

Criteria Number	Previous Criteria	New Criteria
I.A.3	Candidate must use PHI about individuals only as is necessary for the processing of appropriate electronic transmissions as authorized by the trading partner.	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.
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.	Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it.
I.A.8	Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices.	Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.
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.	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.
II.E.2		Candidate must notify trading partners regarding critical service outages outside the standard maintenance schedule prior to the planned outages.
II.H.2	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.	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.
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.	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.
V.B.24		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.
V.E.5		Candidate must ensure Business Associates are contractually required to comply with all applicable Federal and State regulations including HITECH privacy and security requirements.
V.E.6		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.

Criteria Number	Previous Criteria	New Criteria
V.E.7		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.