The {{companyShortName}} Contingency Plan establishes procedures to recover {{companyShortName}}

following a disruption resulting from a disaster. This Disaster Recovery Policy

is maintained by the {{companyShortName}} Security Officer and Privacy Officer.

{{#needStandardHIPAA}}

\*\*HIPAA:\*\* This {{companyShortName}} Contingency Plan has been developed as

required under the Office of Management and Budget (OMB) Circular A-130,

Management of Federal Information Resources, Appendix III, November 2000, and

the Health Insurance Portability and Accountability Act (HIPAA) Final Security

Rule, Section §164.308(a)(7), which requires the establishment and

implementation of procedures for responding to events that damage systems

containing electronic protected health information.

{{/needStandardHIPAA}}

{{#needStandardNIST}}

\*\*NIST:\*\* This {{companyShortName}} Contingency Plan is created under the

legislative requirements set forth in the Federal Information Security

Management Act (FISMA) of 2002 and the guidelines established by the National

Institute of Standards and Technology (NIST) Special Publication (SP) 800-34,

titled "Contingency Planning Guide for Information Technology Systems" dated

June 2002.

{{/needStandardNIST}}

## Policy Statements

{{companyShortName}} policy requires that:

(a) A plan and process for business continuity and disaster recovery (BCDR),

including the backup and recovery of systems and data, must be defined and

documented.

(b) BCDR shall be simulated and tested at least once a year. Metrics shall be

measured and identified recovery enhancements shall be filed to improve the BCDR

process.

(c) Security controls and requirements must be maintained during all BCDR

activities.