

HPH Cybersecurity Performance Goals (CPGs)



Compliance Manager GRC now includes built-in support for the Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs). A set of actionable, baseline security objectives, the HPH CPGs are designed to strengthen cyber resilience across the healthcare and public health (HPH) sector. Compliance Manager GRC includes integrated controls and features that make it easy for MSPs and MSSPs to support, implement and report on these essential safeguards for their healthcare clients.



What are the HPH Cybersecurity Performance Goals?

The HPH CPG represent a cybersecurity framework created by the U.S. Department of Health and Human Services (HHS) in collaboration with the U.S. Cybersecurity and Infrastructure Security Agency (CISA). The framework is designed to help HPH organizations prioritize essential security practices to improve cyber resilience, especially against ransomware, phishing and data theft.

Unlike general-purpose frameworks, the HPH CPGs are:

- Sector-specific: Built to address the real-world threats faced by hospitals, clinics and public health entities.
- Risk-informed: Focused on actions that offer the most impact for the least complexity.
- Scalable: Organized into essential and enhanced tiers based on organizational size and risk exposure.



Why MSPs should care.

Healthcare is one of the most frequently targeted sectors for cyberattacks, and it faces some of the strictest regulatory scrutiny. The HPH CPGs provide a predefined roadmap that MSPs can use to help healthcare clients:

- Prioritize the right safeguards
- Prove due diligence to insurers, regulators and boards
- Prepare for HIPAA and other compliance audits
- Reduce operational, legal and reputational risk

With Compliance Manager GRC, you can easily deliver this new service without adding complexity to your stack.



Who should follow the HPH CPGs?

The framework is designed for any organization operating in or supporting the healthcare sector, including:

- Private practices and clinics
- Regional and community hospitals
- Public health departments
- Health IT vendors and business associates
- Long-term care and behavioral health providers



HPH CPG Structure

The HPH CPGs are built around a set of practical, high-impact security outcomes tailored to the healthcare sector. Each goal is categorized as either Essential (the baseline protections that all HPH entities should implement) or Enhanced (for organizations with more complex risk profiles or resources).

Here are some of the Essential CPGs included in Compliance Manager GRC:

Requirement	Description
Mitigate known vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks accessible from the internet.
Email security	Reduce risk from common email-based threats, such as spoofing, phishing and fraud.
Multifactor authentication	Add a critical, additional layer of security to protect systems and accounts accessible from the internet.
Basic cybersecurity training	Ensure organizational users learn and perform more secure behaviors to reduce human error and increase awareness.
Strong encryption	Deploy encryption to maintain the confidentiality and integrity of sensitive data across both IT and OT systems.
Revoke credentials for departing personnel	Prevent unauthorized access by ensuring access for former employees, contractors and volunteers is revoked promptly.
Basic incident planning and preparedness	Enable the organization to respond effectively to, and recover from, significant cybersecurity incidents.
Unique credentials	Use unique credentials to help detect anomalous activity and prevent lateral movement by attackers within and across IT and OT networks.
Separate user and privileged accounts	Establish secondary privileged accounts to prevent escalation of access if common user credentials are compromised.

These goals are not abstract. They're actionable controls that MSPs can directly support, implement and report against using Compliance Manager GRC.



How Compliance Manager GRC streamlines CPG implementation



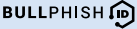

You don't need to be a healthcare compliance expert to deliver high-quality HPH CPG services. With Compliance Manager GRC, everything is prebuilt and ready to go:

- Quick assessments: Evaluate where clients stand across all CPG categories in less than 30 minutes.
- Technical risk assessments: Use built-in tools and Kaseya integrations to gather device-level evidence, verify configurations, and document enforcement of controls.
- Automated POA&MS: Turn assessment findings into a plan of action & milestones (POA&MS) with due dates, risk levels and task ownership.
- Evidence of compliance storage: Capture logs, screenshots, policy documents and other artifacts all in one place.
- Built-in policy templates: Generate and distribute security policies aligned to the CPG goals ready for signatures and audits.
- Progress tracking and reporting: Monitor improvements over time and demonstrate progress to stakeholders or regulators with one-click reporting.



Integrations that empower your service delivery

Compliance Manager GRC works seamlessly with other tools in the Kaseya ecosystem. Here are just a few:

	Document system roles, vendors and IT assets as part of the Identify category
	Import internal and external vulnerability scans for evidence of compliance
	Launch end-user training campaigns aligned to Protect goals
	POA&M tasks to your ticketing system for execution and tracking



Unlock value for you and your clients

Compliance Manager GRC equips you with the tools you need to uncover new business opportunities and help your clients strengthen their security posture with assessments aligned to the HPH CPG.

As an MSP or MSSP, HPH CPG assessments help you:

- Launch new vCISO services aligned with a federal security framework
- Offer meaningful add-ons to existing HIPAA or endpoint security packages
- Stand out in competitive RFPs and renewals
- Proactively prepare clients for regulatory scrutiny and insurance underwriting

For clients, it means:

- A clear cybersecurity roadmap
- Visibility into cyber risks
- Alignment with federal guidance
- Faster recovery from potential attacks

Affordable. Powerful. Purpose-built for you.

Compliance Manager GRC brings together the robust capabilities of enterprise-grade GRC platforms with the simplicity and affordability MSPs demand. It's the only solution built from the ground up to make compliance deliverable as a managed service. With Compliance Manager GRC, you get everything you need to help clients meet industry standards, strengthen their security posture, grow your revenue and reduce your liability with ease.

Schedule your demo today to see how quickly you can deliver risk-aligned, auditor-ready healthcare security assessments with Compliance Manager GRC.

[Request a demo](#)