csb ITS
SECURITY SOLUTIONS FOR HEALTH CARE

CONTINGENCY PLANNING

Methodology

HIPAA 45 CFR Part 160 and Part 164, Subparts A and C set security standards and require each covered entity to adopt administrative, physical, and technical safeguards. A key component of the administrative safeguards is §164.308(a)(7) contingency planning. The Contingency Plan standard includes five implementation specifications:

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

CSB IT Security utilizes NIST Special Publication 800-34 to guide our contingency planning efforts which includes all of the required implementation specifications.

The Results

A contingency planning project with CSB IT Security will provide you with a formal custom plan that covers each required topic. The plan will follow the NIST SP 800-34 Rev. 1 template and include a Business Impact Analysis.

When complete you will have a clear picture of your organizations dependencies on the systems you deliver and what it will take to recover from an interruption.

csb ITS

www.CSBITSolutions.com
admin@CSBITSolutions.com

(508) 817-7692

csb ITS
SECURITY SOLUTIONS FOR HEALTH CARE

CONTINGENCY PLANNING

CSB IT Security Experience

Why CSB IT Security?

Healthcare CIO executive experience

Certified technical experts

Risk Assessments that have passed CMS and OCR audits

Security experience with diverse healthcare organizations – hospitals, large physicians groups, HIEs, managed care organizations, IPAs and business associates

Modular approach designed to meet the practical needs of healthcare organizations

Practical solutions to combat the increasing threat of Hackers

csb ITS

www.CSBITSolutions.com
admin@CSBITSolutions.com

(508) 817-7692