HIPAA Compliance Solutions

for Premier GPO Members

Cybersecurity for Healthcare

An organization's most important asset, after its own employees, is its information. Protection of this asset against unauthorized access or attack (cybersecurity) is always important for an organization—but it happens to be legally mandated for healthcare-related organizations that create, receive, maintain, store, or transmit PHI. HIPAA has specific privacy, security, and breach notification rules governing the proper protection of PHI—including rules for assessment, backup, and training.

Contact

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

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

Expert PHI Protection

Secure your data, avoid fines and penalties

Collective Group offers a comprehensive cybersecurity program tailored to the specific needs of Premier GPO member's team environments, assist them and their business associates with HIPAA compliance:

- Security Risk Assessments
- Privacy Program Assessments
- Data Protection Assessments
- HIPAA training and phishing testing to ensure malware resistance
- HIPAA Compliance as a Service

Whether working with you on a regular basis to perform assessments or running them automatically and remotely, we will bring to your organization **the qualities of Collective—meticulous, timely, trustworthy.**

Why choose Collective?

Expertise in healthcare IT:

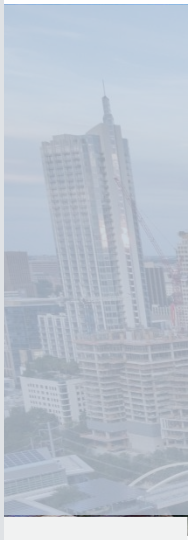
Cybersecurity	UNIX/Linux	Cloud
Database admin.	Virtualization	Windows
Data storage	Networking	HIPAA
Data migration		

Extensive history with IT clients:

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

Proven success stats:

99.987%	average client backup success rate
100%	client restore success
$0	paid by clients to ransomware attackers
27	years of industry experience
7	million hours of IT services delivered



Service Options

HIPAA Compliance Assessment | *Know where you stand*

As a Premier GPO member, you know that regular assessments must be made of your security policies and procedures. A good practice is to perform them annually—biennially at the least—to rapidly identify changes in technology, infrastructure, or posture, as well as to demonstrate to regulators that your organization takes HIPAA compliance seriously. Our Security Risk Assessment and Privacy Program Assessment services cover all six content areas required by HIPAA to be assessed regularly. Applying one of these services in your organization will supply detailed identification of the HIPAA-specific areas needing attention, as well as detailed remediation steps that can be taken. Combining them delivers the tracking mechanisms for remediation as evidence of maintaining compliance and/or working to be fully in compliance.

Data Protection Assessment | *Be confident in your data protection*

Electronic record-keeping in the healthcare industry has reduced costs for providers and has streamlined record access for patients and providers alike. The evolution to electronic healthcare records, though, has made the protection of these data from theft, damage, or loss even more critical. The Collective Data Protection Assessment takes an in-depth look at the configuration of your data protection program to ensure that you don't just have a data backup program in place—but that all your ePHI is protected sufficiently so that you can create and maintain retrievable exact copies of ePHI on demand. We will pinpoint places in your environment where gaps in protection may exist and will provide actionable plans for closing those gaps—ensuring that all data are optimally protected.

Training and Malware Resistance | *Make your workforce a data barrier*

Across industries, employees are the primary source of hacker access to data—phishing attacks that introduce ransomware and viruses get more efficient and sophisticated every day. To prevent this type of exposure in healthcare, Collective Group offers a "white hat" service, in which we evaluate the fortitude of your team members against phishing scams and then engage them in customized training when they mistakenly submit to a scam. These tests and any necessary follow-up training sessions are tracked and documented for easy addition to other HIPAA security documentation.

HIPAA Compliance as a Service (CaaS) | *Automate your compliance and security*

HIPAA compliance is not a one-time event, but regular checks don't need to be so cumbersome and consuming. HIPAA CaaS supplies you with technology to run the same tools that run during an assessment—but in an automated and low-impact way. These automatic events are analyzed, and any issue of noncompliance is documented and resolved, after which another automatic network and data-gathering process verifies its new compliance. Instead of waiting for your next scheduled assessment to find gaps in protection—and possibly experiencing an unintended disclosure or breach—HIPAA CaaS supplies constant compliance and gap detection as close to real time as possible.

What's at stake for healthcare organizations?

Health and Human Services Office of Civil Rights (OCR)

OCR has the authority to audit all entities covered under HIPAA to ensure their compliance—both after breaches that have occurred and randomly as OCR deems appropriate. Noncompliance can carry steep fines if OCR determines breaches to have been caused by negligence or chronic rule violations. In 2020, OCR cited each violator as failing to conduct enterprise-wide risk analysis, failing to implement risk management, or insufficient controls.

OCR-mandated fines

$107.5 million	=	2015–2020 total
$16.8 million	=	highest ever imposed on an entity
$13.5 million	=	2020 total
$6.8 million	=	highest in 2020
$3500	=	lowest in 2020

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