

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

**Healthcare Network
Accreditation Program
HNAP Plus Select SAS 70 (©) Criteria
(HNAP-70)**

**For The
HEALTHCARE INDUSTRY**

*Version 1.3
Released: January 2012*

Lee Barrett, Executive Director

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

© Copyright 2012 Electronic Healthcare Network Accreditation Commission (EHNAC). All rights reserved.

The HNAP Plus Select SAS 70(©) Criteria (HNAP-70) program is meant to assist companies to avoid the expense and effort of securing a SAS70 if this additional criteria will allow them to meet the requirements of some entities.

Please note that SAS70 is a proprietary term owned by the American Institute of Certified Public Accountants and that a SAS 70 audit can only be performed by an independent certified public accountant (CPA) or firm. CPA firms that perform SAS 70 audits must adhere to specific professional standards established by the American Institute of Certified Public Accountants (AICPA). Licensed public accounting firms are required to follow specific guidance related to planning, execution, and supervision of the audit procedures and the reporting of the results of the audit. In addition, public accounting firms are required to undergo a peer review to ensure that their firm's audits are conducted in accordance with the applicable professional standards. Specific practicing requirements may vary depending on the requirements of the applicable State Board and/or other governing bodies.

Prefatory Notes:

If a criterion is marked with [MANDATORY] it 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.

Please refer to EHNAC's [Glossary of Terms](#) for definitions of any unfamiliar terms referenced throughout this document. The Glossary of Terms is located at the EHNAC web site, www.ehnac.org.

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.

Some of the Criteria may not apply, or may apply in different ways, to some applicants. These Criteria have been given a designation at the beginning of the Criteria to accommodate the various business models Electronic Healthcare Networks (EHNs) support today. Among the modules listed are:

- G (General) – To be addressed by all candidates,
- B (Batch) – To be addressed by EHNs supporting any batch transaction processing,
- P (Payer) – To be addressed by Payer EHNs
- R (Real-time) – To be addressed by EHNs supporting any real-time transaction processing
- S (Scanning) – To be addressed by organizations that scan transactions for conversion to EDI
- V (VAN) – To be addressed by Value Added Networks. Note: A VAN is a private network provider (sometimes called a turnkey communications line) that is hired by a company to facilitate electronic data interchange (EDI) or to provide other network services.
- Z (Paper) – To be addressed by organizations that print transactions to paper

Note that if your organization supports more than one type of processing, you will need to complete the appropriate Criteria module for each type.

SECTION I: INTRODUCTION TO CANDIDATE ENVIRONMENT

Accredited companies must provide a diagram or a spreadsheet identifying where the organization's PHI is stored, received, maintained or transmitted.

I. A. PHI Flow

[I.A.1](#) **[MANDATORY]** (G) Candidate must provide a diagram or spreadsheet listing all Essential Function sites including their name, address, relationship to the entity under review, and the functions performed.
{493}

SECTION II: 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.

II. A. Measures to Ensure Data Privacy and Confidentiality

- [II.A.1](#) [MANDATORY] (G) Candidate must have policies to protect against disclosure of PHI.
{177}
- [II.A.2](#) (G) 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.
{178}
- [II.A.3](#) (G) Candidate must limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request.
{437} HITECH §13405(b)(1)(A); 45 C.F.R. §164.502(b)
- [II.A.4](#) (G) Candidate must refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.
{180}
- [II.A.5](#) [MANDATORY] (G) Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it.
{450} HITECH § 13402(h); 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312 (e)(2)(ii)
- [II.A.6](#) (G) Candidate must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software.
{182} 45 C.F.R. § 164.308(a)(5)(ii)(B)
- [II.A.7](#) [MANDATORY] (G) Candidate must maintain a list of all individuals, contractors, and business associates with access to Electronic PHI.
{409} 45 CFR §§ 164.530(c)
- [II.A.8](#) [MANDATORY] (G) Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.
{410} 45 CFR §§ 164.530(c)

- [II.A.9](#) (G) Candidate must demonstrate that appropriate security is in place for wireless networks to protect the privacy of data during transmission and in storage.
{185}
- [II.A.10](#) (G) Candidate must demonstrate that configuration standards are in place that include patch management for systems which store, transmit, or access Electronic PHI, including workstations.
{186}
- [II.A.11](#) (G) Candidate must implement a security measure to ensure that electronically transmitted PHI is not improperly modified without detection.
{187} 45 C.F.R. § 164.312(e)(2)(i)
- [II.A.12](#) **[MANDATORY]** (G) Candidate must implement policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.
{494}

SECTION III: TECHNICAL PERFORMANCE

Accredited companies must provide their customers with the capability to communicate messages and records electronically (e.g. Electronic Data Interchange) through compliance with the technical performance criteria in this section.

III. A. Transmission of Data

[III.A.1](#) [MANDATORY] (B,R,P) Candidate must be able to receive and submit 100% of all eligible transactions electronically from and to all trading partners who accept or generate transactions electronically.
{191}

[III.A.2](#) [MANDATORY] (V) Candidate must be able to convert data to ensure interoperability as required by any service level agreements.
{411}

[III.A.3](#) (B,P) Candidate must make available for transmission reports and/or data received electronically from trading partners to customers within one business day of receipt.
{193}

[III.A.4](#) [MANDATORY] (G) Candidate must comply with all applicable federal and state requirements and regulations.
{194}

III. B. Customer Service Inquiries

[III.B.1](#) (G) Candidate must have an acknowledgment system and a trading partner tracking system that documents response times and procedures that are appropriate to different levels of requests.
{195}

[III.B.2](#) (G) Candidate must be able to acknowledge trading partner inquiries within three business hours.
{196}

[III.B.3](#) (B,R,P) Candidate must respond with a plan of action to open trading partner inquiries within one business day.
{197}

[III.B.4](#) (V) Candidate must respond with a plan of action to operational critical trading partner inquiries within four hours during normal business hours.
{198}

[III.B.5](#) (G) Candidate must have documented escalation procedures to follow the inquiry to completion.
{199}

III. C. Timeliness

- [III.C.1](#) (B,P) Candidate must submit 95% of all batch transactions within one business day or the next applicable window of opportunity.
{200}
- [III.C.2](#) (V) Candidate must transmit 100% of all valid batch transactions and store and forward data within thirty minutes of receipt.
{201}
- [III.C.3](#) (R,P) Candidate must process real-time transactions on an average of no longer than two seconds from the time any transaction is received until it is passed on to the next recipient.
{202}

III. D. Accuracy

- [III.D.1](#) (B,R,P) Candidate must be able to demonstrate that 100% of transactions are either delivered successfully to the trading partner or are reported to the originator as undeliverable.
{203}
- [III.D.2](#) (V) Candidate must have 95% of transactions accepted on the first transmission to the trading partner.
{204}
- [III.D.3](#) (B,R,P) Candidate must provide for the identification of errors and allow for correction by the trading partner prior to resubmission to candidate or transmission to the payer.
{205}
- [III.D.4](#) (V) Candidate must provide for the monitoring and reporting of failed data transmissions to the sender. Reporting should specifically indicate the source of the problem for resolution if known.
{206}
- [III.D.5](#) (G) Candidate must have sufficient controls in place to ensure that transactions are delivered accurately and completely between internal systems, including financial systems.
{148}
- [III.D.6](#) (G) Candidate must have controls in place to ensure that any data conversion is tested between its origin and its destination to confirm the integrity of that conversion.
{149}

[III.D.7](#) (S,Z) Candidate must have formal policies and procedures for handling damaged documents that include notification to customer of the problem and instructions for resubmission.
{170}

[III.D.8](#) (S) Candidate must provide a scanning resolution of at least 200 DPI.
{171}

[III.D.9](#) (S) Candidate must have procedures to maintain the proper calibration for conducting Intelligent Optical Character Recognition (IOCR).
{172}

[III.D.10](#) (S) Candidate must have the ability to measure Intelligent Optical Character Recognition (IOCR) failure rates and have developed an ongoing monitoring and process improvement process.
{370}

III. E. System Availability

[III.E.1](#) **[MANDATORY]** (B,R,V,P) 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 include outages due to acts of God.
{412}

[III.E.2](#) (G) Candidate must notify trading partners regarding critical service outages outside the standard maintenance schedule prior to the planned outages.
{421}

III. F. Configuration Management

[III.F.1](#) (G) Candidate must develop and enforce clear policies restricting the use of personal, unlicensed, and unapproved software.
{150}

[III.F.2](#) **[MANDATORY]** (G) Candidate's SDLC framework must include the periodic testing and assessment of software and systems to ensure their ongoing appropriate configuration.
{151}

III. G. Compliance with Industry Standards

[III.G.1](#) (G) Candidate must have the capability to support generally accepted industry standard formats and those required by federal and state regulations in a line of business as specified in the trading partner agreement.
{208} 45 C.F.R. § 162

[III.G.2](#) [MANDATORY] (G) Candidate must have an established implementation plan for compliance with all applicable federal and state adopted rules and implementation guides. This implementation plan should include at least an implementation sequence and timetable for implementation within mandatory timeframes.
{496} 45 C.F.R. § 162

[III.G.3](#) (G) Candidate must maintain a current analysis of any federal or 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.
{210} 45 C.F.R. § 162

III. H. Editing

[III.H.1](#) (B,R) Candidate must provide editing capabilities for all trading partners for administrative transactions.
{211}

[III.H.2](#) (B) Candidate must provide editing capabilities for administrative transactions that allow for a 99.9% acceptance rate on first transmission based on the documented editing criteria.
{212}

III. J. Capacity Monitoring

[III.J.1](#) (G) Candidate must have the ability to measure system capacity and have developed an on-going monitoring capability for that system capacity.
{214}

[III.J.2](#) (B,R,P) Candidate must have a formal system capacity plan for handling peak load and expansion including a demonstration of 99.5% availability on communication exchange components per the advertised service level agreements. This requirement does not include outages due to acts of God.
{414}

III. K. Auditing

[III.K.1](#) (B) Candidate must provide a clear and accurate audit trail permitting monitoring of all data transactions for a minimum of seven years.
{216}

III. L. Storage and Retrieval

- [III.L.1](#) [MANDATORY] (B,P) Candidate must have an off-site minimum of six-month back-up archive, storage and retrieval capability for all batch transactions and adhere to all applicable federal and state regulations.
{415}
- [III.L.2](#) (R) Candidate must have one-day storage and retrieval capability for real-time transactions.
{218}
- [III.L.3](#) (B) Candidate must have, or show progress toward having, a seven-year back-up archive, offsite storage, and restore capability for all batch claim transactions. Backup should include the inbound transaction as received and outbound as sent at a minimum.
{497}
- [III.L.4](#) (B) Candidate must have the ability to regenerate a batch transaction going back 90 days within two business days.
{418}

III. M. Internet

- [III.M.1](#) [MANDATORY] (G) Candidate must have a firewall configured to protect the system integrity.
{221}
- [III.M.2](#) (G) 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.
{222}
- [III.M.3](#) (G) Candidate must authenticate the trading partner sending or receiving healthcare data.
{223}
- [III.M.4](#) (G) Candidate must provide capacity and bandwidth adequate for business needs. Candidate must have a process in place to monitor Internet bandwidth and communication server performance daily.
{224}

- [III.M.5](#) **[MANDATORY]** (G) 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.
{225}
- [III.M.6](#) (G) Candidate must have documented procedures to respond to a successful intrusion or attack from the Internet within 2 hours of alarm generation or notification.
{226}
- [III.M.7](#) **[MANDATORY]** (G) Candidate must on at least a quarterly basis conduct threat and vulnerability assessments and have an improvement process based on the results of those assessments. At least annually these assessments must be conducted through an independent third party.
{498}
- [III.M.8](#) (G) 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 identify potential security weaknesses and update web server O/S and application configurations to eliminate or reduce those known weaknesses.
{228}
- [III.M.9](#) (G) Candidate must have documented web server security configurations to protect the web server from attack or intrusion.
{229}
- [III.M.10](#) (G) 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.
{230}

III. N. Change Management

- [III.N.1](#) **[MANDATORY]** (G) Candidate must have a formal change management framework and procedures must be implemented to ensure all system software changes are controlled in line with this framework.
{153}
- [III.N.2](#) (G) Candidate must ensure that its change management procedures include formal procedures for addressing requests for changes, system maintenance, and supplier maintenance, and that all such requests are categorized and prioritized.
{154}
- [III.N.3](#) (G) Candidate must include in its change management framework a formal process for declaring, assessing, authorizing and recording an emergency change.
{155}

III. O. Transport of Physical Documents

[III.O.1](#) **[MANDATORY]** (S,Z) Candidate must have policies and procedures to ensure documents containing PHI are neither stored nor transported in an insecure manner outside the secured environment.
{371}

[III.O.2](#) **[MANDATORY]** (S,Z) Candidate must have a clean desk policy that requires that employees shred or securely lock all paper documents containing PHI when the employee's workspace is unoccupied.
{372}

SECTION IV: BUSINESS PRACTICES

Accredited companies must have business practices that facilitate the maintenance of the technical performance Criteria and must exhibit truth-in-advertising -- i.e., the company must actually be doing what it says it will do for customers.

IV. A. Truth-in-Advertising

[IV.A.1](#) (G) Candidate must meet their own published service levels.
{231}

[IV.A.2](#) (G) Candidate must have policies and procedures to assure that any re-marketing agreements do not endanger compliance with the EHNAC Healthcare Network Accreditation Criteria.
{232}

IV. B. Access

[IV.B.1](#) (G) Candidate must provide other organizations access to advertised services in conformance with applicable healthcare legislation.
{233}

[IV.B.2](#) (V) Candidate must be capable of interconnecting to other VANs complying with accepted ANSI ASC X12 mailbag standards or X400.
{234}

IV. C. Quality Management

[IV.C.1](#) **[MANDATORY]** (G) Candidate must have a documented Quality Management System (QMS) that defines and maintains goal-driven quality metrics for its IT organization.
{156}

IV. D. Formal SDLC Program

[IV.D.1](#) **[MANDATORY]** (G) Candidate must utilize a system development life cycle (SDLC) methodology that governs the process of developing, acquiring, implementing, and maintaining information technology. Such methodology must be utilized for the acquisition or development of new technology as well as for major changes to existing technology.
{157}

[IV.D.2](#) (G) Candidate must include requirements that systems employ appropriate controls for processing transactions to assure completeness, accuracy, and proper authorization.
{158}

[IV.D.3](#) (G) Candidate's IT function must involve appropriately qualified users in designing and testing systems and in performing formal post-implementation reviews.
{159}

[IV.D.4](#) (G) Candidate must ensure that the business requirements to be addressed by new or modified systems be formally documented and approved prior to the development, implementation or modification.
{160}

IV. E. Formal Testing Process

[IV.E.1](#) **[MANDATORY]** (G) Candidate must utilize formal testing procedures for all significant changes to applications and infrastructure technology. Such procedures must address unit system integration, user-acceptance-level, and load and stress testing.
{161}

IV. F. IT. Strategic Planning

[IV.F.1](#) **[MANDATORY]** (G) Candidate must have formal strategic plans for Information Technology (IT), based on input from the appropriate internal and external stakeholders, which align with the organization's short- and long-range plans. IT objectives and direction must be regularly communicated at the appropriate level of detail to all members of the organization.
{162}

[IV.F.2](#) (G) Candidate's IT management must communicate its activities, challenges and risks on a regular basis to the CEO and CFO, with appropriate information communicated to the board of directors.
{163}

[IV.F.3](#) (G) Candidate must establish a feedback mechanism for IT, management, and key stakeholders using candidate's services. This feedback must be evaluated against its strategic plan and considered in the IT planning process.
{164}

IV. G. Third Party Services Management

[IV.G.1](#) (G) Candidate must ensure that third parties are properly qualified to deliver the required service (due diligence), and that they are regularly monitored and reported on regarding the achievement of service-level performance criteria.
{165}

IV. H. End-User Computing

- [IV.H.1](#) (G) Candidate must identify all critical end-user systems, including spreadsheets and other user-developed programs, and ensure they are documented and subject to appropriate controls including privacy and security requirements.
{166}

SECTION V: 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.

V. A. Physical Resources

[V.A.1](#) [MANDATORY] (G) Candidate must have physical resources (including plant facilities and the relevant hardware and software) adequate for accomplishing the stated mission.
{235}

[V.A.2](#) (G) Candidate must have formal facility expansion plans in place to anticipate increased growth. These plans should be reviewed at least annually.
{499}

V. B. Personnel

[V.B.1](#) (G) Candidate must have sufficient qualified personnel to perform all tasks associated with accomplishment of the stated mission.
{237} 45 C.F.R. § 164.308

[V.B.2](#) (G) Candidate must ensure that employees receive effective, relevant job training, and access to professional development opportunities necessary to remain current in knowledge and skills.
{238} 45 C.F.R. § 164.308

[V.B.3](#) [MANDATORY] (G) Candidate must provide, at a minimum, annual job training, which includes breach reporting and notification, privacy, and confidentiality, and security for all employees and contractors with access to PHI.
{419} 45 C.F.R. § 164.308(a)(5)(i); HITECH § 13402

[V.B.4](#) (G) Candidate must maintain a list of individuals, down to the manager level, who are responsible for HIPAA compliance including the protection of Electronic PHI.
{240} 45 C.F.R. § 164.308

[V.B.5](#) (G) Candidate must identify the IT regulatory official responsible for the identification of legal or regulatory requirements relevant to the IT resources and operations of its organization.
{167}

SECTION VI: 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.

VI. A. Organizational Requirements for Hybrid Entities

[VI.A.1](#) (H) Candidate must have policies and procedures to ensure that its healthcare component protects PHI from another component within the candidate organization in accordance with the HIPAA Privacy and Security Rules.
{241} 45 C.F.R. § 164.105

[VI.A.2](#) (H) Candidate must document the designated health care components of any Hybrid Entity in accordance with the Security Rule.
{242} 45 C.F.R. § 164.105

VI. B. Administrative Safeguards

[VI.B.1](#) **[MANDATORY]** (G) 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.
{244} 45 C.F.R. § 164.308(a)(1)(ii)(A)

[VI.B.2](#) (G) 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.
{245} 45 C.F.R. § 164.308(a)(1)(ii)(C)

[VI.B.3](#) (G) Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies to the security officer for review.
{246} 45 C.F.R §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C)

[VI.B.4](#) (G) Candidate must identify the privacy official and the security official, and those persons' backups, that are responsible for the development, implementation and enforcement of the policies and procedures required by the Privacy and Security

Rules. These responsibilities must be documented, including a description of their responsibilities, and communicated internally.

{247} 45 C.F.R. § 164.308(a)(2)

[VI.B.5](#) (G) 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 their work assignment and to prevent access to those Workforce members who do not have a need to access Electronic PHI.

{248} 45 C.F.R. § 164.308(a)(3)

[VI.B.6](#) (G) Candidate must implement 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.

{249} 45 C.F.R. § 164.308(a)(3)(ii)(B)

[VI.B.7](#) (G) 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 the previous criterion.

{250} 45 C.F.R. § 164.308(a)(3)(ii)(C)

[VI.B.8](#) (G) Candidate must implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI with the applicable requirements in the HIPAA Privacy Rule.

{251} 45 C.F.R. § 164.530(c)

[VI.B.9](#) (G) 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.

{252} 45 C.F.R. § 164.308(a)(4)(ii)(A)

[VI.B.10](#) (G) Candidate and their contractors 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. Documentation must be provided showing which software resides on which hardware.

{253} 45 C.F.R. § 164.308

[VI.B.11](#) (G) 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.

{254} 45 C.F.R. §§ 164.308(a)(4)(ii)(B)-(C)

- [VI.B.12](#) (G) Candidate must implement and document a security awareness and training program for all members of the candidate's Workforce, including management.
{255} 45 C.F.R. § 164.308(a)(5)
- [VI.B.13](#) (G) Candidate must implement and document periodic security updates, reminders and refresher programs for the members of the candidate's Workforce, including management.
{256} 45 C.F.R. § 164.308(a)(5)(ii)(A)
- [VI.B.14](#) (G) Candidate must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.
{257} 45 C.F.R. § 164.308(a)(5)(ii)(D)
- [VI.B.15](#) **[MANDATORY]** (G) Candidate must have a process in place to 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 appropriately document security incidents and their outcomes.
{258} 45 C.F.R. § 164.308(a)(6)(ii)
- [VI.B.16](#) (G) 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 impacts systems that contain Electronic PHI.
{259} 45 C.F.R. § 164.308(a)(7)
- [VI.B.17](#) (G) Candidate must establish and implement procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI if candidate stores PHI.
{260} 45 C.F.R. § 164.308(a)(7)(ii)(A)
- [VI.B.18](#) **[MANDATORY]** (G) 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 48 hours for critical transaction processing.
{500}
- [VI.B.19](#) (G) Candidate must establish, document, and implement emergency mode operations plans to enable continued protection of the Electronic PHI.
{501} 45 C.F.R. § 164.308(a)(7)(ii)(C)
- [VI.B.20](#) **[MANDATORY]** (G) Candidate must implement and document procedures for periodic testing, assessment, review and revision of disaster recovery and emergency mode operation plans. Testing and all appropriate revisions should occur no less than annually.
{502} 45 C.F.R. § 164.308(a)(7)(ii)(D)

- [VI.B.21](#) (G) Candidate must establish a process and perform an annual applications and data criticality analysis by assessing the relative criticality of specific applications and data in support of other contingency plan components.
{264} 45 C.F.R. § 164.308(a)(7)(ii)(E)
- [VI.B.22](#) (G) Candidate must establish a process to continuously monitor and perform an annual technical and non-technical evaluation based on applicable Federal and State regulations and standards 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 Federal and State regulations.
{265} 45 C.F.R. § 164.308(a)(8)
- [VI.B.23](#) (G) Candidate must have Business Associate contracts in place that obtain satisfactory assurances that the Business Associate will uphold applicable Federal and State regulations.
{266} 45 C.F.R. § 164.308(b)(1)
- [VI.B.24](#) (G) Candidate must have security and breach notification procedures in place in conformance with HIPAA and HITECH requirements. These procedures must require that the notifications are to be delivered without unreasonable delay.
{422} HITECH § 13402; 45 C.F.R. §§ 164.400-14

VI. C. Physical Safeguards

- [VI.C.1](#) (G) Candidate must implement and document 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.
{268} 45 C.F.R. § 164.310(a)(1)
- [VI.C.2](#) (G) Candidate must establish procedures that allow secure 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.
{269} 45 C.F.R. § 164.310(a)(2)(i)
- [VI.C.3](#) (G) Candidate must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
{270} 45 C.F.R. § 164.310(a)(2)(ii)
- [VI.C.4](#) (G) 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.
{271} 45 C.F.R. § 164.310(a)(2)(iii)

- [VI.C.5](#) (G) 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.
{272} 45 C.F.R. § 164.310(a)(2)(iv)
- [VI.C.6](#) (G) 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.
{273} 45 C.F.R. § 164.310(b)
- [VI.C.7](#) (G) 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.
{274} 45 C.F.R. § 164.310(d)(1)
- [VI.C.8](#) **[MANDATORY]** (G) 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.
{275} 45 C.F.R. § 164.310(d)(2)(i)
- [VI.C.9](#) (G) Candidate must implement procedures for removal of Electronic PHI from electronic media before the media are made available for re-use.
{276} 45 C.F.R. § 164.310(d)(2)(ii)
- [VI.C.10](#) **[MANDATORY]** (G) Candidate must implement policies and procedures to address the final disposition of paper containing PHI, including the appropriate shredding and disposal of such documents.
{98} 45 C.F.R. § 164.310
- [VI.C.11](#) (G) Candidate must implement policies and procedures to create a retrievable exact copy of Electronic PHI before movement of equipment where PHI is stored.
{277} 45 C.F.R. § 164.310(d)(2)(iv)

VI. D. Technical Safeguards

- [VI.D.1](#) **[MANDATORY]** (G) 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.
{278} 45 C.F.R. § 164.312(a)(1)
- [VI.D.2](#) (G) Candidate must assign a unique name and/or number for identifying and tracking all systems' user identity.
{279} 45 C.F.R. § 164.312(a)(2)(i)

- [VI.D.3](#) (G) Candidate must establish procedures for accessing necessary Electronic PHI during an emergency.
{280} 45 C.F.R. § 164.312(a)(2)(ii)
- [VI.D.4](#) (G) Candidate must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
{281} 45 C.F.R. § 164.312(a)(2)(iii)
- [VI.D.5](#) (G) Candidate must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic PHI.
{282} 45 C.F.R. § 164.312(b)

VI. E. Organizational Requirements for Business Associate Contracts

- [VI.E.1](#) (G) 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.
{283} 45 C.F.R. § 164.314(a)(2)(i)(A)
- [VI.E.2](#) (G) 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.
{284} 45 C.F.R. § 164.314(a)(2)(i)(B)
- [VI.E.3](#) (G) Candidate must require Business Associates to report to the candidate any security incident of which it becomes aware.
{285} 45 C.F.R. § 164.314(a)(2)(i)(C)
- [VI.E.4](#) (G) 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.
{286} 45 C.F.R. § 164.314(a)(2)(i)(D)
- [VI.E.5](#) (G) Candidate must ensure Business Associates are contractually required to comply with all applicable Federal and State regulations including HITECH privacy and security requirements.
{423} HITECH §§ 13401(a), 13404(a)
- [VI.E.6](#) (G) Candidate must require that all Business Associates notify the Candidate in the event any PHI is improperly used or disclosed, including for the purpose of the breach notification rule.
{491} HITECH §13404(b), 45 CFR §§ 164.314(a)(2)(i)(C)

[VI.E.7](#) (G) Candidate must have business associate agreements in place with every organization that contracts with it for the purpose of exchanging or routinely accessing electronic PHI.
{495} HITECH §13408, 45 CFR § 164.502(e)(2)

VI. F. Policies and Procedures and Documentation Requirements

[VI.F.1](#) (G) Candidate must record and maintain the policies and procedures implemented to comply with applicable federal and state regulations, and policies and procedures should be available to those that need access to them.
{291} 45 C.F.R. §§ 164.316(b)(1)(i), 164.316(b)(2)(ii)

[VI.F.2](#) (G) Candidate must maintain a written and/or electronic record of any action, activity, or assessment that may be required by applicable Federal and State regulations.
{292} 45 C.F.R. § 164.316(b)(1)(ii)

[VI.F.3](#) (G) 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.
{293} 45 C.F.R. § 164.316(b)(2)(i)

[VI.F.4](#) (G) Candidate must review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of the Electronic PHI.
{294} 45 C.F.R. § 164.316(b)(2)(iii)