



Overall

LIPIX hired Cyber Trust/Verizon (a top security firm) to perform a HIPAA and Security Assessment to validate LIPIX's Policies, Procedures and Technologies are in line with HIPAA and the protection of patient data. The below are the responses to each of Cyber Trust's findings. It should be noted that the over all assessment was very positive. The findings requiring mediation were all addressed immediately after receiving the Assessment.

HIPAA Assessment Results

There were 3 areas that needed attention-

- 1) Disaster Planning - It was agreed that CSC has a great DR plan and LIPIX will work with CSC to create a test schedule. The Policy notes backup testing once a quarter and a DR Site test annually.
- 2) Physical Security - Office Area Access - The Office building in which LIPIX resides has limited physical security. The security guards procedures for allowing entry to visitors are inconsistent. Even though NO PHI is stored at the LIPIX offices, there is access to the LIPIX workstations. A new closed door policy was implemented until a card reader can be installed at the front door. All offices are closed when not in use and the front door is closed at all times now.
- 3) Physical Security - Workstation Security. Even though LIPIX has a very strong remote access policy and technology, access to the physical workstation is still required to be restricted. See #2.

Security Assessment Results

There were 4 results, none posed a threat to PHI. They were all addressed immediately after the audit results were published.

- 1) /cgi-bin/w3-msql was found on one of the web servers in the Stage environment. This file could be exploited and cause buffer overflowing. The file was removed, all other web servers were searched and the file was not found. Any future server created this file will be removed if present.
- 2) One of the local LIPIX workstation had an older version of Dameware on it. This could cause a buffer overflow. The Dameware application was removed. LIPIX does not support the use of this remote control tool.
- 3) Unsecured Cookies were noted - this could be an issue if connections to LIPIX were not secure. LIPIX requires a secure connection (https:) to access the applications. This minor issue was noted and will be addressed in the next release of Healthshare (12/08) to avoid any issues in the future.
- 4) Web Sever Certificate was ready to expire on SSL Extender (11/14/08) - This is the CSC managed remote access media used by LIPIX administrators to gain access to the secure network. The certificate was renewed on 11/01/08 as scheduled by CSC.

Other Minor Findings-

- 1) 164.306a Security Notification - LIPIX will start to send out "reminder" emails to staff on the importance of Patient Data Security.
- 2) 164.308- Security Training. - LIPIX will conduct annual refresher training classes on treatment of PHI.

For any further questions, please contact Mark E. Grecker, Chief Technology/Security Officer, LIPIX. (516) 428-8246 mgrecker@nshs.edu