

TITLE: Risk Analysis Policy

Category: Technical Support	
Original Effective Date: 3-12-08	Review Date: February 2008

ACCEL and BARTON will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the ACCEL Systems prior to implementation and on a periodic basis thereafter.

As part of this assessment, ACCEL also expects each Participant to be responsible for performing a risk analysis prior to ACCEL implementation and on a periodic basis thereafter which includes:

- how Participant's existing systems interact with the ACCEL system(s)
- how Participant's existing policies and procedures support the privacy and security objectives of the ACCEL system(s)

1. Policy & Procedures Review

Policies and procedures will be evaluated on the basis of industry standards, HIPAA Regulations, and the security objectives of ACCEL. When reviewing existing policies, ACCEL and Participant will assess their comprehensiveness, identify specific strengths and weaknesses, and evaluate for HIPAA compliance.

At their discretion, ACCEL and Barton may request to review Participant policies and procedures and outcomes of their assessments including risk mitigation approaches/actions.

2. Internal Vulnerability

The internal vulnerability analysis to identify risks and vulnerabilities from within the network, as well as to assess compliance with industry standards, HIPAA regulations and guidelines, and ACCEL security policies, will be conducted using automated tools (where available) as well as direct, hands-on techniques, or observation where appropriate. The vulnerability analysis will be performed for ACCEL system(s) identified as critical by the Participant's HIPAA Security Officer and the Barton Director of IT. Note: Each participant's HIPAA security and privacy officers have responsibility to ensure their organization's policies and procedures support ACCEL).

The internal vulnerability analysis should include:

- a) Review of current network operating system security configurations including password and file access rights and an analysis of virus protection configurations and products for the ACCEL servers to ensure that acceptable anti-virus software is installed, properly updated, and maintained.
- b) ACCEL Systems will be identified and logged into a common catalogue with the appropriate level of file, system, and owner information. This information will be reviewed and updated, as necessary, on a periodic basis. As of January, 2008, the ACCEL system(s) in place to be catalogued are:
 - Repository Name:
 - Custodian Name:
 - Custodian Contact Information:

- System Name:
- System Location:
- System Manager:
- System Manager Contact Information:
 - phone-
 - e-mail:

3. Physical Security - The physical security analysis consists of an inspection and analysis of external conditions, windows and doors, alarm systems, mainframe/computer room security, surveillance systems, contract services (courier, janitorial, etc.), media storage, security administration, and limited review of contingency planning for the physical protection and disaster recovery of the facility as well as clinical information also referred to as electronically protected health information or EPHI in storage.

4. Barton will perform two basic types of information security risk analysis: baseline risk analysis and periodic risk.

- Baseline Risk Analysis will be conducted when establishing and implementing information security policies and procedures. This analysis will provide information required in the design and deployment of security applications, implementation strategies, and configuration of security devices and applications as well as a baseline for measuring the effectiveness of the information security program.

Baseline Risk analysis will be performed by qualified independent Information Systems security professionals, or qualified internal staff, independent of those who configure or maintain the systems, experienced in information system risk analysis, and will include: Policy & Procedures Review, Internal Vulnerability Assessment, External Vulnerability Assessment, and Physical Security Assessment.

- Periodic Risk analysis will be performed in compliance with the policy of the ACCEL and Barton regarding risk analysis. The periodic risk analysis may be performed by contracted information security professionals or qualified IT staff. The analysis will always be conducted under the direction of a certified systems engineer, experienced in information system risk analysis and may consist of Policy & Procedures Review, Internal Vulnerability Assessment, External Vulnerability Assessment, and Physical Security Assessment.