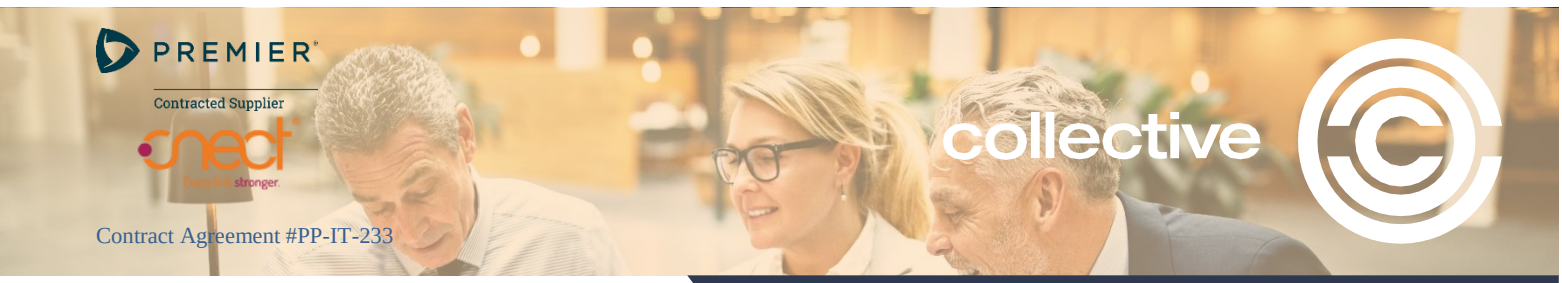


Contract Agreement #PP-IT-233

Security Risk Assessment

Delivering on the promise of technology **for healthcare**

Comprehensive Security Risk Assessment (SRA)

HIPAA requires that healthcare entities meet various national standards of security for the privacy of protected health information (PHI). Performing an SRA can aid Premier GPO member's business in its compliance efforts and provide a roadmap to full compliance.

Collective Group's SRA for Premier GPO member organizations looks at the numerous best practices and technology standards put together by HHS, NIST, ISACA, HIMSS, and AHIMA for healthcare-organization privacy and security—and supplies a simple-to-understand risk score matrix highlighting your organization's risks, as well as actionable recommendations for mitigating them.

Using our well-honed technology and high-level expertise, Collective's SRA provides a comprehensive review of your environment in a low-touch way. We let you know exactly where your business needs to focus to achieve full compliance—enabling your team to focus on your core business.

What's at stake?

Secure your data, avoid fines and penalties

The Health and Human Services Office for Civil Rights (OCR) has the authority to audit all entities under HIPAA—at any time for any reason. If an entity is found noncompliant, OCR can choose to levy fines and set up resolution agreements to enact constraints on the organization for years to come.

In 2020, OCR cited fined violators as failing to conduct **enterprise-wide risk analysis**, failing to implement **risk management**, or having **insufficient controls**.

OCR-mandated fines

$107.5 million = 2015–2020 total
$16.8 million = highest-ever fine
$13.5 million = 2020 total
$6.8 million = highest in 2020
$3,500 = lowest in 2020

—ranging from a major-insurer PHI breach of 10+ million people's data to a small provider's lack of individual-record access.

Don't let your business become a statistic.

About Collective Group

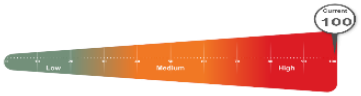
Since 1994, Collective has delivered more than 7 million hours of world-class IT services to clients across the United States. Our healthcare clients benefit by receiving the technical expertise we have gained from working with notable hardware and software partners over the years, such as EMC, Dell, NetApp, Microsoft, and Veritas. Our services are tailored to the specific needs of your team and environment. Choose Collective to deliver a standard of excellence and help you achieve your technology and business goals.

Contact

Trey Davis, VP Professional Services
Phone: 512-961-3582
Email: trey@collectivegroup.com
www.collectivegroup.com

120 S. Lakeline Blvd., Bldg. 1-200
Cedar Park, TX 78613
Phone: 512-263-5500
Fax: 512-263-0606

SRA Process and Results



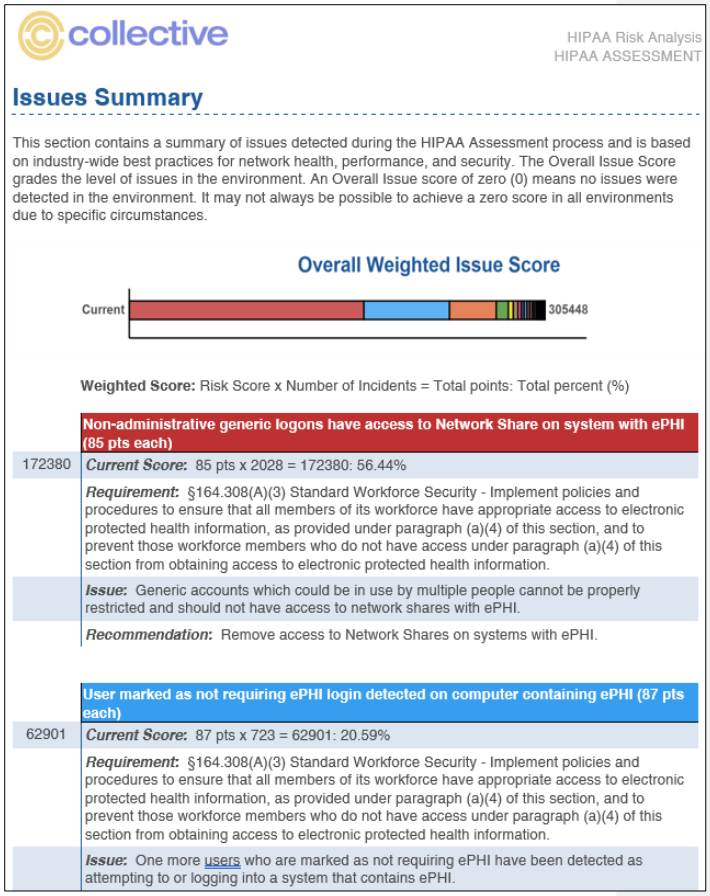
To be HIPAA-compliant, healthcare entities must follow the frameworks offered by NIST, specifically the Common Security Framework (CSF). The Collective SRA looks at more than 70 different items across seven high-level technical errors throughout your entire environment to ensure that the CSF requirements are being met.

Collective's SRA for Premier GPO combines technology scanning with subject-matter expertise to check all your systems and processes and then provides comparison on where you believe your security posture to be versus where it actually is.

Deliverables are supplied with a high level of detail to point you to the precise spot in your environment requiring attention, and direct recommendations are actionable in order to attain compliance quickly. Some of the things we look at include:

- Physical environment (policies and procedures)
- Users (security, access management, password controls)
- Servers and local computers (anti-malware, encryption)
- Firewall (rulesets, policies and procedures, anti-virus, external vulnerability scans)
- Email
- Wireless (access authorization, policies and procedures, termination procedures)
- Business associates (agreements with all required service providers, cloud providers)

Example Deliverable



collective

HIPAA Risk Analysis
HIPAA ASSESSMENT

Issues Summary

This section contains a summary of issues detected during the HIPAA Assessment process and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

Overall Weighted Issue Score

Current 305448

Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	Non-administrative generic logons have access to Network Share on system with ePHI (85 pts each)
172380	***Current Score:*** 85 pts x 2028 = 172380: 56.44%
	Requirement: §164.308(A)(3) Standard Workforce Security - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
	Issue: Generic accounts which could be in use by multiple people cannot be properly restricted and should not have access to network shares with ePHI.
	Recommendation: Remove access to Network Shares on systems with ePHI.
	User marked as not requiring ePHI login detected on computer containing ePHI (87 pts each)
62901	***Current Score:*** 87 pts x 723 = 62901: 20.59%
	Requirement: §164.308(A)(3) Standard Workforce Security - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
	Issue: One more users who are marked as not requiring ePHI have been detected as attempting to or logging into a system that contains ePHI.

Why choose Collective?

Expertise in healthcare IT:

Cybersecurity
Database admin.
Data storage
Data migration
Windows
UNIX/Linux
Virtualization
Networking
Cloud
HIPAA

Extensive history with IT clients:

Ohio Co. Healthcare
Johnson & Johnson
TX Children's Hospital
Molina Healthcare
Weill Cornell Medicine
BlueCross BlueShield
Fresenius
Medline
MultiCare
Carevide
Bio-Rad
VisionWeb
Citi
eBay
Yahoo
MGM
WAMU
FedEx