Ethics in Public Health Research

Privacy and Public Health at Risk: Public Health Confidentiality in the Digital Age

Julie Myers, MD, Thomas R. Frieden, MD, MPH, Kamal M. Bherwani, and Kelly J. Henning, MD

Public health agencies increasingly use electronic means to acquire, use, maintain, and store personal health information. Electronic data formats can improve performance of core public health functions, but potentially threaten privacy because they can be easily duplicated and transmitted to unauthorized people.

Although such security breaches do occur, electronic data can be better secured than paper records, because authentication, authorization, auditing, and accountability can be facilitated. Public health professionals should collaborate with law and information technology colleagues to assess possible threats, implement updated policies, train staff, and develop preventive engineering measures to protect information.

Tightened physical and electronic controls can prevent misuse of data, minimize the risk of security breaches, and help maintain the reputation and integrity of public health agencies. (*Am J Public Health.* 2008;98:793–801. doi:10.2105/AJPH.2006.107706)

BALANCING PERSONAL AND societal interests has always been a challenge. As a society, we place great value on individual rights and uphold the importance of protecting personal information from external, and especially governmental, intrusion.[1] However, the acquisition, storage, and use of personal health information are required for many core public health activities.[2]

Concerns about confidentiality have fueled debates about the proper balance of individual and societal interests. Disease surveillance and reporting have often been controversial, particularly for sexually transmitted disease and tuberculosis in the first half of the 20th century[3] and more recently regarding HIV[4] and diabetes.[5] New York City's public health champion of the early 20th century, Hermann M. Biggs, MD, recognized that the only way to make public health reporting more acceptable was to ensure confidentiality. As Biggs explained in 1897 when emphasizing the confidentiality of tuberculosis reporting, "Notification to [public health] authorities does not involve notification to the community at large."[6(p155)]

Confidentiality concerns are even more sensitive in the digital age. High-profile breaches of individuals' health information have heightened anxiety about privacy,[7] as have plans to create interconnected electronic health information networks.[8] In the public health arena, several well-publicized breaches have occurred within the past few years, including the accidental attachment of an electronic file containing the names and addresses of 6500 HIV/AIDS patients to an e-mail in a county health department,[9] the theft from an employee's car of a state health department laptop computer containing information on approximately 1600 families,[10] and a state health department employee's misuse of a computerized list of AIDS patients to look up acquaintances,[11] among other breaches.[12–15]

Although only a few of these incidents have received significant media attention, breaches might not be particularly rare. Despite a possible reporting bias caused at least in part by increased scrutiny given matters of information technology over the past 8 to 10 years, security breaches appear to have increased in general and in the medical field in particular;[15,16] there is no reason to think that public health departments are immune from the phenomenon. In fact, when probed, one quarter of state public health agencies reported at least 1 security breach in the previous 2 years,[17] and a similar proportion of health care information executives and security officers reported attempted or successful intrusions into their companies' electronic information systems within the previous year.[18] These incidents are probably underestimated, given the increasing extent to which public health agencies have been operating and transmitting information electronically in recent years, although the data to confirm an increasing trend (such as comparative studies of breaches in the pre–electronic and electronic eras) are lacking. Although breaches occurred in the pre–electronic era, and continue to occur involving data in paper formats, certain features of electronic data have dramatically increased the potential magnitude and severity of these incidents.

Here, we identify and provide means to address threats to the delicate balance between the need for public health agencies to acquire data and the demand for security of sensitive information.

This review is particularly relevant to those who are implementing programs but are not yet fully conversant with information technology security principles and practices; a basic understanding of these topics is important for effective collaboration and cooperation with colleagues in multiple fields, including those in information technology. This review applies not only to public health agencies, but also in clinical, research, and academic settings. Preventive measures including policies, education, and engineering controls can be implemented to protect data; some emerging technologies may further strengthen data security. Failure to take preventive action can put both privacy and public health at risk.

COMPETING DEMANDS IN THE PUBLIC HEALTH CONTEXT

Public health agencies frequently require individually identifiable health information to conduct certain public health activities. An increasing number of functions, including terrorism preparedness, public health surveillance, outbreak and incident investigations, program implementation and evaluation, and direct health services such as clinical public health services and research, require the acquisition, use, maintenance, and storage of personal health information. Successful execution of these functions depends on data quality and accessibility.[2]

Heightened security is paramount to maintaining public confidence; good health care and good public health practice depend on patients providing accurate, sensitive information to their providers in a timely manner. Patients are justifiably concerned that a breach may lead to embarrassment, stigma, or discrimination; that they could potentially lose their job, health insurance, and housing[1]; or they could suffer other serious consequences. Patients may also be increasingly wary of breaches as reports of identity theft from illicitly obtained identifiable health information become more common.[19] As perceived risks of privacy or security breaches increase, patients might avoid care.[20,21] Such behavior could harm an individual's health (e.g., forgoing tests or treatment to avoid collection of personal health information),[20,21] as well as the public's health (e.g., avoiding treatment for a contagious disease as a result of fearing an invasion of privacy).[20]

Certain information, including HIV/AIDS surveillance information and mental health or substance abuse data, is particularly sensitive and often receives greater confidentiality protection under the law[22]; some states and localities have enacted "superconfidentiality" laws for these diseases.[23] However, placing restrictions on data acquisition, use, and disclosure also poses risks, particularly if these restrictions impede acquisition of key surveillance data that would otherwise be used to prevent disease, investigate causation, or identify and enable interventions to protect an exposed population.[20]

THE MIXED BLESSING OF THE DIGITAL AGE

Improved information technology benefits many areas of public health including health care delivery, surveillance, research, and education.[24] Electronic patient information offers many advantages over paper records. For example, information can be more easily standardized, permitting faster retrieval and review. The number of forms, both paper and electronic, can be reduced as well. Although institutions transitioning to electronic data will incur costs initially, this transformation could ultimately increase data reliability and access, reduce errors, and save money.[25] Additionally, electronic data can potentially permit real-time public health surveillance[21] and facilitate faster emergency response. Although not within the scope of this article, other benefits of implementing electronic systems include improved data collection speed, reduced errors in field research settings (with the use of electronic devices and data collection), and improved health education and training programs (with enhanced electronic access to essential information).

In some ways, electronic media may be easier to protect than paper records, because authentication, authorization, and auditing—the key components of identity and access management—are all facilitated. Authentication, the process of determining whether the person accessing data is authorized to do so, can restrict access to sensitive electronic databases. Information in these databases can be organized into security levels, giving users access to different levels of information depending on each user's security clearance.[1] For example, with paper records, clerical staff can have access to an entire record; with electronic records, this access can be limited only to that information to which that specific person has a right and a need to know. Public health agencies can improve accountability by establishing the capacity to create a precise audit trail that determines who has accessed a record, when the record was accessed, and what changes if any were made to the record.[26] Authentication, multilevel authorization, and audit trails are difficult or impossible to implement with paper records.

However, some features of electronic data present significant security threats. Information can be easily and rapidly copied, transported (e.g., via mobile computers such as laptops or portable media devices such as flash drives), and disseminated (e.g., via e-mail or Web posting) using a variety of wireless or wired networks, anywhere in the world, at little or no cost, in very little time, and possibly without a trace. This would have been impossible in the era of paper records. Furthermore, access may be uncontrolled, or access controls may fail; often, a single entry point provides access to information about many thousands of individuals.[27] In addition, tampering with unprotected electronic files may be more difficult to detect.[26]

THREATS

Security threats are both physical and electronic (Table 1). Devices that might threaten physical and electronic security if stolen or illicitly accessed include wireless e-mail devices (e.g., Blackberries), tokens used for remote network access ("hard tokens"), portable flash drives and other portable media, and computers (both stationary desktops and portable laptops). Network access management and information transfer (i.e., fax or e-mail), either intra- or extrainstitutional, also pose unique challenges (Table 2).

Public health departments are also at risk for internal and external intruders (Table 3). Internal intruders include current employees with malicious intent as well as former employees or contractors whose physical or electronic access has not been revoked. Current employees with electronic access to agency systems may abuse their access or hack into systems without authorization. External intruders may be burglars, who threaten physical security, or hackers, who threaten electronic security. Therefore, intrusion detection and prevention systems should be deployed to monitor both internal and external networks.

PREVENTION

Policy

Although the federal Health Insurance Portability and Accountability Act (HIPAA) has strengthened protections for health information in some medical contexts, public health agencies are largely exempt from HIPAA except when providing direct care and electronically transmitting information in connection with certain transactions (e.g., billing).[28] States and municipalities have been assigned primary responsibility for protecting public health confidentiality, yet state and local public health laws vary and have been described as "antiquated, fragmented, inconsistent and incomplete."[29(p77)] Only one third of state public health agencies have written policies regarding privacy and confidentiality of patient information.[17]

Even where they exist, state and local public health laws pertaining to the protection of health information require review and reform.[29] Several model acts have been proposed[2,29,30] but not widely adopted. To prevent information breaches that might erode the public's trust, state and local public health agencies should implement and enforce new policies.

As a preventive measure, public health agencies should establish routine disclosure protocols. Such protocols should include a brief verification process consisting of 4 separate confirmations: (1) the appropriateness of the disclosure (i.e., is the disclosure authorized by policy or law?), (2) the integrity of the information being disclosed (i.e., if the information is being manipulated for purposes of disclosure, has it been double-checked to verify that it still accurately reflects the information received by the agency?), (3) the identity of the person receiving the disclosed information (i.e., is this person authorized to receive this information?), and (4) the security of the mode of information transmission (i.e., is this how information is usually sent to this person?).

Before allowing nonroutine disclosure (i.e., if an aspect of a routine disclosure changes or disclosure occurs outside of regular operations), public health departments should follow a written policy that ensures a brief period of contemplation, or time-out, to minimize risk of improper disclosure. The concept of a time-out has recently been adopted by clinical medicine in high-risk settings and may also be applied to risky disclosures in public health settings. This time-out involves a pause in activity to review the impending disclosure. The time-out should be adapted to the specific setting of the disclosure but should include at least the above 4 verifications plus an additional reverification (or double-check) in consultation with a program-level personnel expert in the program's confidentiality policy. In particularly complicated cases, legal counsel should also be consulted for guidance.

Practice

Public health agencies can incorporate specific measures into practice to prevent physical and technological security breaches (Tables 1–3). Prevention strategies can be divided into 2 major categories: education and preventive engineering. Although education is important, human error will always occur; embedding preventative measures into both electronic and organizational structures is essential.

Education

Education, including technical training and empowering personnel around issues of confidentiality, is an integral part of prevention in the public health agency setting. Contrary to popular belief, most breaches arise internally and are not initiated by external hackers.[17,26] Educational initiatives are needed to create cultural change within health departments,[26] with a move toward greater vigilance in handling documents and devices as well as greater accountability for data protection. State and local public health agencies should consider designating a high-level official (e.g., a Public Health Information Officer,[30] Chief Information Security Officer, or Chief Privacy Officer) to oversee and lead this charge. This official's mandate should include developing and organizing staff training, monitoring the security of the local environment, and enforcing local policies. Knowledge of state and local laws pertaining to privacy protection and of applicable record retention policies is also important, as is a close working relationship with a high-level information technology expert, such as the Chief Information Officer, who can assist in developing appropriate electronic security systems and policies for handling identifiable health information in an electronic format, as well as adapting them as new threats inevitably arise.

Special training is needed to ensure that practice is consistent

TABLE 1—Potential Physical and Electronic Security Threats to Patient and Personal Information

Risk	Risk Description	Prevention (Education)	Prevention (Preventive Engineering)
Sites			
File/server rooms	Access keys may be copied. Keys may be retained by employees after termination or reassignment. Combinations of locks may be shared or not changed often enough.	Establish a policy that instructs users not to copy keys or share combinations.	Restrict access to file/server rooms to authorized users. Video surveillance of file/server rooms. Ensure that access is appropriately assigned/de-assigned depending on user's status. For highly sensitive file/server rooms, create multifactor authentication access including biometric validation and restrict access to when supervisor is present.
Desks/work stations	Sensitive information may be left on a desk or, if placed inside desk, in an unlocked drawer or cabinet.	Establish a policy that instructs users not to leave sensitive data on desks or in unlocked drawers/cabinets.	Assemble desks and structure work stations separated by spaces or partitions to create and maintain a secure work environment.
Paper media			
Print outs (paper reports of electronic data)	Sensitive information is left in a printer before being retrieved, is sent to the wrong printer, or is improperly discarded.	Establish a policy that instructs users not to leave sensitive data on printers, to confirm the printing location of sensitive information, and to avoid making copies of sensitive data. Establish a policy that instructs users to expunge print outs appropriately (e.g., by shredding) when no longer necessary according to established record retention policy.	Disconnect servers containing sensitive data from printers. Enable only local printers for computers containing sensitive information.
Faxes	May go to unintended phone number (i.e., different organization) or recipient (i.e., incorrect person at correct organization). May not include confidentiality statement.	Establish a policy that instructs users about verification of fax number before sending fax and about coordination of fax transmission between sender and recipient. Post reminder signs beside fax machines to include confidentiality statement with faxes. Establish a policy that instructs users to consider other, more secure means of transmission for sensitive information.	Program fax machines with speed dial function and master lists to avoid dialing errors. Restrict certain fax machines to dial only certain numbers. Program fax machines to automatically include confidentiality statement with all faxes.
Electronic devices			
Wireless devices (e.g., Blackberries)	May be lost or stolen. May not be password protected. May not be collected upon employees' leaving the agency.	Establish a policy that instructs users not to leave sensitive data on devices.	Enforce password protection on all devices and encrypt all devices. Employ inventory control procedures and deactivate devices if unaccounted for.
Flash drives/other portable media	May be lost or stolen. Data may not be appropriately expunged from portable media after transfer of information.	Establish a policy that instructs users not to leave sensitive data on portable media other than for a specific information transfer and to expunge copies appropriately immediately after transfer.	Create chain of custody for all sensitive data on removable media. Use encryption-enabled portable media. Host sensitive data on thin client or other computers without data (e.g., USB) ports. Password protect flash drives and employ biometric authentication if drive used for sensitive data.

Continued

TABLE 1—*Continued*

Remote intranet access tokens (for multifactor authentication)	May be lost or stolen. May not be collected/de-activated upon employees' leaving the agency.	Establish a policy that instructs users about the importance of careful handling of token.	Ensure that token is recovered when user no longer requires access. Consider assigning "smart cards" for multifactor authentication (token implanted within a wallet-card format; decreased likelihood of being misplaced compared with standard remote access token). Employ inventory control procedures and de-activate token if unaccounted for. Monitor use and map to authorized employees to identify users, and deactivate any unauthorized use.
Computers/drives/servers			
Computers (stationary desktops)	May be lost or stolen. Data may not be encrypted. Information stored on hard drive may not have been erased before being reassigned to another employee or discarded.	Establish a policy that instructs users not to leave sensitive data on hard drive. Track computers to ensure that data are appropriately erased, if appropriate, per the record retention policy.	Password protect all desktops. Encrypt hard drives of at least all desktops with sensitive data.
Computers (portable laptops)	May be lost or stolen. Data may not be encrypted. Information stored on hard drive may not have been erased before being reassigned to another employee or discarded.	Establish a policy that instructs users about not storing sensitive data on laptops. Track computers to ensure that data are appropriately erased, if appropriate, per the record retention policy.	Password protect all laptops. Encrypt hard drives of at least all laptops with sensitive data. Centrally store all shared laptops in an area with restricted access.
Shared network drives	May be inappropriately used for storage of information to which not all shared users should have access.	Establish a policy that instructs users about appropriate storage of information on shared user drives.	Password protect shared user drives.
Servers (containing sensitive databases)	May be inappropriately accessed by unauthorized user. User may transfer sensitive information from server to unauthorized users via e-mail or portable media, or to other application.	Establish a policy that instructs users about appropriate handling of sensitive information.	Create thin client workstations for managing data on an isolated network (no other applications and no internet access available at workstation, beyond data-entry program; no external drives, data ports, or printers or ability to install them). Encrypt server. Encrypt back-up of server; store in off-site location with restricted access. Video surveillance of file/server rooms. Audit both user access of and activity on the server.

with policy in any authorized disclosures of personal health information, because the risk of a breach is particularly great when information changes hands.

Preventive Engineering

Preventive engineering is a traditional and effective public health strategy[31] in that it shifts responsibility for action away from the individual, making the default choice the safest choice. Limiting both electronic and physical access is a preventive engineering approach essential to preventing breaches. Access control consists of 3 processes: authentication, authorization, and auditing. Authentication is the process of confirming user identity and can involve multiple factors. *Single-factor authentication* refers to something the user *knows* (e.g., a password); *multifactor authentication* might add either something the user *has* (e.g., remote access token, smart card) or *is* (e.g., biometric characteristic such as voice print verification, fingerprint, or retinal scan).[32] Recent technologies have greatly improved access to and reduced the cost of biometric (particularly fingerprint) authentication.

Ideally, authentication for access to sensitive areas or networks should include at least 2 factors, a physical device (e.g., remote access token) and a

TABLE 2—Potential Network Access Management and Information Transfer Security Threats to Patient and Personal Information

Risk	Risk Description	Prevention (Education)	Prevention (Engineering)
Network access management			
Within agency	Sensitive data on health department intranet accessible to unauthorized user, either on-site or remotely.	Not applicable.	Establish effective centralized processes for access provision and revocation and password reset. Require at least single-factor authentication for on-site network access.
Remotely	Sensitive data on health department intranet accessible to unauthorized user, either on-site or remotely.	Not applicable.	Require multifactor authentication for remote network access and access to sensitive information
Information transfer (e.g., e-mail)			
Within health department	Sensitive data transmitted in inappropriate format.	Establish a policy that instructs users about best practices for transfer of sensitive data via e-mail.	Not applicable.
Outside health department	Sensitive data transmitted in inappropriate format. Sensitive data transferred to and from unauthorized users.	Establish a policy that instructs users about best practices for the transfer of sensitive data via e-mail. Establish a policy that instructs users to request encryption of all sensitive data being transmitted via e-mail.	In the future, employ agency-wide e-mail encryption and quarantine of suspicious emails.

biometric characteristic. There should also be a requirement for reauthentication after a period of time. For highly sensitive information, protocols that include biometric authentication should be standard. For example, the HIV Surveillance and Epidemiology Program at the New York City Department of Health and Mental Hygiene installed an access control system so that individuals entering the area containing the HIV/AIDS registry server cannot proceed unless they simultaneously confirm their identity by fingerprint with a biometric scanner and swipe a smart card through a digital reader.

Authorization is the process used to determine whether a user should be granted access on the basis of that user's job title, function, and information acquisition needs. Public health agencies should centralize the provision and revocation of access, with substantial input from program supervisors. Frequent auditing serves as both a deterrent and form of enforcement, and should be carried out electronically (e.g., surveilling network access logs) as well as physically (e.g., video surveillance of highly sensitive areas). For example, in the HIV Surveillance and Epidemiology Program, digital video recorders were installed both inside and outside the main entrance as well as within the server room.

Preventive engineering can also include computerized applications to prevent and detect electronic intrusion (i.e., hacking). In areas in which concern about hackers is greatest and in which highly sensitive information is involved, agencies should isolate servers on internal networks without internet connections and use desktop computers that cannot transport data in and out either physically or electronically ("thin clients"). Use of thin clients, which lack Internet access and do not contain hard drives, ports for portable media (e.g., flash drives), or printers, also eliminates the possibility that authorized users will inappropriately transmit highly sensitive information. Another aspect of a systems approach to security is encryption, which is possible for both data "at rest" (i.e., stored on a computer's hard drive) and data "in flight" (i.e., transmitted over a network). Servers, desktop computers, mobile computers, portable media, and e-mail or other forms of data transmission can all be encrypted. Encryption is an important component of preventive engineering because, even if a physical or electronic intrusion occurs, confidential information will still have a high degree of protection.

A summary of key strategies for handling sensitive and highly sensitive information can be found in the box on page 800.

EMERGING TECHNOLOGIES

Several emerging technologies may further improve the ability of public health agencies to

TABLE 3—Risks to Public Health Departments, by Type of Intruders and Security Threats Posed

Risk	Risk Description	Prevention
External intruders		
Physical intruders (i.e., burglars)	Physical theft of health department property such as files and computers.	Lock buildings. Employ security guards and require identification for access. Centralize and enforce access management. Encrypt sensitive computers so that data are unavailable if computers are stolen or otherwise accessed.
Electronic intruders (e.g., hackers)	Unlawful access to equipment (desktop or laptop computers) or network (intra- and internet). May create hole for subsequent hacking (e.g., by sending viruses to Web-based e-mail).	Enhance both intrusion detection and intrusion protection systems. Contract with "ethical hacking" firms to identify and fix vulnerabilities.
Internal intruders		
Current employees	Internal access with malicious intent.	Background checks of all personnel handling sensitive data. Video surveillance of areas where highly sensitive data are stored. Monitor Web-browsing activity of personnel.
Former employees	Continued physical and electronic access despite termination of employment with the agency.	Immediately and automatically revoke access, both physical (i.e., keys, identification card) and electronic (i.e., network access, remote access token), upon termination.

maintain the privacy and security of records in transmission or storage. Most of these technologies have already been widely adopted in other fields, such as finance and commerce. Some of this technology has also been adopted within clinical arenas, but in general, adoption by public health agencies lags behind.

Write Once, Read Many (WORM) technology and electronic signatures can protect the integrity of an electronic file during transmission and storage. WORM prevents data modification after the initial file is created; the file can only be altered through tracking every change since the file's creation. For example, WORM can protect digital copies of health department–generated birth or death certificates against tampering. Electronic signatures also protect a file during transmission and storage. Three elements compose electronic signature technology: verifying a signer's identity, assuring the authenticity of the document, and using techniques that make it difficult for signers to claim they did not actually sign the document (nonrepudiation).[33] Although being utilized increasingly in clinical care settings, this technology has not yet been widely adopted in the public health sphere.

Technology is evolving to scale up multifactor authentication in situations in which many users require remote access to a given network. In such instances, the cost and administrative complexity of distributing separate pieces of hardware (e.g., remote access devices or smart cards) becomes too burdensome. Instead, remote access control can be achieved through use of "soft tokens," which are digital certificates downloaded to an identified user's computer. (The digital certificate becomes the second authentication factor, where the user identification and password is the first.) For example, health departments can provide soft tokens to community-based physicians that grant remote access to the agency's server to securely submit required health documents.

New technology also allows for the creation of a single sign-on to agency networks. By moving user identifications and passwords into a centrally organized directory, users need only log onto the network once, without having to log on separately for each application they wish to use. The philosophy behind this approach is to enforce a single, secure authentication step instead of multiple weaker steps that encourage people to use the same easy-to-remember (and potentially easy-to-guess) password for the different systems and applications they use, or to write down their numerous passwords in nonsecure locations.

Another promising technology is digital rights management. Already in use to protect copyrighted materials such as recorded music, this technology might be applied to protect public health agency data. Digital rights management would allow the data's owner to designate access for only a finite period, after which access expires. For example, this technology might enable the tuberculosis control bureau of a public health department to disclose the record of a patient's previous tuberculosis treatment to a physician currently treating the patient's relapse, but would only permit the physician to read this record within a specified time from its receipt, and could place additional controls over whether the information can be copied, disseminated, or printed. This technology helps preserve confidentiality even after data disclosure and limits harm in the event of a breach.

The rapid pace of technology development and evolution underscores the importance of guidance from high-level information technology experts regarding the

Key Strategies for Handling Routine Sensitive and Highly Sensitive Information Through Prevention, Practice, Education, and Preventive Engineering

Routine sensitive information

1. Designate a high-level individual in the agency for leadership and oversight of confidentiality and security issues (e.g., public health information officer, chief information security officer, or chief privacy officer).
2. Create a comprehensive agency confidentiality policy to instruct personnel on best practices paired with an interactive training program about critical security issues, including how to report a suspected breach.
3. Review and analyze data and storage practices and perform a detailed, periodic audit of vulnerabilities.
4. Establish centralized processes for access provision and revocation as well as password reset; automatically revoke access at the end of employment and when on an extended leave of absence.
5. Secure and encrypt computers and laptops that store sensitive data to limit breaches if the device is stolen; enable only local printers for computers containing sensitive information.
6. Require multifactor authentication for remote network access with the use of user identification and password login plus a remote access token; require re-authentication after a period of inactivity on the network.
7. Require password protection on all wireless devices, portable media, desktops, laptops, and shared user drives.
8. Employ electronic intrusion detection and protection systems; test integrity of network by hiring independent computer security professionals to perform "ethical hacking" to identify security gaps.
9. For routine authorized disclosures, establish a brief verification protocol for personnel to confirm the following:
   a. The appropriateness of the disclosure,
   b. The integrity of the information being disclosed,
   c. The identity of the person receiving the information, and,
   d. The security of the mode of transmission before the release of sensitive information.
10. For nonroutine authorized disclosures, establish a "time-out" period (i.e., a contemplative pause in activity) to both double-check the above verifications and to consult with someone expert in the program's or agency's disclosure policy.

Highly sensitive information

1. Perform a background check of all personnel handling highly sensitive information.
2. Host highly sensitive information on thin client workstations on isolated networks with no other applications, no Internet access, no external drives, data ports (e.g., USB ports), or printers.
3. Restrict access to rooms containing highly sensitive information by use of multifactor authentication, including biometric validation (e.g., hand scan).
4. Perform video surveillance of rooms in which highly sensitive information is stored or electronically accessed.
5. Regularly audit both user access of and activity on servers containing highly sensitive information.

rational acquisition and adoption of technology.

CONCLUSION

Public health agencies are challenged to balance the best interests of the public's health with the rights and privileges of individuals.[2] Public health agencies should assess all possible threats and address as many as feasible using policies, education, and preventive engineering. Emerging technology may help address threats by enhancing the privacy and security of data in transmission and storage. Although an assurance of perfect privacy of health and personal information is impossible, public health agencies should minimize risk by improving staff skills and the ways data are acquired, used, maintained, stored, and shared. Individuals will be more likely to provide personal health information if they have confidence in the security of their data. Public health agencies must proactively impose data security; they depend on the data they receive to promote and protect the public's health. ■

About the Authors

J. Myers, T.R. Frieden, K.M. Bherwani, and K.J. Henning are with the New York City Department of Health and Mental Hygiene, New York, NY.

Requests for reprints should be sent to Thomas R. Frieden, New York City Department of Health and Mental Hygiene, 125 Worth St, Rm 331, New York, NY 10013 (e-mail: tfrieden@health.nyc.gov).

This article was accepted September 29, 2007.

Contributors

T.R. Frieden conceptualized the article. J.E. Myers led the writing. T.R. Frieden, K.M. Bherwani, and K.J. Henning provided key comments on content and reviewed drafts of the article.

Acknowledgments

The authors thank Drew Blakeman for assistance with article preparation and Wilfredo Lopez, JD, Roslyn Windholz, JD, Emily Flynn, and Shadi Chamany, MD, MPH, and Stanley Trepetin, PhD, for thoughtful review of the article. Lucia Torian, PhD, provided key insight about many of the confidentiality and security issues described here.

Human Participant Protection

No human participants were involved in this study.

References

1. Gostin L. Health care information and the protection of personal privacy: ethical and legal considerations. *Ann Intern Med.* 1997;127(8 Pt 2):683–690.
2. Gostin LO, Hodge JG Jr, Valdiserri RO. Informational privacy and the public's health: the model state public

health Privacy Act. *Am J Pub Health.* 2001;91:1388–1392.

3. Fairchild AL, Colgrove J, Bayer R. The myth of exceptionalism: the history of venereal disease reporting in the twentieth century. *J Law Med Ethics.* 2003;31:624–637.

4. Bayer R, Fairchild A. The limits of privacy: surveillance and the control of disease. *Health Care Anal.* 2002;10:19–35.

5. Fairchild AL. Public health: diabetes and disease surveillance. *Science.* 2006;313:175–176.

6. Winslow C-EA. *The Life of Hermann Biggs.* Philadelphia, PA: Lea and Febiger, 1929.

7. Editorial. Rebooting Veterans Affairs. *The New York Times.* August 10, 2006:A22.

8. Starr P. Smart technology, stunted policy: developing health information networks. *Health Aff.* 1997;16(3): 91–105.

9. Daugherty J. E-mail gaffe reveals HIV, AIDS names. *Palm Beach Post.* February 20, 2005:1b.

10. The Denver Channel. Patients not notified that their health records were stolen. *The Denver Channel.* May 2, 2005. Available at: http://www.thedenverchannel.com/7newsinvestigates/4438964/detail.html. Accessed November 3, 2006.

11. Pittman C. Ruling propels AIDS-list case towards trial. *St. Petersburg Times.* July 31, 1997:B3.

12. Associated Press. Computer stolen from state health office in Montana. *Boston Herald.* July 7, 2006. Available at: http://attrition.org/dataloss/2006/07/montana01.html. Accessed October 17, 2006.

13. Norris K. 4,000 People at risk of ID theft, state says. *Detroit Free Press.* September 16, 2006. Available at: http://attrition.org/dataloss/2006/09/mdch01.html. Accessed November 3, 2006.

14. Kestin S. Workers say they were told to destroy report on AIDS records. *Tampa Tribune.* November 7, 1996:Nation/World,1.

15. Privacy Rights Clearinghouse. Chronology of Data Breaches database. Available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP. Accessed June 24, 2007.

16. Etiolated Consumer\Citizen. Privacy breach database search engine; organization type medical, publicized incidents, since 2003. Available at: http://etiolated.org/search. Accessed June 24, 2007.

17. O'Brien DG, Yasnoff WA. Privacy, confidentiality, and security in information systems of state health agencies. *Am J Prev Med.* 1999;16:351–358.

18. Morrissey J. Securing the Internet frontier. *Mod Healthc.* 1996;26:56–64.

19. American Society for Healthcare Risk Management. ID theft in health care emerging as major risk. *J Healthc Risk Manag.* 2006;Nov:124–128.

20. Deapen D. Cancer surveillance and information: balancing public health with privacy and confidentiality concerns (United States). *Cancer Causes Control.* 2006;17:633–637.

21. Rothstein MA, Talbott MK. Compelled disclosure of health information: protecting against the greatest potential threat to privacy. *JAMA.* 2006;295: 2882–2885.

22. Turkington RC. Medical record confidentiality law, scientific research, and data collection in the information age. *J Law Med Ethics.* 1997;25: 113–129.

23. Hodge JG Jr, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. *JAMA.* 1999;282:1466–1471.

24. Bellows B, Bhandari A, Ibrahim M, Sandhu JS. Peering into the black box: a holistic framework for innovating at the intersection of ICT and health. In: Gasco-Hernandez M, Esquiza-Lopez F, Acevedo-Ruiz M, eds. *Information Communication Technologies and Human Development.* Hershey, PA: Idea Group; 2007:235–265.

25. Wang SJ, Middleton B, Prosser LA, et al. A cost-benefit analysis of electronic medical records in primary care. *Am J Med.* 2003;114:397–403.

26. Morrissey J. Data security. *Mod Health.* 1996;26:32–38.

27. Lillis K. Going global: AHIMA convention offers international perspective on health information management, along with the hottest HIM issues of the day. *Health Manag Technol.* 2004;25: 26–28.

28. Centers for Disease Control and Prevention. HIPAA privacy rule and public health: guidance from CDC and the US Department of Health and Human Services. *MMWR Morb Mort Wkly Rep.* 2003;52(suppl):1–20.

29. Hodge JG Jr, Gostin LO, Gebbie K, Erickson DL. Transforming public health law: the Turning Point Model State Public Health Act. *J Law Med Ethics.* 2006;34:77–84.

30. Public Health Statute Modernization National Excellence Collaborative. *Turning Point Model State Public Health Act.* September 2003. Available at: http://www.hss.state.ak.us/dph/improving/turningpoint/PDFs/MSPHAweb.pdf. Accessed November 3, 2006.

31. Lee T, Jordan NN, Sanchez JL, Gaydos JC. Selected nonvaccine interventions to prevent infectious acute respiratory disease. *Am J Prev Med* 2005; 28:305–316.

32. M-Tech Information Technology, Inc. Password Management Best Practices. Available at: http://psynch.com/docs/password-management-best-practices.html#variousauth. Accessed November 3, 2006.

33. Security and electronic signature standards–HCFA. Proposed rule. Fed Reg. 1998 Aug 12;63(155):43242–43280. To be codified at 45 CFR § 142.