



**Information Security Office
2005 Safeguard Assessment Summary Report
January 20, 2006**

Introduction

The Department of Human Services successfully completed its third annual Safeguards Assessment. Administrative, Technical, and Physical Safeguards Policy AS-100-05, and federal HIPAA Privacy and Security Rules require DHS to apply reasonable safeguards to all information assets. The policy applies to information assets in any medium, and requires that a Safeguards Assessment be completed annually.

The Safeguards Assessment is intended to help DHS managers and supervisors conduct a self-assessment to determine if reasonable administrative, technical, and physical safeguards are in place to protect information assets.

The assessment does not result in an actual score, but rather results in a remediation plan where needed. Meeting a safeguard at least 75% of the time is considered compliant. Some elements of the assessment are not applicable to all parts of the Department. Therefore, there is a “Not Applicable” option on the assessment tool.

2005 Technological Enhancement

For the first time, the Assessment Tool was offered as a Web-based form. It was accessed, completed, and analyzed electronically. This option created greater convenience in the completion and summarization of the results. Hard copies of the assessment were provided to program areas without Internet access. Results from these hard copies were entered for analysis using the Web-based form.

Assessment Categories

The Safeguard Assessment Tool examined seven arenas in which confidential information assets could be protected:

- A. Physical Environment B. Reception and Pedestrian Traffic
- C. Workstations, Printers, Copiers, Fax Machines D. Electronic Media Storage
- E. Document Storage F. Document Destruction G. Administrative Procedures

2004 Remediation Accomplished

The Office of Information Security coordinated efforts to address some of the safeguard issues identified in 2004 with a long-term, systemic approach.

- Policies were written and implemented to address disposal of confidential information, secure email, access control, and reporting privacy and security incidents.
- Data Use Agreements were revised and implemented for both internal and external users of DHS information assets.
- Privacy and security reminders and guidance are provided to all DHS staff through the bi-monthly Privacy/Security Update newsletter. Other all-staff messages or action requests are distributed as needed to address particular incidents or issues.

One issue identified in 2004, and as yet not fully resolved, was confidentiality clauses in janitorial service contracts. DHS program staff and managers often do not have any knowledge of who administers the janitorial contract or of what is written into the contract. Janitorial service contracts are executed in more than one way. When the contract is initiated and administered by the Department of Administrative Services (DAS), it includes clauses requiring high levels of confidentiality. By contrast, some janitorial contracts are initiated and administered by building owners, from whom DHS leases office space. It is at this juncture that program staff is unable to address the safeguard about signed confidentiality agreements with janitorial staff. This issue is not completely resolved at an administrative level at this time.

2005 Results

- There were 198 completed assessments returned, compared to 169 in 2004 and 145 in 2003. Managers provided contacts in all work areas under their responsibility that were responsible for completing the assessment. The higher return numbers may indicate that there is greater awareness of the assessment. And, perhaps, the yearly improvement of the distribution and process methodologies each contributed to the enhanced return rate.
- The “Not Applicable” option was selected 7.5% of the time.
- There were 2.4% of the safeguards not answered on the assessments. The likely explanation for this is human error.
- Ninety-nine percent of the safeguards were met in 2005, as compared to 97.43% in 2004. Assessment results are based on self-reports, not on external audits.
- Overall, the results of the assessment show reasonable safeguards were applied in the majority of settings.

(Summary responses to the individual safeguard are represented on [bar graphs](#).)

Assessment Factors	% of Safeguards Met*	Examples of Remediation Plans for Standards Not Met
A. Physical Environment	98.4%	<ul style="list-style-type: none"> › Close off reception area; working with facilities to implement › Order locking file cabinets › Reconfigure reception workstation to prevent casual view of computer screen › Implement re-keying some doors and/or adding key pads › Make better use of interview rooms
B. Reception and Pedestrian Traffic	98.9%	<ul style="list-style-type: none"> › Have janitor sign confidentiality agreement › Enforce policy to have visitors sign in at reception › Reception desk procedure has been updated and visitor procedure reviewed with reception staff
C. Workstations, Printers, Copiers, Fax Machines	99.7%	<ul style="list-style-type: none"> › Purchase and install view-limiting screens › Local Area Technical to ensure that all computers are set to automatically lock when not in use › Present staff reminder to pick up confidential material from fax or printer immediately
D. Electronic Media Storage	98.8%	<ul style="list-style-type: none"> › Will implement new policy and new access form coming from central office › Add quarterly calendar reminder to review staff

		access privileges
E. Document Storage	99.4%	<ul style="list-style-type: none"> › Will have locks installed in the closed file cabinets by the unlocked back door › Remind staff to cover or file documents when leaving the office
F. Document Destruction	99.5%	<ul style="list-style-type: none"> › Purchase lids for barrels containing confidential material › Label bins containing confidential material
G. Administrative Procedures	98.5%	<ul style="list-style-type: none"> › Schedule semi-annual review of confidentiality stuff › Implement the new access control/IUP process (Individual User Profile) › Request and review reports on who has access to client serve files › Use interview rooms for client conversations; remind community partners

**The percentage of Safeguards Met was calculated by subtracting the percentage of unmet safeguards from 100%. Two other figures (i.e., Not Applicable and Not Answered) are documented on the [bar graphs](#) and other raw data. Consequently, the percentage of Safeguards Met noted in the survey data differs from the final calculation reported above.*

Issues Raised

Programs identified two areas of concern that exist outside of their ability to fully remediate. Both concerns were identified during the 2004 assessment as well.

- A lack of auditory privacy in some offices. Most offices took some steps to address this by staggering appointments for adjoining cubicles, putting up room divider screens, and coordinating the use of interview rooms.
- Cubicle configuration that allows site access to computer screens. Facilities management limitations impact the opportunity to remediate this safeguard completely. View-limiting screens can be put in place, as can “rear view mirrors” attached to computer monitors.

The HIPAA Privacy Rule does not require that solid walls be constructed between interview stations or that all conversation happen within the confines of a closed room. The Rule requires that we apply reasonable safeguards to keep information confidential within the existing environment.

Conclusion

Department of Human Services program and work areas self-reported that reasonable safeguards for information assets are being met at a rate of 99%. Meeting a safeguard at least 75% of the time is considered compliant. Remediation plans for unmet safeguards are documented and will be tracked for completion. The Safeguard Assessment will be administered again in 2006.