA. 1995; 274:1796-1799.

to account for violations, or perceived violations, of individual privacy. In an increasingly litigious society, lack of adequate attention to this crucial area of concern potentially will have severe consequences for the registry and its operators.

For the immunization registry, confidentiality must be addressed within the context of the topics discussed in the other three chapters of the manual on community immunization registries: **Planning** (Ch. I), **Technology** (Ch. 3), and **Operations** (Ch. 4), the AKC/CDC manual on how to plan, design and operate immunization registries. As this chapter discusses, confidentiality and the above three topics impact and influence each other. This chapter will demonstrate the importance of gathering and sharing information on people while guarding individual confidentiality. This is a demanding, but not impossible task. Many states have already aided the process by mandating reporting of such information as sexually transmitted diseases, cancer, birth defects, and in a few cases, childhood immunizations. This chapter has been prepared specifically to aid the registry developer and manager in finding that delicate balance.

The registry development experiences of others, particularly the All Kids Count projects, have been cited for their value as "lessons learned." Addressed herein are the principal confidentiality issues the registry developer and manager will face. These issues are not restricted solely to areas of information data control, though that area is one of major concern. Registry developers and managers also need to be cognizant of the confidentiality risks associated with maintaining and sharing data. Human error of laxness on the part of the staff are major contributing factors to breeches in confidentiality. The technology of hardware, software, and physical security must be designed and utilized in a manner to minimize such risks. Additionally, this chapter will deal with the necessity for having a tool to enforce confidentiality rules, many of which take the form of existing laws and statutes.

Developments in information technology pose both major confidentiality challenges and effective security risks for the immunization registry manager.***** Information on individuals must be gathered and maintained without permitting any harm to the individual from the inappropriate disclosure of that information. With respect to immunization registries, various reports on this topic have been made.[2, 3] The findings of the National Vaccine Advisory Committee's Subcommittee on Vaccination Registries include confidentiality among the important issues to consider when developing immunization registries. For registries to be successful, they must assure to the greatest extent possible that:

- data are accurate and complete.

---

[4] Gostin, L.O., et. al., "Privacy and Security of Personal Information in a New Health Care System," JAMA. 1993:270; 2487-2493.

- records are built around a core of standard items needed to exchange information between health care providers.

- data are adequately protected to assure individual privacy.

Providers and their staffs must constantly be vigilant not to indiscriminately disclose information about their patients without the patient's authorization, or as required by law.

There are several practical considerations for protecting the confidentiality of information held by an immunization registry. Moreover, health officials can increase community confidence and participation in the system by assuring the public of the following: (1) Data in the system will be collected for the sole purpose of guaranteeing that children will be vaccinated on time. (2) Access to the system will be limited to authorized users. (3) Disclosure of information to authorized users will be on a "need to know" basis only. (4) Information will be released for the exclusive purpose for which it is requested. The more detailed personal information is, the greater the probability it will contain items that could be harmful to an individual if inappropriately disclosed. Yet, if registry data are not complete and accurate, parents and providers will lose confidence in it and cease to participate.

The editors wish to acknowledge the contributions made to this chapter by representatives of the following organizations: The Task Force for Child Survival and Development; the All Kid Count projects; state, county, city, and local health departments; The National Association of County and City Health Officials; health managed care organizations; physicians, and other professional health care organizations; and the Centers for Disease Control and Prevention. Among those participating at various times were immunization program managers, attorneys, and privacy advocates.

The National Vaccine Advisory Committee of the Department of Health and Human Services has reviewed and adopted this document.

1: CONFIDENTIALITY PRINCIPLES

Although the information contained in the registry is confidential, the existence of the registry should not be. Health departments need to make known to parents, providers, and other health departments information regarding the registry. This goal can be accomplished on an individual basis with parents by the health department, providers, or on a community level through public information campaigns.

Immunization registries are intended to be in the best interest of the public as a whole. However, it is acknowledged that some individuals may not desire participation for themselves or their children. History has shown this to be the case with other public immunization initiatives. Reasons given in the past for nonparticipation have included religious or philosophical grounds, concerns about the safety of specific vaccines, or a wish to protect personal privacy. Registry designers and managers need to establish formal policies and procedures to ensure registry users are properly guided concerning community confidentiality standards. Transformation of these standards into working policies and procedures will likely require careful review and interpretation. The need for new federal, state, or local laws or regulations on this sensitive issue may be revealed. The existence of adequate confidentiality statutes notwithstanding, a clear policy needs to be defined for those implementing and using an immunization registry. Clearly delineating how specific issues will be handled is an important safeguard against breach of confidentiality through ignorance, accident, or intentional abuse.

To address the issues of privacy and confidentiality, every immunization registry should have a written policy on these related topics. The policy should strike a balance between the need for sharing immunization information to protect the public, and the privacy and confidentiality rights of children, parents, providers, and other users of the system.

The policy should be reviewed periodically in order to address any issues which may arise during the administration of the registry.

2: DEFINITIONS

Any discussion of confidentiality should begin with a clear definition of the terms used. If state laws or regulations are being developed, defining the terms to be used in those laws is an absolute necessity. Terms that may need defining are: registry, immunization-related data, privacy, confidentiality, disclosure, parent or guardian, provider, and security. Some sample definitions follow:

IMMUNIZATION REGISTRY

For the purposes of this document, an immunization registry may be defined as a computerized system to consolidate and record immunization histories of numerous individuals, or for an entire community, based on information from a number of practices. Immunization registries have the goal of ensuring that: (1) Providers will be assisted in evaluating the immunization status of their patients. (2) Providers and public health officials will be assisted in issuing immunizations reminders to individuals or their children as needed. (3) Public health officials will be assisted in assessing immunization coverage in a community.

IMMUNIZATION-RELATED DATA

This data includes information about which vaccines have been received or are due for an individual. Other information under this heading includes identifier or demographic data, locator data, and linking data. Identifier or demographic data entails such things as names, dates of birth, and gender. Locator information involves address and telephone numbers. Linking information may consist of identifiers (IDs) used in other systems such as Women, Infants, and Children's program (WIC) and regional systems. The immunization history should include the type of vaccine administered, the dose, the vaccine lot number, and the vaccine manufacturer. Potentially sensitive information such as the existence of contra-indications or objections to immunization also should be part of the immunization history. Demographic information may extend to family relationships and socio-economic data related to a person's ability to pay for medical services. **To many people it may by more important to protect their demographic information than their immunization information from disclosure.** Concerns about this data include disclosing an address or phone number to an estranged or divorced spouse, disclosing immigration data to the Immigration and Naturalization Service (INS), and releasing information for marketing purposes. A registry should consider isolating and safeguarding not only medically sensitive information, but also locator or demographic information.

PRIVACY

Information privacy has been defined by the Institute of Medicine as the interest of an individual to control the dissemination and use of information that relates to the individual, or to have information about oneself be inaccessible to others.[******] Individuals may not wish to have their personal information shared with a provider without their permission, or may view receiving notifications of immunizations due as an invasion of their personal privacy.

Access to the data in the system must be limited to only authorized users for authorized purposes. Obtaining community input about registry goals can aid developers in setting appropriate user access limits to personally identifiable information. Access should depend on whether the information is needed to provide services to the patient, a parent, a provider, or the community. For example, providers of immunization services and public health officials might be authorized full access to all registry immunization data and records. School officials, on the other hand, might be authorized only to receive a summary of children requiring additional vaccinations. Only the minimum demographic information necessary to correctly identify children would be added. Researchers might receive aggregate immunization information and limited demographic information, but not personal identifiers.

CONFIDENTIALITY

Confidentiality is a normal part of the relationship between patients, physicians and their staff. It is the duty of the health care provider not to disclose information about an individual to others, except as authorized. When participating in an immunization registry, providers transfer patient data into the system, and need assurance that their patients' confidentiality will be protected. Therefore the registry must ensure data is entered with an appropriate **confidentiality status**. This status indicates to what extent the data are to be protected from unauthorized disclosure, regardless of who holds the information.

SECURITY

Within an immunization registry **data security** necessitates special **policies and procedures** to protect sensitive data from accidental or intentional disclosure to an unauthorized person, and from loss or unauthorized alteration. Security procedures should include software and hardware protection, physical measures (including protection from fire or flood), and an informed and alert staff.

3: CONFIDENTIALITY ISSUES

---

[5] Institute of Medicine, Health Data in the Information Age; Use, Disclosure, and Privacy, 1994.

Confidentiality policies need to address the following issues:

- What information is to be provided to the public about the collection and use of data?
- How can information be protected when it is held by different providers and agencies?
- How is access to the data in the registry databases to be controlled?
- How is appropriate disclosure of information to be controlled?
- Are the security procedures implemented by the registry adequate?
- Are there appropriate penalties rendered for those who make unauthorized disclosures or changes to information?

With the exception of the security issue which is covered in **Chapter III, Technology**, as well as **Chapter IV, Operations**, guidance on each of the above topics follows.

COLLECTION OF IMMUNIZATION INFORMATION

Notification and consent

Before collecting information, prior notification to individuals and informed consent must be considered. These are two of the most sensitive issues for developers of immunization registries. A single notification might be used to cover both of these purposes. First, the notification informs individuals about who is gathering the information (the registry), the source of the information (patients and providers), the type of information requested (immunization and demographic), the types of data that will and will not be disclosed, the purposes for which it will and will not be released, and who the authorized users of the registry will be. Second, the same notification may be used to obtain informed consent from individuals for gathering the necessary data. Individuals also need to know the process by which they may review data on them and request corrections when errors are found.

Options for informing the public or for obtaining formal individual consent which should be considered by the registry include:

- **repeated public announcements** in the media, in which the routine nature of the registry's operations, such as gathering data for all new births, is stressed. Such announcements should discuss the purposes and benefits of the registry, and describe how one may "opt out," if so desired.

- **individual notifications** that information has been collected . These could take the form of public health authorities making written notification if an electronic birth certificate is the initial source of information, or from providers at the time immunizations are given. Such notifications should also define how one may "opt out." of the registry.

- **informed consent** using signed forms authorizing the inclusion of the individual in the registry. This option should be exercised before or at the time the first immunization is recorded, including birthing centers administering hepatitis B vaccine to newborn infants.

A significant concern regarding requiring informed consent is that it will tend to decrease the number participating in the registry. Non-participants could be left vulnerable to vaccine-preventable diseases, thus putting others at risk and compromising the efforts of the community to prevent the introduction and spread of these diseases. The need for notification or informed consent might be obviated by existing or new regulations or legislation at the state or local level.******* Some states or communities may require registries to provide the option of being removed from the database at any time, even if the "opt out" provision was not initially exercised.

Amount of data collected

Another issue to address is the amount of data to be collected on individuals.

- **When the registry is used for immunization information only,** the information collected should only be that which is required to ensure immunization coverage. Such information would include the facts required to issue reminder/recall notifications, to assist providers in assessing a child's immunization status, and to assess immunization coverage in the community.

- **If the registry is linked to or functions as part of a larger data system,**[********] the extent to which the information is shared with other parts of the data system may need to be limited. It is desirable to advise parents and registry users if any or all of that data will be shared with other parts of the data system.

- **The community should be informed about the importance of the registry.** The community needs to be fully apprised about the registry's purpose and operation.

---

[6] see report by Gostin, JAMA, 1995.

[7] The Rhode Island Children's Access Program (RICAP) plans to integrate the databases of 11 separate infant/toddler programs for continuous tracking of pediatric preventive health indicators.

Additionally, a consensus should be reached with representatives of the local providers on the data elements to be collected and the level of confidentiality and sensitivity of each element.

The information collection policy also should address the period of time the information may be held in the registry and how it will be deleted at the end of that period. The retention and disposal of records may already be addressed under state or other laws. In this case the requirements of the registry policy should conform to existing statutes.

HOLDERS OF IMMUNIZATION INFORMATION

Immunization registries are intended to carry out the important task of immunization record consolidation on individuals who may obtain medical care from multiple providers. Implicit in the concept of a registry is the sharing of immunization information between providers without the necessity for a traditional provider-to-provider request. Additionally, registries make it possible for schools to learn a child's immunization status without specific requests from parents to providers to release the information.

Proprietary or commercial activities should be excluded as registry uses. Thus, the issue of ownership of the complete records should not occur in normal functioning. Nevertheless, situations might arise where issues of ownership of the data and control over its disclosure may affect the willingness of providers to participate. For example, managed care organizations might not wish competitors to have access to certain parts of their clients' records. If the issue of "ownership" of information in the registry is not adequately addressed under existing statutes, the registry must facilitate a resolution with its participants. The confidentiality policy needs to clarify and inform all information holders concerning these points.

Holders of immunization-related information will include providers, health departments, and non-providers. Policies are needed governing the protection of information at each location where it is held. Certain circumstances may require special provisions for the protection of immunization-related information. If the registry is operated in conjunction with a health department, but is actually administered by a non-profit organization, the immunization-related data in the registry may NOT be protected under the state public health laws. Public health laws often apply only to the health department. If the data are not protected by the public health laws, it must be determined whether state laws on the confidentiality of medical records apply, whether new legislative or administrative actions are required, or whether certain requests for access to, or use of the data must be denied under existing laws.

Providers

In a provider setting, immunization-related information is part of the patient record. This information should be disclosed only to authorized recipients. Responsibility for protecting the confidentiality of immunization-related information extends to other health care providers and support staff where the vaccine was administered. A signed acknowledgment from every user (medical, managerial, and support staff) affirming his or her assent to protecting the confidentiality of immunization-related information is highly desirable.

Health departments

Information that is considered public health data may be defined under existing state or local public health laws. Health departments that operate a registry need to review these statutes. Requests for legislative action to meet operational needs for the registry, including confidentiality, may be in order.

Non-providers

Non-providers of immunization services, such as schools, researchers, and insurers may seek access to the information in an immunization registry. For example, an authorized school official, such as the school nurse, might use the registry to make necessary immunization determinations on students. In such cases, non-providers using registry information should be held to the same standards of confidentiality and accountability as are providers and health departments. Non-providers should release immunization-related information only to another authorized user for an immunization-related purpose. Signed forms similar to those suggested for providers and their staffs might be appropriate to ensure confidentiality is maintained in this area.

ACCESS TO THE DATA IN THE REGISTRY

Access means having authorization and the capability to enter or review system data. Registry access authorization is dependent upon having a legitimate need for immunization-related information on a specific individual. A confidentiality policy needs to define who will have access, to which records will they be granted access, and to which data fields they will have access. For example, providers making an inquiry of the registry using a patient's name only, should be permitted to obtain basic information to confirm the child's identity (e.g., date of birth, and gender) and immunization history. The history may include a list of vaccines given, the dates they were administered, and the possible existence of a contraindication. In another circumstance, outreach workers for whom under-immunization of children is an indicator of general risk, might be allowed access to the demographic portion of the child's record, but not medical information.

Access to the registry ordinarily would be granted to:

- any provider authorized to administer an immunization,
- parents,[8]
- health departments or collaborating programs such as WIC or perhaps Aid to Families with Dependent Children (AFDC),
- licensed day care centers, schools or colleges, and
- others with appropriate need for immunization information without personal identifiers, such as researchers.

Granting access to other organizations is more controversial and may require decisions on a case-by-case basis. Some examples include administrative, legal,[9] financial, or actuarial companies that service providers or health care organizations. It may be desirable to have a policy in place that delineates procedures for handling requests from such agencies. To illustrate, the policy might require written authorization from parents or guardians to release information to these types of organizations.

As with release of data, access to the information in a registry may be governed by Federal, state, or other laws or regulations. To the extent that registry information is in the possession of the Federal government, the Freedom of Information Act and the Privacy Act will protect name-identified information from disclosure by the Federal government without the consent of the individual named. The reader should refer to state law to determine the confidentiality status of name-identified information maintained in state or local registries. Each registry should ensure that their access policies and procedures are consistent with applicable laws.

A procedure also will be needed to authenticate users of the system. Each user may be assigned a unique Personal Identification Number (PIN) number. Access by non-providers to immunization-related data should be based on the purpose for which the information is

---

[8] Parents should be allowed to request correction or amendment of their children's records when they contain errors. Also, there may be conditions under which parents may not be granted access to information on their child, e.g., when the child reaches a certain age. Registry operators may determine how long data will be stored and whether access to information changes with the age of the individual, e.g. a child turns 18 years of age. However, since this information has been collected for public health purposes, health departments may consider whether to retain this information in a non-identifiable form.

[9] Note: The data in the registry, like many public health records, may be subject to subpoena. Operators need to determine which laws would apply if the registry data were subpoenaed.

sought. Non-provider access needs to be limited to certain information and those limits need to be clearly identified in the confidentiality policy. Also a policy needs to be established delineating how much unique patient information a user is required to enter before access to that patient's record is granted.

Access options include:

- All providers have access to all records.
- All providers have access only to their own patient records.
- All providers have access to all information on their own patients and access to immunization information only, on individuals who are not their own patients.

Each registry needs to establish its policy as to which of these, or other possible options, will apply.

DISCLOSURE OF INFORMATION

The release of medical information, such as immunization-related data, may already be addressed under Federal, state or other laws or regulations. Each registry should determine which laws and regulations apply to the release of information so that their confidentiality policy is written to be consistent with them. Establishment of additional pertinent local regulations may be necessary or desirable. For example in California, the implementation of registries required new legislation to permit exchange of immunization information between public and private providers.

At a minimum, a registry confidentiality policy is needed to set forth an understandable and acceptable set of procedures for all users. The confidentiality policy of the registry should identify authorized users to whom information may be disclosed and the level of information that may be disclosed, consistent with applicable laws and regulations. The confidentiality policy should limit the information that is disclosed to authorized users based on the users' legitimate needs.

In cases where users have electronic access to the system, the terms "access" and "disclosure" become virtually synonymous in meaning. However, in other situations disclosure of information may require the active participation of a registry staff member through such means as telephone responses, preparation of special reports, or preparation of data files. Special policies may be needed in these situations to provide guidance to registry staff in protecting confidentiality. Earlier an example was cited of a school nurse having registry access only for the purpose of determining the names of students who are known to

be up to date. This example is again referenced to illustrate one approach to minimizing the potential for risk of disclosing sensitive data when registry staff assist users with access.

Another area of concern which might be addressed in a policy on confidentiality is the identification of geographic areas where overall coverage levels are low ("pockets of need"). Identification of "pockets of need" may be necessary for public health planning and outreach activities, but does not necessitate revealing individual data. Yet another possibility might require supporting a provider whose electronic access fails and who then telephones the registry for needed information. In this case positive identification of the provider is necessary before any data is released. Identification may take the form of verbal verification or a secure way for the provider to telephonically enter an identification number or password. The confidentiality policy should preclude any sensitive personal information being released verbally over the telephone. Consideration might be given to using only fax transmissions to the provider's **verified** office fax number. By so doing, the registry can protect against unknowingly disclosing information to an individual who telephones requesting information, impersonating a provider, parent, or guardian.

PENALTIES FOR UNAUTHORIZED DISCLOSURES

Commensurate penalties may discourage abuse or inappropriate use of the registry. For example, 16 states have imposed penalties for the unauthorized disclosure of immunization data.[**********] The confidentiality policy might establish other penalties, such as suspension or dismissal of employees, if permitted under the law. Regular periodic review and update of penalty provisions are recommended. Other considerations about penalties include:

- Penalties for public sector providers are generally addressed in state laws and regulations.

- Penalties for unauthorized disclosures by private providers, including those employed by managed care organizations, might be structured and promulgated to apply to:

  - the organization as a whole,

  - to individuals within the organization, or

  - both the organization and the individual. Penalties could be designed to apply to the individual who releases information without authorization, and/or to staff who did not adequately supervise that employee or maintain the security system.

- Penalties may be established for people who receive immunization information they

---

[10] Gostin, L.O., Lazzarini, Z. Childhood Immunization Registries. JAMA. 1995; 274:1796

know was obtained without authorization. These penalties may apply to individuals and organizations.

- Penalties may be administrative, civil, criminal, or result in professional sanctions.

Laws may exist or be developed to protect providers and health care organizations from liabilities or other penalties when they make disclosures in good faith or within the law.

4: SUMMARY OF FIFTEEN KEY ACTION STEPS: CONFIDENTIALITY

1. Recognize that absolute protection of electronically stored data on individuals from inappropriate disclosure or abuse is not possible. The only data that cannot be disclosed is that which is never collected.

2. Obtain a review by expert legal counsel on the applicability of all relevant Federal, state, local, or other (e.g. military) laws, regulations and penalties. Particular attention should be given to those pertaining to medical records.

3. Identify potential areas of confusion or omission in existing laws, regulations, and penalties. Determine whether legislative or administrative clarification specific to an immunization registry is necessary.

4. Prepare a written confidentiality policy. This document should be based upon the best interpretation by legal counsel of existing or proposed laws, regulations, or penalties. Seek community input to best ensure that it represents a fair balance between protecting the community through high immunization rates, and protecting individuals' confidentiality.

5. Ensure that all critical terms are adequately defined within the confidentiality policy to prevent misinterpretation.

6. Determine an acceptable approach within the community to informing individuals that information about them or their children will be in an immunization registry, how their confidentiality will be protected, and affording them the opportunity to decline to be included.

7. Scrutinize all aspects of the registry's technical design and operational procedures for possible confidentiality implications.

8. Define the data set to be collected. Minimize collection of information that could be potentially harmful to individuals if inappropriately disclosed.

9. Assign levels of sensitivity to all data elements to be collected. Define the stringency with which they must be protected against inappropriate disclosure. Demographic information, particularly that potentially useful in locating individuals, should be treated as sensitive and confidential.

10. Specifically define the purposes for which access to data may be routinely granted according to each category of qualified user. Delineate the methods by which their authorization will be verified. Include atypical situations such as when there is a system malfunction requiring normal procedures to be circumvented.

11. Provide for systems to record when and by whom access to the registry database is sought. In this way attempts to gain unauthorized access can be noted.

12. Specify the amount of information that must be entered by users prior to gaining access to any record, and to what extent they may "browse" the registry searching for the correct individual without entering more than a name.

13. Establish and publicize guidelines in advance on how to respond to requests for data from researchers, the justice system, government agencies, and other organizations.

14. Develop explanatory and training materials in "non-legal" language defining the responsibilities of users and operators to protect confidentiality. Establish mechanisms to obtain from providers and their staffs, system operators, and others participating, written agreements accepting these responsibilities.

15. Incorporate a specific requirement that the confidentiality and security policies are formally reviewed and re-evaluated at set time intervals. Ensure that there is a procedure in place to update them and re-educate the public and users concerning system changes.