Hospitals, health systems, physician practices, payers such as insurance organizations, as well as business associates must conduct a comprehensive risk analysis exercise to meet HIPAA mandates, including HITECH Meaningful Use requirements. Security standards such as ISO 27000 and NIST guidelines require a thorough risk assessment.

Have you completed a risk analysis exercise recently?

HIPAA™ Academy

ecfirst Perfecting the Art of Active Cyber Defense

Risk Analysis Solutions

bizSHIELD™

Risk Analysis: Critical for a Information Security Baseline

A key requirement of the HIPAA and HITECH regulations is that covered entities and business associates *must conduct a comprehensive and thorough assessment of the potentials risks and vulnerabilities to the confidentiality, integrity, and availability (CIA) of all electronic Protected Health Information (EPHI)*. These HIPAA and HITECH mandates require that organizations must complete a comprehensive and thorough vulnerability assessment on a regular schedule.

OCR Guidance on HIPAA Risk Analysis

The guidance published by the Office of Civil Rights states that, "Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational…" Further, OCR states that "All EPHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. Risk analysis is the first step in that process."
ecfirst's bizSHIELD™ program satisfies this HIPAA requirement.

HITECH Meaningful Use Requirements Include Risk Analysis

Demonstrating Meaningful Use of an Electronic Health Record (EHR) requirement tells organizations that they must, "Implement systems to protect the privacy and security of patient data." Organizations seeking to demonstrate Meaningful Use must, "Conduct or review a security risk analysis and implement security updates as necessary and correct identified security deficiencies."
ecfirst's bizSHIELD™ program satisfies this HITECH requirement.

*biz*SHIELD™ – An ecfirst Risk Analysis Service

ecfirst developed the *biz*SHIELD™ program to assist Covered Entities, Business Associates, and vendors of Electronic Health Records (EHRs) and Personal Health Records (PHRs) in meeting the requirements of the HIPAA Privacy and Security Rule, The HITECH Act, and all subsequent guidance documentation and settlement agreements.

As a part of the *biz*SHIELD™ program, ecfirst will list every requirement of the HIPAA Security Rule including every Safeguard, Standard, and Implementation Specification in a risk analysis format that identifies an organization's state of compliance with the requirement, recommended remediation activity, and associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the *biz*SHIELD™ Corrective Action Plan (CAP) table. The *biz*SHIELD™ report is an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

Privacy Gap Assessment Service

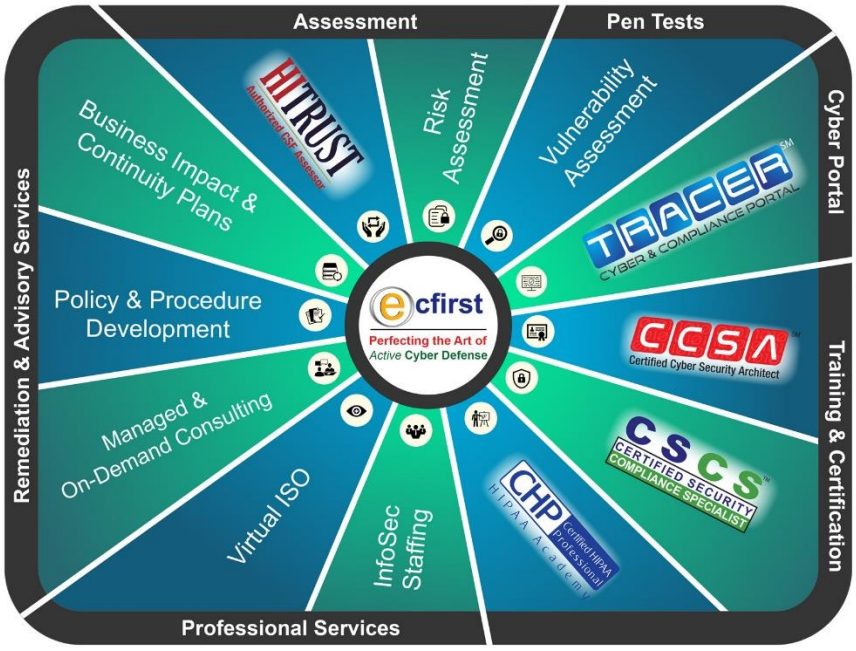
*biz*SHIELD^{tm} helps an organization to understand, improve, or verify their compliance with the HIPAA Privacy Rule. *biz*SHIELD^{tm} provides both summary and detailed compliance information as well as all necessary remediation activities pertinent to the organization's business model. *biz*SHIELD^{tm} will enable an organization to quickly determine the state of compliance, needed remediation, and will list actionable steps to achieve compliance.

HITECH Data Breach Service

Under the HITECH Data Breach Rule, organizations are required to take steps to prevent, identify, report, and remediate data breaches of unsecured information. The ecfirst Data Breach solution will document the ability of the organization to detect a breach, review the incident management policy and procedures, and make recommendations. In addition, organizations will receive a HITECH Data Breach policy and several Data Breach procedures to ensure compliance, should a breach happen.

ecfirst

Perfecting the Art of *Active* Cyber Defense



Client Reference

"BrightOutcome is focused in improving patient health outcomes across the continuum of care. BrightOutcome is deeply committed to securing patient information across our systems and Web-based applications. We have been working with Ali Pabrai and his wonderful team at ecfirst since 2012."

"The ecfirst team literally helped us build our HIPAA practices from ground up, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome
COLLABORATIVE SYMPTOM MANAGEMENT

DerShung Yang | Founder & President

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"We at BRG are always looking to improve and enhance our compliance and cybersecurity posture. This is an area of executive and strategic priority for our organization to secure confidential client information. From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time."

BRG
Berkeley Research Group

Chip Goodman | Vice President of Information Technology

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST
Authorized CSF Assessor

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

John T. Schelewitz

Regional Sales Director

ecfirst/HIPAA Academy

Phone: +1.480.663.3225

Email: John.Schelewitz@ecfirst.com

www.ecfirst.com