



Security Solutions powered by Cybertrust

LIPIX

HIPAA Security Assessment

Report

CONFIDENTIAL AND PROPRIETARY

Prepared by: Verizon Business

October 22, 2008

Executive Summary

LIPIX (“LIPIX”) contracted with Verizon Business to perform an assessment of their security posture against the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandate. LIPIX sought an independent, third-party evaluation of its security program and the identification of program compliance gaps. This assessment was designed to be completed in a period of two weeks. As such, Verizon Business focused this assessment on only performing interviews, some testing, and reviewing prepared policies; therefore, not every aspect of a typical HIPAA audit was included. This assessment does identify key strengths, as well as gaps in compliance, and will help LIPIX prepare for additional reviews.

Verizon Business’ efforts consisted of assessing LIPIX’s security program based on series of interviews with key personnel and a review of documentation provided against the standards and implementation specifications, collectively known as safeguards, in the HIPAA Security Final Rule. Where the meaning or intent of the Final Rule’s safeguards were unclear or vague, Verizon Business referred to the ISO 27001 standard for industry best practice guidance. By consulting the ISO standard in this way, Verizon Business was better able to consider the reasonableness of LIPIX’s program in light of information security norms. The resulting Assessment Report documents current shortcomings in LIPIX’s program with respect to the HIPAA Safeguards and provides recommendations for achieving compliance goals that are in line with current best practices.

Verizon Business produced this HIPAA Assessment Report to document findings regarding the comprehensiveness of LIPIX’s security program. LIPIX intends to use these findings as a guide for enhancing safeguards to protect against reasonably anticipated threats to the security of and access to its proprietary environment and electronic protected health information (ePHI) as required by the HIPAA Security Standards. Verizon Business recommends that LIPIX address the findings in this report as soon as practicable.

Verizon Business’ approach to this evaluation consisted of assessing documentation evidence of compliance to assess LIPIX’s overall ePHI protection posture from various parts of the organization such as human resources, legal, and physical security. Evidence was provided through interviews, documented policies, documented business processes, legal agreements, etc.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

Key Observations:

Verizon Business evaluated LIPIX's HIPAA Security compliance program against the 47 standards and implementation specifications ("safeguards") contained in the HIPAA Security Final Rule. Summarized results are as follows:

- Evidence of compliance has been found for 43 safeguards;
- Additional key improvements are recommended for four safeguards.

Program Strengths:

Verizon Business found the LIPIX overall security program and the use of CSC for hosting and monitoring to be well managed and generally consistent with industry best practices.

CSC provides strong Physical and Logical security controls over networks and systems that comprise the LIPIX staging and production environments.

LIPIX authentication and authorization controls to access production and staging environments are strong at the network and application layers.

Provisioned servers are security tested by CSC prior to deployment and Internet-facing systems are security tested monthly by CSC as part of the services agreement.

Intrusion detection and incident response processes provided by CSC provide real time monitoring over LIPIX network assets and data.

Key Areas requiring improvement for "Required" Safeguards:

- Workstation Security

Security controls are weak to prevent access to LIPIX offices and computers that could potentially connect to the Access Gateway (AG) and ePHI.

Key Areas requiring improvement for "Addressable" Safeguards:

- Facility Access

LIPIX physical security controls at the Northern Blvd offices do not prevent intruders from entering office spaces with connectivity to LIPIX networks and data.

- Business Continuity

The Business Continuity/Disaster Recovery process is not jointly tested with CSC to ensure it can maintain business processes; nor can it be modified to meet new requirements without proper testing to discover weaknesses

The body of the report contains a description of each finding and a corrective action and recommendation. Verizon Business expects that LIPIX will continue to address compliance in its environment.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

TABLE OF CONTENTS

INTRODUCTION	1
HIPAA Final Security Rule	1
Scope of Assessment	2
Verizon Business Methodology	2
Participants	4
Report Organization	4
OVERALL FINDINGS	5
Summary of Key Findings	6
Program Strengths.....	6
Program Findings.....	6
HIPAA Security Assessment	7
RECOMMENDATIONS	20
HIPAA Security Final Rule Recommended Activities	22
1) Address Risk – Contingency Plans § 164.308(a)(7)(i): Testing and Revision Procedure.....	22
2) Address Risk – Physical Safeguards § 164.310: Facility Access Controls.....	23
3) Address Risk – Workstation Security § 164.310(c).....	24
Access Control and Validation.....	24
CLOSING REMARKS	25

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Section 2

Introduction

LIPIX is a small, but dynamic organization that is focused on delivery of a healthcare-based solution that allows physicians to more effectively treat their patients through medical history data aggregation and viewing via a secured information portal. Because LIPIX processes and transmits Electronic Protected Health Information (ePHI) to which the HIPAA Security Rule is addressed, they are considered a covered entity and must show compliance with HIPAA. A significant part of this [showing] is assessing the "... risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information..." Also required is "Risk Management ... sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." (HIPAA Section 164.308(a)(1)(ii)(A & B)).

LIPIX contracted with Verizon Business to complete a review of its security program in an effort to identify the potential compliance gaps with the Final Rule's standards and implementation specifications. This assessment should not be construed as a comprehensive HIPAA audit; as not every aspect of a HIPAA audit was included. This assessment does identify key strengths, as well as gaps in compliance, and will help LIPIX prepare for a full audit in the future.

HIPAA Final Security Rule

HIPAA (the "Act") was signed into law in 1996 (Public Law 104-191). Title II (Fraud, Simplification, and Abuse) of the Act contains the Administrative Simplification provisions with which Covered Entities (CEs) must comply in order to facilitate the exchange of electronic Protected Health Information (PHI) and to ensure the security and confidentiality of consumer information. The Act asserts that CEs that collect, store, and/or process PHI in electronic form must make a good faith effort to protect the corporate computing environment from reasonably anticipated threats and vulnerabilities, and take reasonable and appropriate measures to protect the integrity, confidentiality, and security of such electronic data. The security protections selected may be examined in the event that the CE and its associated business partners and service providers are the subjects of a compliance audit.

The HIPAA Security Final Rule that implements the Act requires CEs to perform an analysis of the potential risks to the electronic PHI for which they are responsible, and

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. Security plans must fully document the security measures implemented by the organization and should reflect the management of risk to acceptable levels. Periodic evaluation of the risks to the corporate computing environment and ePHI is also a requirement. Security plan updates because of these periodic evaluations are expected.

The HIPAA Security Final Rule is a regulatory framework that incorporates recognized security objectives and protections, but which is technology neutral. The Final Rule provides standards and in some cases, implementation specifications, that require CEs to implement predetermined controls. To achieve a baseline level of compliance, a covered entity like LIPIX must have a comprehensive security program. The scope and nature of each covered entity's security program will vary according to its proprietary environment and associated vulnerabilities as determined through risk analysis processes. Although the standard is objective, a covered entity's specific security controls may vary, as the Final Rule permits flexibility in approach to compliance. The Final Rule permits CEs to select "reasonable and appropriate" control measures according to level of risk and potential tolerance within the environment. For example, CEs can achieve compliance with authentication requirements by using strong passwords or through biometric technology. The choice to implement one authentication tool over another should typically be based on the likelihood that a security breach will occur and the potential damage that could result from such a breach.

Scope of Assessment

As agreed in the statement of work, the deliverables are a HIPAA Security Rule Assessment Report that includes:

- Verizon Business will prepare a Report of Findings that documents the results of our controls assessment.

This evaluation primarily targeted information technology resources of LIPIX. Verizon Business investigated controls and compliance efforts in other parts of the organization to determine whether all parts of the organization follow a common set of policies and procedures.

Verizon Business Methodology

Verizon Business used an evaluation methodology based on a strictly construed interpretation of the Final Rule, supplemented by industry best practice criteria. Our

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

criteria identified a few areas related to the administrative, physical and technical safeguards required by HIPAA that are in need of enhancement.

Verizon Business's testing and analysis included the following steps:

- Identifying the platforms, applications and data stores of ePHI; Business information flow documentation was also solicited
- Identifying employees who have access to ePHI
- Collecting and reviewing existing policies and SOPs that apply to Human Resources; Legal, IT Security; Physical Security; Business Continuity; Disaster Recovery; and Change Control Management;
- Collect and review existing network diagrams; network device configurations and application architectural documents
- Identifying employees who have remote access to LIPIX's information systems
- Reviewing existing Business Associate Contracts
- Performing a risk analysis that includes both internal and external vulnerability assessments including information systems identified as containing or potentially containing ePHI
- Documenting any differences between LIPIX's existing administrative, physical and technical measures and the Security Rule standards
- Documenting potential impacts the gaps present to LIPIX
- Recommending control measures to mitigate risk to ePHI, when it is identified

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Participants

Verizon Business met with the following individuals on the dates indicated in the table:

DATE	PERSONS	SUBJECT
10/13	Mark Greaker - CTO	Overall review of Information Security Program, Onsite Agenda, Documentation collection, Testing Parameters and scheduling
10/14	Mark Greaker – CTO	Incident Response, Account Administration, Intrusion Detection, Security Testing, Firewalls, Human Resources
10/14	John LoSchiavo – Director of Infrastructure	Physical Security, Systems Operations, Backups, Media Handling, AntiVirus, Email Administration, Desktop Engineering, Server Engineering
10/14	James Heiman – Project Manager Raman Vig – Project Manager/Developer	Development, Databases, Change Control
10/15	Mark Greaker – CTO	Internal Audit, Network Engineering
10/15	Ben Stein, MD – CEO	Leadership, Application Architecture
10/16	Jeremy Derby – InterSystems Developer/Project Manager	LIPIX Application temporary data storage

Report Organization

Organization of the remainder of the report is as follows:

Section 3 – Overall Findings: documents the HIPAA Security Assessment findings; the basis for the findings; the ePHI impact potential; and recommends for improving ePHI protection.

Section 4 – Recommendations: provides a detailed explanation of tasks LIPIX may undertake to achieve compliance.

Section 5 – Closing Remarks: Summarizes the overall evaluation process

Appendix – Vulnerability Testing: Verizon Business security testing results

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Section
3

Overall Findings

This section covers Verizon Business' HIPAA Security Rule Assessment findings. The Assessment report focuses on areas for improvement in organizational, administrative, procedural, and higher-level technical architecture controls, but observations of program strengths are also included to provide context and balance where applicable.

The HIPAA Security Rule Assessment table below presents the compliance assessment results for each requirement. The table also provides summarized evidence (and/or evidence references) for each statement to convey how compliance was determined. A discussion of the finding's impact on ePHI security accompanies each statement when applicable. Brief recommendations are also included and follow one-for-one from the findings. The recommendations focus on two areas: new initiatives required to eliminate compliance gaps, and extension of existing initiatives that would mitigate risk beyond a baseline level. Section 4 presents these recommendations in additional detail.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Summary of Key Findings

Verizon Business evaluated LIPIX's HIPAA Security Program for compliance against the 47 safeguards (standards and implementation specifications) contained in the HIPAA Security Final Rule. Summarized results are as follows:

- There was sufficient evidence of compliance for 43 safeguards;
- Additional key improvements could be made for four safeguards.

Verizon Business approach to this evaluation consisted of conducting interviews and assessing documented evidence of compliance to assess LIPIX's overall ePHI protection posture from various parts of the organization. Evidence was provided through interviews, documented policies and processes, legal agreements, and technical testing.

Program Strengths

- Verizon Business found the LIPIX overall security program and the use of CSC for hosting and monitoring to be well managed and generally consistent with industry best practices
- CSC provides strong data center Physical and Logical security controls over networks and systems that comprise the LIPIX staging and production environments
- LIPIX authentication and authorization controls to access production and staging environments are strong at the network and application layers
- Provisioned servers are security tested by CSC prior to deployment and Internet-facing systems are security tested monthly by CSC as part of the services agreement
- Intrusion detection and incident response processes provided by CSC provide real time monitoring over LIPIX network assets and data

Program Findings

Key improvements are recommended with regard to one “**Required**” safeguard:

- Workstation Security

Key improvements are recommended with regard to three “**Addressable**” safeguards:

- Business Continuity
- Facility Access (2)

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

HIPAA Security Assessment

The following table summarizes the result of the HIPAA Security Final Rule Assessment. The table below contains Verizon Business' "Yes/No" statements regarding documented evidence of compliance supplied, together with specific finding statements. A "Yes" statement means that LIPIX provided sufficient evidence to meet baseline control objectives in line with the Final Rule. A "No" statement means that the evidence presented by LIPIX could be improved to meet control objectives and that recommended actions are indicated. The table also presents anticipated impacts to ePHI and summarizes other corrective action recommendations. Section 4 presents the corrective action recommendations in additional detail.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
Security standards: General rules § 164.306			
1. General requirements- § 164.306(a)		Defined in the rule as:	“Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.”
(Required)	Yes Observation: LIPIX has taken material measures to ensure the confidentiality, integrity and availability of ePHI handled by the LIPIX application. LIPIX has put controls in place to ensure that ePHI is not stored/accessible to employees or non-authorized users on their networks.	Ensure that business processes and information systems that handle (or potentially handle) ePHI are reasonably and appropriately safeguarded and documented.	RECOMMENDATION: Verizon Business recommends that LIPIX continue to perform periodic security risk assessment to addresses any changes in workflows, infrastructure or applications.
Administrative Safeguards § 164.308			
1. Security Management Process - § 164.308(a)(1)(i)		Defined in the rule as:	“Implement policies and procedures to prevent, detect, contain, and correct security violations.”
Risk Analysis (Required)	Yes Observation: LIPIX has an active compliance program with an annual training requirement that is supported by policies and disciplinary processes that appear to be responsive to employee/contractor/consultant security violations. The initial training is conducted upon hire and is updated annually for each employee.	Ensure that business processes and information systems that handle (or potentially handle) ePHI are reasonably and appropriately safeguarded and documented.	RECOMMENDATION: Verizon Business recommends that LIPIX expand the compliance-training program to include follow-on testing to better demonstrate user understanding of ePHI safeguards.
Risk Management (Required)	Yes Observations: LIPIX is continuing efforts to maintain a high level of compliance through a methodical method of technical and process based control framework.	Ensure that business processes and information systems that handle (or potentially handle) ePHI are reasonably and appropriately safeguarded and documented.	RECOMMEDATION: Verizon Business further recommends the expansion and further definition of the risk management process at LIPIX once the stakeholders in the Technical Committee are identified to ensure that all stakeholders have inputs and that risk acceptance/avoidance decisions are taken at the appropriate level, with full understanding of the implications of

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
			these decisions.
Sanction Policy (Required)	Yes Observations: LIPIX presented documentation evidence of a well-established disciplinary policy with well-defined sanctions for violations. Due to the size of the organization and length of existence, there were no documented cases of the sanctions having been applied.	This policy defines the sanctions available to management for enforcement of security policy and procedure compliance.	RECOMMEDATION: No recommendation in this area.
Information System Activity Review (Required)	Yes Observations: LIPIX presented documented evidence in the form of screen display samples and architectural drawings that show that ePHI is only accessible on the AG by authorized users temporarily once retrieved from organizations that own the ePHI data. Access to this temporary data is logged to application transaction, database, and server logs. Activity reports are provided by CSC and reviewed by LIPIX management.	Both the Privacy and Security Rules require monitoring of PHI access. For LIPIX, this activity is applicable only to the AG (Access Gateway) server. Both technical and procedural controls are necessary.	RECOMMENDATION: No recommendations in this area.
2. Assigned Security Responsibility - § 164.308(a)(2)		Defined in the rule as:	“Identify the security official who is responsible for the development and implementation of the policies and procedures required by this sub-part for the entity.”
Assign a Security Official (Required)	Yes Observations: the current LIPIX CTO is taking responsibility for Information Security.		RECOMMENDATION: No Recommendation in this area.
3. Workforce Security - § 164.308(a)(3)(i)		Defined in the rule as:	“Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.”
Authorization and/or Supervision (Addressable)	Yes Observations: LIPIX presented documentation evidence of Authorization controls	Authorization and supervision of LIPIX workforce ensures compliance with “minimum necessary” access to ePHI.	RECOMMENDATION: No recommendation to this area.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
	that ensure compliance through proper supervision of the LIPIX workforce. There is no access to ePHI by LIPIX workforce personnel.		
Workforce Clearance Procedure (Addressable)	Yes Observations: LIPIX presented documentation evidence of a well-established workforce clearance procedure using a 3 rd party contractor called First Advantage. However, in the case of access to ePHI data – no LIPIX workforce members have access to ePHI data.	Such procedures determine that the access of a workforce member to electronic protected health information is appropriate.	RECOMMENDATION: No Recommendation in this area.
Termination Procedures (Addressable)	Yes Observations: LIPIX presented documentation evidence of a well-established sanction policy. CTO notifies system administrator for account disabling in the case of an employee who voluntarily or involuntarily leaves LIPIX.	Provides for termination of access to PHI when the employment of a LIPIX workforce member ends or is no longer required for a particular role.	RECOMMENDATION: No recommendation in this area.
4. Information Access Management - § 164.308(a)(4)(i)		Defined in the rule as:	“Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of sub-part E of this part.”
Isolating Healthcare Clearinghouse Functions (Required)	N/A Observations: Not Applicable to LIPIX		RECOMMENDATION: No recommendation in this area.
Access Authorization (Addressable)	Yes Observations: LIPIX presented documented evidence of a well-established access authentication and authorization policy that control employees’ rights and privileges at the network, system and application levels. These rights and privileges are audited on a monthly basis by LIPIX administrators. None of the LIPIX employees will have direct access to ePHI through systems or applications.	Ensures appropriate access to electronic protected health information via policies and procedures	RECOMMENDATION: No recommendation in this area.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
Access Establishment and Modification (Addressable)	Yes Observations: See "Access Authorization.	Ensures appropriate access to electronic protected health information via policies and procedures.	RECOMMENDATION: See "Access Authorization"
5. Security Awareness and Training- § 164.308(a)(5)(i) Defined in the rule as: "Implement a security awareness and training program for all members of its workforce (including management)."			
Security Reminders (Addressable)	Yes Observations: LIPIX presented documentation evidence of pre-employment training an annual HIPAA compliance-training program sponsored by North Shore Long Island Jewish Health System. (North Shore LIJ).	Ensuring organizational awareness of privacy and security policies and practices is a requirement of the HIPAA regulations. LIPIX workforce members are the foundation of ensuring compliance and should receive training so that they know and understand expectation regarding ePHI protection. An untrained LIPIX workforce member could unwittingly participate in activities that could put LIPIX at risk.	RECOMMENDATION: Verizon Business recommends that LIPIX provide security reminders in the form of emails, posters, and intercompany memos that specifically address risk to ePHI.
Protection from Malicious Software (Addressable)	Yes LIPIX presented documentation evidence of employee training in regards to malicious software. At this point, all LIPIX employees have demonstrated knowledge of malicious software and ways to guard against it.	Employees should be trained to guard against, detect and report malicious software on systems that support ePHI.	RECOMMEDATION: See "Security Reminders" above
Log-In Monitoring (Addressable)	Yes LIPIX presented documentation evidence of Log-In Monitoring activities.	Employees should be trained to monitor login attempts and report discrepancies on systems that support ePHI.	RECOMMEDATION: See "Security Reminders"
Password Management (Addressable)	Yes LIPIX presented documentation evidence of password management policies. Employees demonstrated knowledge of and will to comply with these policies.	Employees should be trained in procedures to create, change and safeguard passwords for systems that support ePHI.	RECOMMEDATION: See "Security Reminders"
6. Security Incident Procedures- § 164.308(a)(6)(i) Defined in the rule as: "Implement policies and procedures to address security incidents."			
Response and Reporting (Required)	Yes Observations: LIPIX presented evidence of response and reporting policies in	Must be able to identify and respond to suspected or known security incidents	RECOMMENDATION: No recommendations in this area.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
	conjunction with their hosting provider – CSC. These responses are tied directly to CSC Security Operations monitoring and notification policy in the services agreement.	that pose a threat to systems that support PHI; mitigate effects and document their outcomes.	
7. Contingency Plans - § 164.308(a)(7)(i)		Defined in the rule as:	“Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.”
Data Backup Plan (Required)	Yes Observations: LIPIX presented documentation evidence of a data backup plan that outlines CSC’s hosted solution that involves Legato tape backups.	Ensures that retrievable exact copies of electronic protected health information are both created and maintained.	RECOMMENDATION: No recommendations for this area.
Disaster Recovery Plan (Required)	Yes Observations: LIPIX presented documentation evidence of a DRP process and facility managed by hosting provider CSC. Documentation specifies notification requirements and critical vendor contacts in detail but does not describe in detail the restoration steps for systems and components.	Establishes procedures to restore any loss of data, including ePHI.	RECOMMEDATION: Verizon Business recommends that Disaster Recovery documentation be modified to include greater detail on restoration steps, rather than high-level descriptions. Testing of Disaster Recovery in conjunction with provider CSC should be performed at least annually.
Emergency Mode Operation Plan (Required)	Yes Observations: LIPIX presented documentation evidence that hosting provider CSC performs data recovery and Business Continuity actions in the event of an emergency via their hot backup site in Chantilly, VA.	Establishes procedures to restore the systems required to protect the security of protected health information during emergency operations	RECOMMEDATION: No recommendation for this area.
Testing and Revision Procedure (Addressable)	No. Observations: LIPIX contract agreements with CSC establish the requirement for CSC to provide Business Continuity. However, no evidence supported that LIPIX and CSC performs any	Establishes procedures to enable the continuation of critical business processes for the protection and security of electronic protected health information while operating in emergency mode	RECOMMEDATION: Verizon Business recommends that testing of the Business Continuity/Disaster Recovery processes be tested at least annually to ensure processes recover systems and data adequately. Ensure that backup tapes are also tested at least quarterly to ensure

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
	periodic testing of the plan.		they are readable and recoverable.
Applications and Data Criticality Analysis (Addressable)	Yes LIPIX presented documentation evidence that Applications and Data Criticality is addressed as part of their hosting agreement with CSC to ensure this data and systems are secured and backed up regularly.	Assess the relative criticality of specific PHI applications and data in support of contingency plans.	RECOMMEDATION: No recommendations for this area.
8. Evaluation - § 164.308(a)(8)		Defined in the rule as:	“Perform a periodic technical and non-technical evaluation, based initially on the standards implemented under the rule, and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity’s security policies and procedures meet the requirements of this sub-part.”
Security Evaluation	Yes Observation: LIPIX enterprise quarterly Security scanning will be done by Verizon Business/Cybertrust. LIPIX selected Verizon Business to provide a third party HIPAA assessment to include External, Internal, and Application Vulnerability testing. CSC performs monthly External Vulnerability tests and testing of: - newly provisioned hosts - to satisfy internal/external audit requests	Periodically review the adequacy of the security program.	RECOMMENDATION: Verizon Business recommends that LIPIX periodically assess the effectiveness of employee security awareness training activities, and that LIPIX expand such activities to form a more substantial portion of the annual compliance testing.
9. Business Associate Contracts and Other Arrangements - § 164.308(b)(1)		Defined in the rule as:	“A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314 (a), that the business associate will appropriately safeguard the information...A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314 (a).”
Written Contract or Other Arrangement (Required)	Yes Observations: LIPIX’s BA contracts were provided that provide strong language concerning ePHI security,	Protects the communication and handling of ePHI between LIPIX and its Business Associates.	RECOMMEDATION: Verizon Business recommends that LIPIX consider adding specific administrative and technical security control requirements into BA agreements.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
	transmission, and storage by Business Associates.		
Physical Safeguards § 164.310			
I. Facility Access Controls - § 164.310(a)(1)		Defined in the rule as:	“Implement policies and procedures to limit physical access to its electronic systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”
Contingency Operations (Addressable)	Yes Observations: LIPIX and CSC address contingency operations through contract for a hot site CSC data center located in Chantilly, VA. This site will be able to provide instant transfer of operations that will not affect customer access or data.	Allow facility access in support restoration of lost data under LIPIX’s Disaster Recovery Policy.	RECOMMENDATIONS: RECOMMENDATION: No recommendations in this area.
Facility Security Plan (Addressable)	No Observations: The LIPIX office door is left open (unlocked/unmonitored) during business hours. The North Shore Physical Security guard at the front door periodically leaves the Security Desk unmanned and does not consistently ask guests to sign in. In regards to CSC Hosting Facility security safeguards, they are a secure hosting facility and though review of their current SAS70 Type II (dated Nov 2007), the physical security controls within that facility are strong.	Safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	RECOMMENDATION: Verizon Business recommends that LIPIX implement card access technology to secure office entry, and to locate a receptionist in the front area of the office to screen and authorize visitor access. Implement a visitor’s badge system for authorized visitors to identify them as authorized personnel while in the workspaces.
Access Control and Validation (Addressable)	No Observations: See “Facility Security Plan” entry.	Controls a person’s physical access to LIPIX’s facilities and software programs based on role or function (including visitors)	RECOMMENDATION: Verizon Business recommends that card access technology and a person inside the front door of the LIPIX office be used to screen visitors and secure the workspace to mitigate poor building access controls. Visitors should wear temporary visitor badges that identify them.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
Maintenance Records (Addressable)	Yes Observations: CSC hosting center performs security infrastructure repairs, maintenance, changes and replacement and are documented according to standard operating procedures.	Documents repairs and modifications to the physical components of LIPIX facilities related to security.	RECOMMENDATION: No recommendations
2. Workstation Use - § 164.310(b)		Defined in the rule as:	“Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.”
Workstation Use (Required)	Yes Observations: Appropriate combinations of procedural, technical, and physical safeguards were observed for workstations at the LIPIX facility. Security testing of these systems was performed that resulted in no significant security vulnerabilities.	Minimizes the possibility of unauthorized access to information due to the location or use of equipment.	RECOMMENDATIONS: No recommendation for this area.
3. Workstation Security - § 164.310(c)		Defined in the rule as:	“Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”
Workstation Security (Required)	No General facility security represents the only physical access control to workstation(s) that can (potentially) access ePHI on the AG. The LIPIX office door is left open (unlocked/unmonitored) during business hours that could potentially allow unauthorized personnel access to workstations.	LIPIX physical safeguards should be based on perceived risks of unauthorized access to workstations that (potentially) contain ePHI.	RECOMMENDATIONS: Verizon Business recommends that LIPIX develop an explicit policy that states physical protections must secure workstations that (potentially) contain or have access to ePHI via the AG. Controls such as employee electronic card access systems and front door visitor screening should be implemented that restrict access to office workspaces. Verizon Business recommends that LIPIX explicitly address workstation security in all future risk assessments.
4. Device and Media Controls -		Defined in the rule as:	“Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
§ 164.310(d)(1) facility.”			
Disposal (Required)	Yes Observations: Current LIPIX policy and practices address electronic and paper media disposal. Note that there is no ePHI stored at LIPIX so this control pertains to applications, architecture information, and proprietary data but not ePHI.	Addresses the final disposition of ePHI and/or the hardware or electronic media on which it is stored.	RECOMMENDATION: No recommendation for this area.
Media Reuse (Required)	Yes Observations: LIPIX policies were observed to address media re-use.	Entity must ensure that its protected health information is removed from electronic media before media are made available for reuse.	RECOMMENDATION: No recommendation for this area.
Accountability (Addressable)	Yes Observations: LIPIX documentation addresses accountability.		RECOMMENDATIONS: No recommendation for this area.
Data Backup and Storage (Addressable)	Yes Observations: LIPIX documentation addresses data backup and storage. Backups are performed by CSC and stored onsite and offsite securely.		RECOMMENDATION: No recommendation for this area.
Technical Safeguards § 164.312			
1. Access Control - §	Defined in the rule as:	“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to those	

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
164.312(a)(2)			
persons or software programs that have been granted access rights as specified in § 164.308 (a) (4)."			
Unique User Identification (Required)	Yes Observations: Verizon Business reviewed user lists during this assessment and noted that all users' actions are traceable. Interviews were consistent in exhibiting an organization-wide practice prohibiting shared logins.	Assigns a uniquely traceable user identifier.	RECOMMENDATION: No recommendation for this area.
Emergency Access Procedure (Required)	Yes Observations: LIPIX does not ordinarily store ePHI, so they have not implemented a specific process for accessing such information in an emergency.	Procedures for obtaining necessary electronic protected health information during an emergency.	RECOMMENDATION: No recommendation for this area.
Automatic-Log-Off (Addressable)	Yes Observations: Automatic session lock is set for 15 minutes, and addition layers of auto-logoff in certain ePHI-handling applications was also observed.	Electronic procedures that terminate an electronic session after a predetermined time of inactivity.	RECOMMENDATION: No recommendation for this area.
Encryption and Decryption (Addressable)	Yes Observations: Verizon noted documentation of full encryption for VPN access, SSH v2 for remote access to Unix and Terminal Services using SSH for Windows, Secure FTP for encrypted data transfer, and HTTPS for encrypted browser sessions.	Creates a cryptographic barrier to unauthorized ePHI access Access control achieved through cryptographic key management processes	RECOMMENDATION: No recommendation for this area.
2. Audit Controls - 164.312(b)	Defined in the rule as:	"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."	

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
Audit Mechanisms	Yes Observations: There is logging from security devices and applications, and formal procedures are used to provide proactive ongoing monitoring at the data center through CSC Security Teams.	Provides a record of information systems activity that can be periodically reviewed for unauthorized creation, modification, duplication, transmission or deletion of ePHI.	RECOMMENDATION: No recommendation for this area.
3. Integrity - 164.312(c)(1)		Defined in the rule as:	“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”
Mechanism to Authenticate Electronic PHI (Addressable)	Yes Observations: Built-in TCP/IP network controls validate the correctness of network packets.	Ensures that electronically transmitted ePHI is not improperly modified without detection	RECOMMENDATION: No Recommendation for this area.
4. Person or Entity Authentication		Defined in the rule as:	“Implement procedures to verify that a person seeking access to electronic protected health information is the one claimed.”
Person or Entity Authentication (Required)	Yes Observations: LIPIX documentation addresses Person/Entity Authentication for systems, networks and application level controls.	Validates identities for all entities, human or machine.	RECOMMENDATIONS: No Recommendation for this area.
5. Transmission Security - 164.312(e)(1)		Defined in the rule as:	“Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”
Integrity Controls (Addressable)	Yes Observations: Built-in TCP/IP network controls and transmission security controls ensure no unauthorized modification are done and validate the correctness of network packets.	Ensures that electronically transmitted ePHI is not improperly modified without detection.	RECOMMENDATION: No Recommendation for this area.
Encryption (Addressable)	Yes Observations:	Encrypts electronic protected health information whenever deemed	RECOMMENDATION:

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

HIPAA Security Rule Implementation Specification	HIPAA Security Final Rule Evidence of Compliance (Y/N) LIPIX Implemented Safeguards	Impact to LIPIX ePHI	HIPAA Security Final Rule - Recommended Action(s)
	Verizon noted documentation of full encryption for VPN access, SSH v2 for remote access to Unix and Terminal Services using SSH for Windows, Secure FTP for encrypted data transfer, and HTTPS for encrypted browser sessions.	appropriate.	No recommendation for this area.
Organizational Requirements § 160.314			
Business associate contracts and other arrangements (Required)	Yes Verizon reviewed contracts for Business Associates that ensure reasonable safeguards to protect ePHI are taken.	Ensures Business Associates implement reasonable and appropriate safeguards to protect ePHI.	RECOMMENDATION: No recommendation for this area.
Requirements for group health plans (Required)	Yes No health plan arrangements were cited for evaluation. Not applicable.	Ensures plan documents are amended to require the plan sponsor to implement reasonable and appropriate safeguards to protect ePHI.	RECOMMENDATION: No recommendation for this area.
Documentation Requirements § 164.316			
Policies and procedures (Required)	Yes LIPIX has a thorough set of General, Internal, and External IT and Security Policies that specify Enterprise and Application/Hosted architecture controls required to safeguard ePHI and systems that access it.	Implement reasonable and appropriate policies and procedures to comply with the standards.	RECOMMENDATION: No recommendation for this area.
Documentation (Required)	Yes Required LIPIX documents to include policies, architecture drawings, hardening documents and standards, contracts, etc. were available for review by Verizon Business while onsite.	Ensure that policies and procedures are documented and available for review.	RECOMMENDATION: No recommendation for this area.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Section

4

Recommendations

This section provides Verizon Business’s recommendations to LIPIX to address requirements of The Final Rule. The recommendations are organized according to the HIPAA Security Final Rule safeguards. Each of the sections is organized in the following manner:

- Type of HIPAA Security Final Rule safeguard
- Description of Actions – the standard or implementation specification
- High-level discussion of Verizon Business’s findings, including both strengths and weaknesses
- Detailed Recommendations, which are organized as follows:
 - Recommendation Number
 - Priority
 - Cost
 - Summary
 - Description

Cost and Priority were determined according to the following criteria:

Cost terminology	Effort required
Minimal	0 – 2 staff weeks
Moderate	2 staff weeks – 6 staff months
High	6 staff months – 2 staff years, or more

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Priority terminology	Description
High	Work on the activity immediately. Recommendations of this rank address identified high-risk exposures or significantly improve the security posture of LIPIX's infrastructure.
Medium	Work on the activity as soon as possible after implementing high priority recommendations. These activities address medium-risk exposures, improve the overall security posture, require minimal cost, or provide the foundation for other medium- and low-priority recommendations.
Low	Work on the activity as time and resources permit. Ensure that prerequisites, which may be medium- or high-priority efforts, have been addressed sufficiently to provide guidance in completing low-priority work.

HIPAA Security Final Rule Recommended Activities

Verizon Business developed the following recommended risk management activities after considering the results of the documentation assessment after considering the complexity of LIPIX’s environment and after discussion with LIPIX staff. Verizon Business bases its recommendations on its knowledge of essential security practices and industry best practices.

1) Address Risk – Contingency Plans § 164.308(a)(7)(i): Testing and Revision Procedure.	
Definition:	<p>§ 164.308(a)(7)(i)- “Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.”</p> <p><i>Testing and Revision Procedure</i> (Addressable). Establishes procedures to enable the continuation of critical business processes for the protection and security of electronic protected health information while operating in emergency mode.</p>
Strengths:	<ul style="list-style-type: none"> • LIPIX has a capable Business Continuity/Disaster Recovery capability in conjunction with their provider, CSC. • CSC includes disaster recovery testing for their common network architecture to their site in Chantilly VA.
Weaknesses:	<ul style="list-style-type: none"> • The Business Continuity and Disaster Recovery process is not tested jointly with CSC periodically to ensure it is capable of maintaining business processes. • The Business Continuity process cannot be effectively managed and modified to meet new requirements without proper testing to discover weaknesses.
REC001	Priority: HIGH
	Estimated Cost: Moderate
Summary:	<p>Verizon Business recommends that LIPIX address this issue through definition and implementation of annual physical testing of Business Continuity processes in concert with CSC. Ensure that critical data backup tapes are also tested at least quarterly to ensure they are readable and recoverable.</p>

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

2) Address Risk – Physical Safeguards § 164.310: Facility Access Controls	
Definition:	<p>§ 164.310(a)(1)- Facility Access Controls -“Implement policies and procedures to limit physical access to its electronic systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”</p> <p><i>Facility Security Plan (Addressable).</i> Safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</p> <p><i>Access Control and Validation (Addressable).</i> Controls a person’s physical access to LIPIX’s facilities and software programs based on role or function (including visitors).</p>
Strengths:	<ul style="list-style-type: none"> • LIPIX hosts the LIPIX application architecture (staging and production) at a physically secure and certified data center managed by CSC. • LIPIX personnel wear employee badges to identify authorized personnel while onsite at the Northern Blvd, Manhasset office.
Weaknesses:	<ul style="list-style-type: none"> • North Shore LIJ office building security personnel do not prevent intruder access to the building as the front desk is occasionally vacant. • The LIPIX external office door is left open with no receptionist to screen personnel entry into the office spaces. • Visitors in the LIPIX office space do not wear visitor badges that identify them as authorized visitors.
REC002	Priority: HIGH
Estimated Cost: Moderate	
Summary:	<p>Verizon Business recommends that LIPIX implement card access technology to secure office entry, and to locate a receptionist in the front area of the office to screen and authorize visitor access. Implement a visitor’s badge system for authorized visitors to identify them as authorized personnel while in the workspaces.</p>

3) Address Risk – Workstation Security § 164.310(c)	
Access Control and Validation	
Definition:	<p>“Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”</p> <p><i>Workstation Security (Required).</i> LIPIX physical safeguards should be based on perceived risks of unauthorized access to workstations that (potentially) contain ePHI.</p>
Strengths:	<ul style="list-style-type: none"> • The internal doors to offices containing systems are locked when employees leave for lunch or at the end of the workday. • Multiple layers of strong logical access controls are in place on workstations to prevent unauthorized entry or use. • No ePHI is stored on user workstations at LIPIX.
Weaknesses:	<ul style="list-style-type: none"> • The LIPIX main office door is open (unlocked/unmonitored) during business hours that could potentially allow unauthorized personnel access to workstations. • There are no physical locks or cables that prevent the workstations (laptops) from being removed from the LIPIX offices.
REC003	Priority: HIGH ESTIMATED COST: Moderate
Summary:	<p>Verizon Business recommends that LIPIX develop an explicit policy that states physical protections must secure workstations that (potentially) contain or have access to ePHI via the AG.</p> <p>Controls such as employee electronic card access systems and front door visitor screening should be implemented that restrict access to office workspaces.</p> <p>Security cables that physically prevent laptops from being removed should be installed.</p> <p>Verizon Business recommends that LIPIX explicitly address workstation security in all future risk assessments.</p>

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Section

5

Closing Remarks

The LIPIX organization has demonstrated its commitment to managing information security risks as an important business issue by undertaking this evaluation and by committing the resources necessary to strengthening its security program. Based on our evaluation of supplied documentation, interviews, and testing, Verizon Business believes that by following the recommendations herein, LIPIX can improve upon its program and establish a solid baseline of Risk Management and security controls.

Information security risk management has been and will continue to be an ongoing concern for LIPIX as it is for all similar organizations that include the use of ePHI within their business processes. Since the threat profile constantly changes, LIPIX must continually strive to increase its protective efforts against this changing landscape. New technologies, lapses in following procedures, standards, or guidelines, and the need to make greater amounts of data available to customers, partners, and regulators can provide an adversary with the opportunity to exploit new or existing vulnerabilities. Further, LIPIX recognizes its important role in protecting employee ePHI. Implementing a strong security posture is a constant process; LIPIX has indicated that it understands the need for continuous risk management improvement.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

APPENDIX – LIPIX Vulnerability Testing

Summary

Long Island Patient Information Exchange (LIPIX) engaged Verizon Business Security Solutions (Verizon Business) to conduct a combined vulnerability assessment during the course of the HIPAA Security review that consisted of:

- Application level security testing of the <https://staging.lipixportal.org> Web Application
- Vulnerability testing of nine staging servers and devices and six internal workstations

The security testing was conducted from Tuesday, October 14 until Friday, October 17, 2008 from LIPIX offices in Manhasset, NY and a Verizon Business office in Branford, Connecticut.

Verizon Business did not identify any high-risk findings that resulted in the successful exploitation of any systems or personnel during any phases of this assessment. The LIPIX environment has been hardened to an appropriately high level. However, it should be noted that Verizon Business did identify security issues that could result in information leaks and additional risk.

These findings are outlined in the Detailed Findings sections found later in this appendix.

Scope

The LIPIX organization provided the following assets to test that included various workstations, a web application, several servers and devices located within the LIPIX staging environment hosted by Computer Sciences Corporation (CSC). All IP addresses were provided by LIPIX prior to the initiation of testing. Verizon Business used an assortment of open source and commercial tools and applications to identify vulnerabilities using both automated and manual techniques.

Host IPs removed. LIPIX Restricted

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Combined Test Methodology

Tools Used

The following is a list of tools that were used during the course of Operating System testing:

- Nmap** – Open Source Port Scanner
- Nessus** – Open Source/Commercial Vulnerability Scanner
- Ethereal** – Open Source Network Packet Sniffer
- Look@LAN** – Open Source Network Scan Utility
- SNScan** – Open Source SNMP Discovery Utility

Network Discovery

Verizon Business was presented with the lists of hosts to test, so free form discovery using DNS or other outside sources was not performed.

Verizon Business attempted to determine all the active/open services on the IP addresses using the security tool NMAP. Versioning Nmap scanning options were further used to identify what versions of services were running on these open ports to ensure older and more vulnerable ones were not being used.

Through port scanning of these systems, Verizon Business determined that the number of open ports was kept to a minimum on all hosts tested. Of the staging systems that did have ports open to the internet, the only ports found open were HTTP and HTTPS. All other services were deactivated or closed per industry best practice.

Vulnerability Identification

With the information that was collected in the previous step, Verizon Business attempted to determine if any of these services are vulnerable to exploitation. Version strings and patch levels were compared with well-known vulnerabilities listings. Testing was also performed for several common configuration problems (web server hardening, ssl certificates, etc.).

Next, Verizon Business tested each responsive host using the vulnerability scanning tools Nessus, SNScan, Look@LAN, etc. to perform checks for known vulnerabilities. These tools perform extensive checks for vulnerabilities based upon predefined attack signatures. Results from these toolsets were then correlated to remove false positives when possible.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Application Testing Methodology

Tools Used

The following is a list of tools that were used during the course of the application testing:

HP WebInspect – Commercial Application Vulnerability Scanner

Paros – Open Source Web Proxy Utility

Firefox Extensions – AnEC Cookie Editor

Testing Process

The LIPIX Application testing was performed in multiple phases to include:

Black Box Testing from an unprivileged perspective from the Internet and inside the organization

White Box Testing from the perspective of an authenticated and privileged user from the Internet or inside the trusted network

Verizon Business performed White Box testing of the application using two provided test accounts (Cybertrust1 and Cybertrust2) to allow trusted access as both users. SessionIDs were collected during various attempts to use for Session Hijacking attacks that proved unsuccessful.

Verizon Business began with a thorough web crawl of the application from both Black Box and White Box perspectives to get a feel for the depth, size and complexity of the application and system involved. This web crawl was done using a browser and web application proxy and to determine the size for the LIPIX Portal application.

Verizon Business then performed both automated and manual-based testing from both Black Box and White Box perspectives to test for vulnerabilities within the application to include:

Parameter Tampering - Query strings, POST parameters, and hidden fields were modified in an attempt to gain unauthorized access to data or functionality.

Cookie Poisoning - Data sent in cookies was modified to test application response to receiving unexpected cookie values.

Session hijacking – Verizon Business attempted to take over a session established by another user to assume the privileges of that user.

Credential manipulation – Verizon Business modified identification and authorization credentials in an attempt to gain unauthorized access to other users' privileges.

Forceful Browsing - Web servers will send any file to a user, as long as the user knows the file name and the file is not protected. Therefore, a hacker may exploit this security hole, and "jump" directly to pages.

Backdoors and Debug Options - Many applications contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making it a target for potential exploitation. Application developers may leave backdoors in their code. These backdoors, if discovered, could potentially allow an intruder to gain additional level of access.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

LIPIX HIPAA Security Assessment

Configuration Subversion – Mis-configuring web servers and application servers is a very common mistake. The most common mis-configuration is one that permits directory browsing. Hackers can utilize this feature in order to browse the application's directories (such as cgi-bin/) by simply typing in the directory name.

Unhardened Server Deployment – This issue is common to many organizations that include leaving default directories, files, and web pages for attackers to discover. Discovery of these default items typically implies servers that have not been hardened properly, giving the attacker more attack channels and giving the impression that the web server is a soft target.

Input validation bypass - Client side validation routines and bounds checking are removed to ensure controls are implemented on the server.

SQL injection – Specially crafted SQL commands were submitted in input fields to validate input type controls.

Cross-site scripting (XSS) – Active content was submitted to the application in an attempt to cause a user's web browser to execute unauthorized code. This test validates user input type controls.

Once Verizon Business completed the testing, the consultant performed manual testing to confirm findings and rule out false positives, as raw data resulting from automated scanning systems typically reports findings that include these to a degree.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust

Security Assessment Findings Summary

Network Testing Summary

Verizon Business found the staging and internal systems to be well locked down in regards to the number of ports and services open to both the Internet and internal network users. This practice is commendable, as it limits attack vectors used by attackers that attempt to exploit these systems. Well done.

However, Verizon Business did identify one workstation with a dangerous CGI file on it that put this system at risk. This dangerous file should immediately be deleted from this system.

Another issue identified during testing included the same workstation that was running an older version of the Dameware Mini Remote control software that is exploitable via a buffer overflow attack. This software should be upgraded to the most recent version to mitigate this issue.

Application Testing Summary

Verizon Business discovered several lower level security issues within the LIPIX Portal application. However, these vulnerabilities do **not put ePHI data at risk**. Though these issues are not considered critical, they should still be remediated to provide additional application hardening and security.

Detail removed LIPIX Restricted.

CONFIDENTIAL AND PROPRIETARY



Security Solutions powered by Cybertrust