

**ELECTRONIC HEALTHCARE NETWORK  
ACCREDITATION COMMISSION  
(EHNAC)**

**Financial Services Accreditation  
Program for Lockbox  
(FSAP-Lockbox)  
Criteria**

**For The  
HEALTHCARE INDUSTRY**

*Version 2.0*

*Release date: January 1, 2009*


**Lee Barrett, Executive Director**

**For additional information see the EHNAC Web Site  
<http://www.EHNAC.org/>**

© Copyright 2008 Electronic Healthcare Network Accreditation Commission (EHNAC). All rights reserved.

Prefatory Notes:



If the criterion is marked with  then it is a MANDATORY requirement and must be addressed in the self assessment. Any MANDATORY criteria that are not fully completed will cause the candidate to FAIL the entire site review.

DEFINED TERMS are capitalized and used throughout these Criteria. The exact definition of each such term appears in the [Glossary of Terms](#) and should be consulted by the Candidate. The Glossary of Terms is located on the EHNAC web site.




Site Review Note: EHNAC realizes that some of the supporting documentation might not be able to be included in the Self assessment for many reasons. If you deem this to be the case, clearly indicate what your supporting documentation is, why you are not including it in your self assessment and how you will demonstrate it during the on-site review with the site reviewer. Please note that your organization may need to compensate EHNAC for an additional site visit, if the time required to review the documents exceeds one day.

## **CRITERIA I: PRIVACY AND CONFIDENTIALITY**

Accredited companies must have appropriate administrative, technical and physical policies and procedures to ensure the integrity and confidentiality of protected healthcare information. These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of such information. As a practical matter, the required level of security is intended to be commensurate with the attendant risks.

### [Narrative Summary indicating how the evidence reflects compliance with Criteria I.](#)

#### I.A. MEASURES TO ENSURE DATA PRIVACY AND CONFIDENTIALITY 45 CFR §§ 164.530(c)

- I.A. 1.  Candidate must have policies to protect against disclosure of PHI.
- I.A. 2. Candidate must have policies and procedures in place to ensure continuing compliance with data security policies, including secure methods of access to and transmission of data.
- I.A. 3. Candidate must use PHI about individuals only as is necessary for the processing of appropriate electronic transmissions as authorized by the customer.
- I.A. 4. Candidate must refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.
- I.A. 5.  Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it. 45 CFR §§ 164.312(a)(2)(iv) See also [CMS Internet Security Policy](#).
- I.A. 6. Candidate must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software.  
45 CFR §§ 164.308(a)(5)(ii)(B)
- I.A. 7.  Candidate must maintain a list of all individuals, contractors, and business associates with access to Electronic PHI.
- I.A. 8. Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices.
- I.A. 9. Candidate must demonstrate that appropriate security is in place for wireless networks to protect the privacy of data during transmission and in storage.

I.A. 10. Candidate must demonstrate that configuration standards are in place that include patch management for systems which store, transmit, or access Electronic PHI, including workstations.


## **CRITERIA II: TECHNICAL PERFORMANCE**

Accredited companies must provide their customers with the capability to communicate messages and records electronically (e.g. Electronic Data Interchange) by complying with the following technical performance criteria:

- Transmission of data
- Customer service inquiries
- Timeliness
- Accuracy
- System availability
- Compliance with industry standards
- Transport of physical documents
- Capacity monitoring
- Storage and retrieval
- Internet

[Narrative Summary indicating how the evidence reflects compliance with Standard II.](#)

### **II.A. TRANSMISSION OF DATA**

[II.A. 1.](#)  Candidate must be able to ensure compliance with all applicable Federal and State requirements and regulations.

### **II.B. CUSTOMER SERVICE INQUIRIES**

[II.B. 1.](#) Candidate must have an acknowledgment system and a customer tracking system that documents response times and procedures that are appropriate to different levels of requests.

[II.B. 2.](#) Candidate must be able to acknowledge customer service inquiries **within three hours.**

[II.B. 3.](#) Candidate must respond with a plan of action to open customer service inquiries **within one business day.**


### **II.C. TIMELINESS**

[II.C. 1.](#) Candidate must convert at least 50% of each business day's batch of eligible paper transactions to electronic transactions within one business day and that business day's remaining balance resolved within two days. This requirement includes all transactions under contract for paper to electronic conversion.

## II.D ACCURACY

- II.D. 1. Candidate must have formal policies and procedures for handling damaged documents that include notification to customer of the problem and instructions for resubmission.
- II.D. 2. Candidate must provide a scanning resolution of at least 200 DPI.
- II.D. 3. Candidate must have procedures to maintain the proper calibration for conducting Intelligent Optical Character Recognition (IOCR).

## II.E. SYSTEM AVAILABILITY

- II.E. 1.  Candidate must have a minimum system availability and appropriate redundancy that assures system access for **98.0% of contracted and/or advertised hours**. This requirement shall not preclude acts of God.

## II.F. COMPLIANCE WITH INDUSTRY STANDARDS 45 CFR §§ 162

- II.F. 1. Candidate must have the capability to produce generally accepted industry standard formats (like CMS-1500, UB04, ADA form, NSF) and approved, HIPAA-mandated implementation guides in a line of business as specified in the trading partner agreement.
- II.F. 2. Candidate must maintain a current analysis of any state privacy or security laws that Candidate reasonably believes apply to information stored or transmitted by Candidate (e.g., security breach notification laws). Candidate must have a plan to comply with any such laws.
- II.F. 3. Candidate must report to the Federal Government, in the course of implementing a customer's account and through periodic account reviews, any names matching the [Specially Designated Nationalist List \(SDN List\) \(Office of Foreign Assets Control\)](#) in accordance with the [USA Patriot Act](#).

## II.G TRANSPORT OF PHYSICAL DOCUMENTS

- II.G.1. Candidate must provide for the secure delivery of physical documents, such as from a Post Office to a lockbox processing facility or from a lockbox site to a check processing center.

## II.H CAPACITY MONITORING



- II.H. 1. Candidate must have the ability to measure hardware capacity and have developed an on-going monitoring capability for that hardware capacity.
- II.H. 2. Candidate must have a hardware capacity plan for handling peak load and expansion including a guarantee of **98% availability** on communication networks, servers, storage and network components.


II. I. Intentionally Left Blank

## II.J. STORAGE AND RETRIEVAL

- II.J. 1. Candidate must have, or show progress toward having, a **seven-year back-up** archive, storage, and regeneration capability for transactions if needed to meet customer Service Level Agreement (SLA) requirements.

## II.K. INTERNET

- II.K. 1.  Candidate must have a firewall configured to protect the system integrity.
- II.K. 2. Candidate must ensure that internal databases cannot be modified directly through an external web site, unless made securely, by authenticated users and contain integrity checks. Otherwise, all modifications to databases are to be made first only to external databases (e.g. those kept on the web server) and integrity checks are to be made on the external database prior to synchronization with any internal database.
- II.K. 3. Candidate must authenticate the trading partner sending or receiving healthcare data.
- II.K. 4. Candidate must have a process in place to monitor Internet bandwidth and communication server performance. Candidate must also provide capacity and bandwidth adequate for business needs.
- II.K. 5.  Candidate must have in place processes and procedures to monitor and/or block intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.

- [II.K. 6.](#) Candidate must have documented procedures to respond to intrusion or attack from the Internet **within 2 hours of alarm generation** or notification and be able to restore the system to pre-intrusion or pre-attack status **within 4 hours of alarm or notification**.
- [II.K. 7.](#)  Candidate must at least annually conduct threat and vulnerability assessments through an independent third party and have an improvement process based the results of those assessments.
- [II.K. 8.](#) Candidate must have documented procedures to check public security web sites, Web O/S vendor and web application vendors on at least a weekly basis to check identify potential security weaknesses and update web server O/S and application configurations to eliminate or reduce those known weaknesses.
- [II.K. 9.](#) Candidate must have documented web server security configurations to protect the web server from attack or intrusion.
- [II.K. 10.](#) Candidate must not have any file transfer servers configured to reside on a firewall in such a manner that the file transfer server may be able to be accessed through a "port forwarding" configuration through the firewall.

### **CRITERIA III: BUSINESS PRACTICES**

Accredited companies must have business practices that facilitate the maintenance of the technical performance Criteria and must exhibit the following:

- Truth in advertising

[Narrative Summary indicating how the evidence reflects compliance with Standard III.](#)

#### **III.A TRUTH-IN-ADVERTISING**

[III.A. 1.](#) Candidate must meet their own published service levels and have the ability to substantiate any claims of HIPAA compliance through third party or self-certification.


[III.A. 2.](#) Candidate must have policies and procedures to assure that any re-marketing agreements do not endanger compliance with the EHNAC Healthcare Network Accreditation Criteria.

## **CRITERIA IV: RESOURCES**


Accredited companies must possess the physical, human and administrative resources necessary to maintain a high level of technical performance and business practices. These resources must include: plant and equipment facilities adequate to conduct the company's current and anticipated business volume; qualified professional and staff personnel; and professional development programs to keep up with changes in the industry. While resource-related Criteria are primarily expressed in terms of inputs, they are required because of their basic role as guarantors of effective outcome performance.

[Narrative Summary indicating how the evidence reflects compliance with Standard IV.](#)

### **IV.A. PHYSICAL RESOURCES**

- [IV.A. 1.](#)  Candidate must have physical resources (including plant facilities and the relevant hardware and software) adequate for accomplishing the stated mission.
- [IV.A. 2.](#) Candidate must have formal expansion plans in place to anticipate increased network transmissions and resultant capacity needs. These formal plans should be reviewed regularly.

### **IV.B. PERSONNEL** 45 CFR §§ 164.308

- [IV.B. 1.](#) Candidate must have sufficient qualified personnel to perform all tasks associated with accomplishment of the stated mission.
- [IV.B. 2.](#) Candidate must provide educational resources to ensure that employees receive effective and periodic training. 45 CFR §§ 164.308(a)(5)(i)
- [IV.B. 3.](#)  Candidate must provide, at a minimum, annual job training, which includes privacy, and confidentiality, and security for all employees and contractors with access to PHI.
- [IV.B. 4.](#) Candidate must provide access for employees to professional development opportunities necessary to remain current in knowledge and skills.
- [IV.B. 5.](#) Candidate must maintain a list of individuals, down to the manager level, who are responsible for HIPAA compliance including the protection of Electronic PHI.

## **CRITERIA V: SECURITY**

Accredited companies must comply with the applicable standards, implementation specifications, and requirements of the HIPAA Security Rule with respect to Electronic Protected Health Information (PHI). When applicable to them, accredited companies must comply with state information security statutes and rules (e.g., security breach notification laws). Accredited companies must;


- Ensure the confidentiality, integrity, and availability of all Electronic PHI that the company creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule; and
- Ensure compliance with the HIPAA Security Rule by its Workforce.
- Implement procedures to identify what individual state health care security statutes and rules may have application; conduct a gap analysis with HIPAA's Security Rules and deploy the necessary systems to ensure compliance.

[Narrative Summary indicating how the evidence reflects compliance with Standard V.](#)

### **V.A. ORGANIZATIONAL REQUIREMENTS FOR HYBRID ENTITIES** 45 CFR §§ 164.314

[V.A. 1.](#) Candidate must have policies and procedures to ensure that its health care component protects PHI from another component within the candidate organization in accordance with the HIPAA Privacy and Security Final Rules.

[V.A. 2.](#) Candidate must document the designated health care components of any Hybrid Entity in accordance with the Security Rule.



[V.A. 3.](#)  Candidate must implement policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.

### **V.B. ADMINISTRATIVE SAFEGUARDS** 45 CFR §§ 164.308

[V.B. 1.](#) Candidate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the candidate. 45 CFR §§ 164.308(a)(1)(ii)(A)

[V.B. 2.](#) Candidate must implement an enforcement policy that will authorize the candidate to apply appropriate sanctions against Workforce members' contractors, vendors and their employees who are not in compliance with the security policies and procedures of the candidate. 45 CFR §§ 164.308(a)(1)(ii)(C)

- V.B. 3. Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 CFR §§ 164.308(a)(1)(ii)(D)
- V.B. 4. Candidate must identify the security official (and that person's backup) that is responsible for the development, implementation and enforcement of the policies and procedures required by the Security Rule for the candidate. 45 CFR §§ 164.308(a)(2)
- V.B. 5. Candidate must implement policies and procedures to ensure that all members of the candidate's Workforce have access only to Electronic PHI necessary to perform the employees work assignment and to prevent access to those Workforce members who do not have a need to access Electronic PHI. 45 CFR §§ 164.308(a)(3)
- V.B. 6. Candidate must implement clearance procedures to determine that the access of a Workforce member, vendor, contractor and their employees to Electronic PHI is appropriate and is limited to only that which is necessary to the performance of work duties. 45 CFR §§ 164.308(a)(3)(ii)(B)
- V.B. 7. Candidate must implement termination procedures for withdrawing access to Electronic PHI when the employment of a Workforce member ends; the Workforce member's duties no longer justify the need to access Electronic PHI or as required by determinations made as specified in criterion V.B.6. 45 CFR §§ 164.308(a)(3)(ii)(C)
- V.B. 8. Candidate must implement policies and procedures to ensure candidate's Workforce has appropriate access to PHI (electronic and non-electronic) that is consistent with the applicable requirements in the HIPAA Privacy Rule. 45 CFR §§ 164.530(c)
- V.B. 9. Candidate must if acting as part of a larger organization, implement policies and procedures that protects and secures the electronic PHI handled by the candidate organization from unauthorized access by the larger organization as well as their employees, vendors and contractors. 45 CFR §§ 164.308(a)(4)(ii)(A)
- V.B. 10. Candidate must maintain a listing of all hardware and software used to store, transmit or maintain Electronic PHI, including all Primary Domain Controllers (PDCs) and servers.
- V.B. 11. Candidate must implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process based on the entity's access authorization policies. 45 CFR §§ 164.308(a)(4)(ii)(C)

- [V.B. 12.](#) Candidate must implement a security awareness and training program for all members of the candidate's Workforce, including management. 45 CFR §§ 164.308(a)(5)
- [V.B. 13.](#) Candidate must implement periodic security updates, reminders and refresher programs for the members of the candidate's Workforce. 45 CFR §§ 164.308(a)(5)(ii)(A)
- [V.B. 14.](#) Candidate must implement procedures for creating, changing, and safeguarding passwords. 45 CFR §§ 164.308(a)(5)(ii)(D)
- [V.B. 15.](#)  Candidate must identify and respond to suspected or known security incidents; mitigate harmful effects of security incidents that are known to the candidate or its Workforce; and document security incidents and their outcomes. 45 CFR §§ 164.308(a)(6)(ii)
- [V.B. 16.](#) Candidate must establish written policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that damages systems that contain Electronic PHI. 45 CFR §§ 164.308(a)(7)
- [V.B. 17.](#) Candidate must establish and implement procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI. 45 CFR §§ 164.308(a)(7)(ii)(A)
- [V.B. 18.](#)  Candidate must establish and implement disaster recovery procedures to restore any loss of data, with the Recovery Point Objective **not to exceed 48 hours** and the Recovery Time Objective **not to exceed 72 hours** for critical transaction processing. 45 CFR §§ 164.308(a)(7)(ii)(B)
- [V.B. 19.](#) Candidate must establish and implement emergency mode operations procedures to enable continuation of critical business processes for protection of the security of Electronic PHI while operating in emergency mode. 45 CFR §§ 164.308(a)(7)(ii)(C)
- [V.B. 20.](#) Candidate must implement procedures for periodic testing, assessment, review and revision of contingency plans. Testing and revision should occur no less than annually. 45 CFR §§ 164.308(a)(7)(ii)(D)
- [V.B. 21.](#) Candidate must perform an applications and data criticality analysis by assessing the relative criticality of specific applications and data in support of other contingency plan components. 45 CFR §§ 164.308(a)(7)(ii)(E)

V.B. 22. Candidate must periodically perform a technical and non-technical evaluation based on the standards implemented in the Security Rule and subsequently respond to changes affecting the security of Electronic PHI that demonstrates the extent to which an entity's security policies and procedures meet the requirements of the Security Rule. 45 CFR §§ 164.308(a)(8)

V.B. 23. Candidate must have Business Associate contracts in place that obtain satisfactory assurances that the Business Associate will uphold the HIPAA Privacy and Security Rule requirements. 45 CFR §§ 164.308(b)(1)

V.C. PHYSICAL SAFEGUARDS  
45 CFR §§ 164.310

V.C. 1. Candidate must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access. 45 CFR §§ 164.310(a)(1)

V.C. 2. Candidate must establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. 45 CFR §§ 164.310(a)(2)(i)


V.C. 3. Candidate must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. 45 CFR §§ 164.310(a)(2)(ii)

V.C. 4. Candidate must implement procedures to control and validate a person's access to facilities based on their role or function including visitor control, and control of access to software programs for testing and revision. 45 CFR §§ 164.310(a)(2)(iii)


V.C. 5. Candidate must implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security such as hardware, walls, doors, and locks. 45 CFR §§ 164.310(a)(2)(iv)

V.C. 6. Candidate must 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 PHI. 45 CFR §§ 164.310(b)


V.C. 7. Candidate must implement policies and procedures, including a log, governing the receipt and removal of hardware and electronic media that contain Electronic PHI into and out of a facility, and the movement of these items within the facility. 45 CFR §§ 164.310(d)(1)

V.C. 8.  Candidate must implement policies and procedures to address the final disposition of Electronic PHI and/or the hardware or electronic media on which it is stored. 45 CFR §§ 164.310(d)(2)(i)

V.C. 9. Candidate must implement procedures for removal of Electronic PHI from electronic media before the media are made available for re-use. 45 CFR §§ 164.310(d)(2)(ii)

V.C. 10.  Candidate must implement policies and procedures to address the final disposition of paper containing PHI, including the appropriate shredding and disposal of such documents.

V.D. TECHNICAL SAFEGUARDS  
45 CFR §§ 164.312

V.D. 1.  Candidate must implement technical policies and procedures for electronic information systems that maintain Electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 CFR §§ 164.312(a)(1)

V.D. 2. Candidate must assign a unique name and/or number for identifying and tracking all systems user identity. 45 CFR §§ 164.312(a)(2)(i)

V.D. 3. Candidate must establish procedures for accessing necessary Electronic PHI during an emergency. 45 CFR §§ 164.312(a)(2)(ii)

V.D. 4. Candidate must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. 45 CFR §§ 164.312(a)(2)(iii)

V.D. 5. Candidate must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic PHI. 45 CFR §§ 164.312(b)

V.E. ORGANIZATIONAL REQUIREMENTS FOR BUSINESS ASSOCIATE CONTRACTS  
45 CFR §§ 164.308(b)(1)

- V.E. 1. Candidate must require Business Associates to implement administrative, physical, and technical policies and procedures that are reasonable, appropriate and required by Federal and State Law to protect the confidentiality, integrity, and availability of the Electronic PHI it creates, receives, maintains, or transmits on behalf of the candidate. 45 CFR §§ 164.314(a)(2)(i)(A)
- V.E. 2. Candidate must require Business Associates to ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate policies and procedures to protect it. 45 CFR §§ 164.314(a)(2)(i)(B)
- V.E. 3. Candidate must require Business Associates to report to the candidate any security incident of which it becomes aware. 45 CFR §§ 164.314(a)(2)(i)(C)
- V.E. 4. Candidate must require Business Associates to authorize termination of the Business Associates' contract by the candidate, in the event candidate determines that the Business Associate has violated a material term of the contract. 45 CFR §§ 164.314(a)(2)(i)(D)

V.F. POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

- V.F. 1. Candidate must record and maintain the policies and procedures implemented to comply with the HIPAA Security Rule in a secure written or electronic form. 45 CFR §§ 164.316(b)(1)(i)
- V.F. 2. Candidate must maintain a written and/or electronic record of any action, activity, or assessment that may be required by the HIPAA Security Rule. 45 CFR §§ 164.316(b)(1)(ii)
- V.F. 3. Candidate must retain the documentation, referred to herein, for 6 years from the date of creation or the date when it was last in effect, whichever is later. 45 CFR §§ 164.316(b)(2)(i)
- V.F. 4. Candidate must review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of the Electronic PHI. 45 CFR §§ 164.316(b)(2)(iii)