



BIA & Disaster Recovery Plan

Prepared for a Disaster?

Contingency planning, also referred to as Business Continuity Planning (BCP), is a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building Contingency Plans.

Once the BIA is completed, Contingency Plans can be developed using the information identified in the BIA. Typically, two types of Contingency Plans will need to be developed. Emergency Mode Plans for business unit recovery and Disaster Recovery Plans (DRP) for Information Technology (IT) systems and infrastructures.

HIPAA COMPLIANCE MANDATE

Contingency plan is a HIPAA Security standard. The objective of the contingency plan standard is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. As shown in bold in the Figure below, the Contingency Plan standard is defined within the Administrative Safeguards section of the HIPAA Security Rule.

Standards	Implementation Specifications	R = Required A = Addressable
Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis	R R R A A

Contingency plan related requirements are also identified as implementation specifications in the Physical Safeguards section of the HIPAA Rule as well as the Technical Safeguards section.

It Starts with a BIA

A BIA is a critical step in contingency planning. The critical steps for a BIA include the need to:

1. Identify business disruption events and measure probabilities
2. Identify critical business functions
3. Identify critical computer resources that support key business functions
4. Identify disruption impacts and allowable outage times
5. Develop recovery priorities

OUR bizSHIELD™ METHODOLOGY

The Seven Steps to Enterprise Security is a methodology that describes a road-map to safeguard sensitive business information and enterprise vital assets. This methodology is also referred to as bizShield™. bizShield™ has also been influenced by the clauses (domains) defined in the ISO 27002 security standards as well as the CobIT and NIST security frameworks.

The bizShield™ methodology delivers *confidentiality, integrity and availability* (CIA) of your vital information and business assets. This methodology provides the blueprint for defending today's enterprise. The Seven Steps methodology provides the framework for addressing contingency requirements.

The bizShield™ security methodology identifies seven critical steps for an organization to follow as a twelve-month framework for organizing and prioritizing enterprise security initiatives.

OUR PROFESSIONAL TEAM

ecfirst only engages credentialed professionals for its BIA engagements. Credentials such as CISSP, CSCS and CBCP are typical of ecfirst teams assigned to client engagements.

YOUR COMMITMENT TO US

- 1) Interviews with key members of IT staff, key individuals in departments and management.
- 2) Copies of IT system and network documentation including downtime procedures and inventory of vital assets such as servers and applications.

OUR DELIVERABLE TO YOU

A bizShield™ Business Impact Analysis (BIA) document will be created based on our review and analysis of information collected from your organization. This bizShield™ Business Impact Analysis (BIA) Report will include information in the following areas:

- Business Risk Assessment
 - Key business processes identification
 - Time-bands for business service interruption management
 - Financial and operational impact
- Key Sensitive Systems and Applications Summary
- Emergency Incident Assessment
 - BIA process control summary for emergency incident assessment
 - Serious information security incidents
 - Environmental disasters
 - Organized and/or deliberate disruption
 - Loss of utilities and services

BIA & Disaster Recovery Plan (DRP) Services from ecfirst

- Equipment or system failure
- Other emergency situations

Fixed Fee with a Monthly Payment Schedule: Call for details and a customized proposal exclusively for your organization. *On-Demand Compliance Solutions from ecfirst provides your organization with access to specialized compliance and security skills with no short term or long term commitments. Get Started Today!*

COMPLIMENTARY PRIVATE WEBCAST ON CONTINGENCY PLANNING & BIA

For a complimentary private Webcast on Contingency Planning & BIA, please contact Audra Curtis at Audra.Curtis@ecfirst.com.

About ecfirst

Devoted To Our Clients. Delivering with Passion.

ecfirst, Home of The HIPAA Academy, is a leader with rich hands-on experience delivering world-class services in the areas of:

- Security regulatory compliance solutions (HIPAA, HITECH Act, PCI DSS, NIST and ISO 27000 Standards, State Regulations)
- Compliance training and certification
- HITECH data breach and incident response management
- End-to-end Meaningful Use EHR Stage 1 objective driven services including gap assessment, risk analysis, reporting and more
- Health Information Technology (IT) services including On-Demand Consulting (starting @ 40 hours), Management Compliance Services Proposal (MCSP), IT professional staffing and project management, customized portal development and security technology implementation

Compliance and Training Certification

ecfirst, home of the HIPAA Academy, offers the gold standard in compliance training and certification. The HIPAA CHA™, CHP and CHSS™ certifications are the only certifications recognized in the Industry. The ecfirst Certified Security Compliance Specialist™ (CSCS™) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

ecfirst delivers world-class information security and regulatory compliance solutions. With over 1,600+ clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes Microsoft, Symantec, HP, McKesson, EMC, IBM, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.



Regulatory Compliance Practice

The ecfirst Regulatory Compliance Practice delivers deep expertise with its full suite of services that include; HIPAA Privacy Gap Analysis, Meaningful Use Risk Analysis, HITECH Data Breach, Technical Vulnerability Assessment, Policy and Procedure Development, Disaster Recovery Planning, On-Demand Consulting, as well as managed security and IT infrastructure solutions.

ecfirst Differentiators

ecfirst combines state of the art tools, the highest credentialed staff, and reporting that maximizes value, efficiency, and information for our clients to deliver the industry's best technical vulnerability assessments.

Critical ecfirst differentiators include:

- Home of The HIPAA Academy – First in the healthcare industry with the Certified HIPAA Professional (CHP) and Certified Security Compliance Specialist (CSCS) programs
- Highly credentialed professional consulting team with expertise in HL7, ICD-9/10, HIPAA, HITECH, Meaningful Use
- Deep experience in the healthcare industry
- Compliance based vulnerability assessments
- Executive dashboards that may be tailored for senior management to highlight critical findings

Talk to ecfirst and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients. *We deliver value with intensity and are paranoid about our performance for your organization.*