

VERMONT2007

HIV Name-Based Reporting

Report to the Legislature on **Act 73** (2007-08)
January 15, 2008



DEPARTMENT OF HEALTH
Agency of Human Services

108 Cherry Street, PO Box 70
Burlington, VT 05402
1.802.863.7341
healthvermont.gov

Table of Contents

Executive Summary	4
Introduction	5
Security Audit	6
Community Input on Security and Adequacy of Penalties	8
Conclusion	11

Executive Summary

A security audit carried out by the Department of Health found no “high” risk problems with the current security practices regarding the collection of reportable disease information, but recommended several low effort and cost measures to address “low” and “moderate” risk problems. These measures will be implemented and will enhance management, operational and technical security of the HARS and NEDSS information systems.

The penalties for unauthorized disclosure of medical information were deemed adequate following an analysis by the Department and a review by members of the HIV/AIDS community.

Introduction

Section 2 of Act 73 (2007-08) required the Department of Health to conduct an information and security audit by November 1, 2007 regarding reportable disease information collected under 18 VSA § 1001. The audit was to include an evaluation of the systems and procedures developed to implement § 1001 and an examination of the adequacy of penalties for disclosure by State personnel.

Section 2 also required the Department to report by January 15, 2008 to the Senate Committee on Health and Welfare and the House Committee on Human Services concerning options available, and the expected costs of such options, for maximizing protection of the information collected pursuant to § 1001.

The report was also to include the Department's recommendations on whether the General Assembly should impose or enhance criminal penalties on health care providers for unauthorized disclosures of medical information.

The Department was mandated to solicit input from AIDS service organizations and the community advisory group regarding the success of the Department's security measures and the examination of the adequacy of penalties as they apply to HIV/AIDS.

Security Audit

As required by Act 73, a security audit was conducted in October 2007 on the HIV/AIDS Reporting System (HARS), and the National Electronic Disease Surveillance System (NEDSS), which is the system used by the Department for collecting information on all reportable infectious diseases. HARS is an older data base system developed by CDC and resides on a stand-alone PC (not connected to the Department's computer network) in the HIV/AIDS program office. NEDSS is a more recent application, also developed by CDC, and used by many states as well as the Federal government. NEDSS has been built to meet today's higher standards for security.

The audit was done by the Information Systems Security Director of the Agency of Human Services using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems, and selected controls. This is a standard methodology recommended by Health and Human Services, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIV/AIDS Reporting System (HARS). The audit found that the HARS security protocols and practices were adequate to protect the data against security risks rated high. However, the audit did reveal moderate and low rated "potential risks" in the areas of Management, Operational and Technical Security. The options available to address these risks are limited because, as a non-networked system, the security of the data in HARS relies primarily on the physical security of the room in which the HARS computer resides. If the HARS database were on a networked system, it would be possible to enhance the security of the data to meet today's security standards. Until it can be replaced by a modern system, the audit recommended several safeguards to bolster the security of the existing system:

- Recommendation #1: Ensure that all staff (including IT) are trained on, understand, and follow the HIV/AIDS policy and procedures.
- Recommendation #2: Encrypt the entire hard disk and back-up copies.

- Recommendation #3: Strengthen auditing capabilities by changing local user accounts on the HARS PC and installing file auditing software to record users and actions taken on the files.
- Recommendation #4: Implement many minimum-effort, low-cost controls and safeguards including: require individual log on authorization to track users; adopt “strong” passwords; update the anti-virus software, activate the built-in firewall, and set the screensaver to lock the machine after 5 minutes of inactivity.

National Electronic Disease Surveillance System (NEDSS). The NEDSS vulnerabilities and recommended safeguards presented in the audit report have been reviewed by infectious disease epidemiology and information technology staff. Two of the recommendations from the audit can and will be implemented by Epidemiology staff within three months – add a staff separation section to the Infectious Disease Section Confidentiality and Security Policies and Procedures document; and fully promulgate that document. The remaining recommendations and controls are all information technology-related, and all of them address moderate and low risks. These will be reviewed, prioritized, assigned and implemented.

Community Input on Security and Adequacy of Penalties

Program staff have met with and solicited input from the HIV/AIDS community regarding the department's security measures to protect HIV case information, and the department's examination of the adequacy of penalties as they apply to unauthorized disclosure of HIV/AIDS medical information. In July, August, and November 2007, staff met with representatives of the following: AIDS Service Organizations; AIDS comprehensive care clinics; the HIV/AIDS program Community Advisory Group; HIV community members; Fletcher Allen Health Care; and Dartmouth Hitchcock Medical Centers. These meetings covered all aspects of the legislation (including patient notification and public education campaign), but focused on the department's security and confidentiality policies and procedures, and the adequacy of penalties for unauthorized disclosure.

Security. In general, the feedback from the community groups indicated that the department's current security measures, along with the enhancements planned, adequately address their concerns around security and confidentiality. We did, however, receive suggestions for changes to the security policies and procedures. These included using stronger passwords, prohibiting the use of laptop computers to collect or store HIV related information, and prohibiting the physical removal of HIV related files from the department offices. All suggestions from the community have been incorporated.

Adequacy of Penalties

Act 73 (2007-08) proposes to change the penalties for disclosure of the content of any confidential public health record without written authorization or as authorized by law or in violation of certain subsections of 18 VSA § 1001. Here is a summary of the new penalty provisions:

STATUTE	PROHIBITION	NATURE OF PENALTY	PENALTY
18 VSA § 1001(e)(1)	Willful or malicious disclosure of the content of any confidential public health record without written authorization or as authorized by law or in violation of 18 VSA § 1001(b)(c) or (d).	Civil	Between \$10,000 and \$25,000, costs and attorney fees as determined by the court, compensatory and punitive damages, or equitable relief, including restraint of prohibited acts, costs, reasonable attorney's fees, and other appropriate relief.
18 VSA § 1001(e)(2)	Negligent disclosure of the content of any confidential public health record without written authorization or as authorized by law or in violation of 18 VSA § 1001(b)(c) or (d).	Civil	Not to exceed \$2500 plus court costs, as determined by the court. Penalty and costs to be paid to the subject of the confidential information.
18 VSA § 1001(e)(3)	Willful, malicious, or negligent disclosure of the results of an HIV test to a third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply without written authorization or as authorized by law or in violation of 18 VSA § 1001(b)(c) or (d) that results in economic, bodily, or psychological harm to the subject of the test.	Criminal	Misdemeanor punishable by imprisonment for a period not to exceed one year or a fine not to exceed \$25,000, or both.
18 VSA § 1001(e)(4)	Any act described at (e)(1), (e)(2), or (e)(3).	Civil	All actual damages, including damages for economic, bodily, or psychological harm that is a proximate result of the act.

The revision also emphasizes that nothing in 18 VSA § 1001 limits or expands the right of an injured subject to recover damages under any other applicable law.

Section 2 of Act 73 requires, among other things, that the Department of Health report on whether the General Assembly should impose or enhance criminal penalties on health care providers for unauthorized disclosures of medical information. The Department must also solicit input from AIDS service organizations and the community advisory group regarding their examination of the adequacy of penalties as they apply to HIV/AIDS and include this input in the report.

The input solicited and received by the Department from AIDS service organizations and the community advisory group indicates that Act 73's penalties are adequate as they apply to HIV/AIDS. The Department agrees with this assessment and does not believe that the General Assembly should impose or enhance criminal penalties on health care providers for unauthorized disclosures of medical information.

Even with only a civil penalty in place for willful or malicious disclosure, the Department is not aware of any breaches of 18 VSA § 1001.

In addition, Act 73 expressly allows the use of other applicable laws such as the Health Insurance Portability and Accountability Act (HIPAA) and its attendant regulations. Under 42 USC § 1320d-6, a person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of \$50,000 and up to one year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

Act 73 penalties viewed in connection with HIPAA penalties provide substantial deterrence against unauthorized disclosure. The Department of Health sees no reason at this time to change the penalty provisions.

Conclusion

A security audit carried out by the Department of Health found no “high” risk problems with the current security practices regarding the collection of reportable disease information, but recommended several low effort and cost measures to address “low” and “moderate” risk problems. These measures will be implemented and will enhance management, operational and technical security of the HARS and NEDSS information systems.

The penalties for unauthorized disclosure of medical information were deemed adequate following an analysis by the Department and a review by members of the HIV/AIDS community.