

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
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.	Candidate must use PHI about individuals only as is necessary for the processing of appropriate electronic transmissions as authorized by the trading partner.	Change
I. A.	11		Candidate must implement a security measure to ensure that electronically transmitted PHI is not improperly modified without detection.	New
I. A.	12	Candidate must implement policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.	(unchanged)	Previously V. A. 3
II. A.	1	Candidate must be able to ensure compliance with all applicable Federal and State requirements and regulations.	Candidate must comply with all applicable federal and state requirements and regulations.	Change
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.	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.	Change
II. B.	2	Candidate must be able to acknowledge customer service inquiries within three hours.	Candidate must be able to acknowledge trading partner inquiries within three business hours.	Change
II. B.	3	Candidate must respond with a plan of action to open customer service inquiries within one business day.	Candidate must respond with a plan of action to open trading partner inquiries within one business day.	Change
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.	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.	Change
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.	No change
II. D.	2		Candidate must provide a scanning resolution of at least 200 DPI.	No change
II. D.	3		Candidate must have procedures to maintain the proper calibration for conducting Intelligent Optical Character Recognition (IOCR).	No change
II. D.	4		Candidate must have the ability to measure Intelligent Optical Character Recognition (IOCR) failure rates and have developed an ongoing monitoring and process improvement process.	New

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
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.	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.	Change
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.	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.	Change
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.	Candidate must report to the Federal Government any names matching the Specially Designated Nationalist List (SDN List) in accordance with the Office of Foreign Assets Control (OFAC) regulations.	Change
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.	No change
II. G.	2		Candidate must have policies and procedures to ensure documents containing PHI are neither stored nor transported in an insecure manner outside the secured environment.	New
II. G.	3		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.	New
II. H.	1	Candidate must have the ability to measure hardware capacity and have developed an on-going monitoring capability for that hardware capacity.	Candidate must have the ability to measure system capacity and have developed an on-going monitoring capability for that system capacity.	Change
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.	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 preclude acts of God.	Change
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.	No change

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
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.	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.	Change
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.	Candidate must have documented procedures to respond to a successful intrusion or attack from the Internet within 2 hours of alarm generation or notification.	Change
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.	Candidate must on at least a quarterly basis conduct threat and vulnerability assessments through an independent third party and have an improvement process based on the results of those assessments.	Change
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.	Candidate must meet their own published service levels.	Change
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.	Candidate must have formal facility expansion plans in place to anticipate increased growth. These plans should be reviewed regularly.	Change
IV. B.	2	Candidate must provide educational resources to ensure that employees receive effective and periodic training.	Candidate must ensure that employees receive effective, relevant job training, and access to professional development opportunities necessary to remain current in knowledge and skills.	Change (combined old IV.B.2 and IV.B.4)
IV. B.	4	Candidate must maintain a list of individuals, down to the manager level, who are responsible for HIPAA compliance including the protection of Electronic PHI.	(unchanged)	Previously IV. B. 5
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.	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.	Change
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.	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.	Change

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
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.	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.	Change
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.	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.	Change
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.	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.	Change
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.	Candidate must implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI with the applicable requirements in the HIPAA Privacy Rule.	Change
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.	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.	Change
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.	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.	Change
V. B.	12	Candidate must implement a security awareness and training program for all members of the candidate's Workforce, including management.	Candidate must implement and document a security awareness and training program for all members of the candidate's Workforce, including management.	Change
V. B.	13	Candidate must implement periodic security updates, reminders and refresher programs for the members of the candidate's Workforce.	Candidate must implement and document periodic security updates, reminders and refresher programs for the members of the candidate's Workforce, including management.	Change

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
V. B.	14	Candidate must implement procedures for creating, changing, and safeguarding passwords.	Candidate must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.	Change
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.	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.	Change
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.	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.	Change
V. B.	17	Candidate must establish and implement procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI.	Candidate must establish and implement procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI if candidate stores PHI.	Change
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.	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.	Change
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.	Candidate must establish, document, and implement emergency mode operations procedures to enable continued protection of the Electronic PHI.	Change
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.	Candidate must implement and document procedures for periodic testing, assessment, review and revision of contingency plans. Testing and all appropriate revisions should occur no less than annually.	Change
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.	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.	Change
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.	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.	Change

FSAP-Lockbox 2.1 Changes - Criteria

Subsection	Number	V2.0 Criterion	V2.1 Criterion	Change
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.	Candidate must have Business Associate contracts in place that obtain satisfactory assurances that the Business Associate will uphold applicable Federal and State regulations.	Change
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.	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.	Change
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.	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.	Change
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.	No change
V. C.	11		Candidate must implement policies and procedures to create a retrievable exact copy of Electronic PHI before movement of equipment where PHI is stored.	New
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.	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.	Change
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.	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.	Change
		Candidate must provide access for employees to professional development opportunities necessary to remain current in knowledge and skills.		Old IV. B. 4 deleted