[Solution Brief]

Protecting Patient Data, Ensuring Compliance, and Strengthening Cyber Resilience in Healthcare

OVERVIEW

Cybercriminals are increasingly targeting sensitive health information, while regulatory bodies continue to impose stricter guidelines to safeguard electronic Protected Health Information (ePHI). Without a proactive security strategy, healthcare providers risk severe financial penalties, reputational damage, and disruptions to patient care.

> *"Healthcare organizations must take a proactive approach to cybersecurity, managing compliance and regulatory burden while strengthening defenses before vulnerabilities are exploited."*
>
> – Jaike Hornreich
> Managing Director, Cybersecurity and Risk Management

CHALLENGES

Healthcare organizations must navigate a complex cybersecurity environment where patient data is a prime target for cybercriminals, facing increasing risks driven by:

- **Sophisticated Cyber Threats:** Targeted attacks on sensitive patient data are becoming more frequent and advanced.
- **Regulatory Pressure:** Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is mandatory, with steep penalties for violations.
- **Service Disruption Risks:** Cyberattacks can halt operations, impacting patient care and organizational reputation.
- **Complex IT Systems:** Integrating electronic health records (EHRs), Internet of Medical Things (IoMT), and hybrid environments increases vulnerabilities.

THE COST OF INACTION

The U.S. Department of Health and Human Services (HHS) imposes significant fines for HIPAA violations based on the level of culpability, with a maximum annual cap of $2,134,831 per violation (which multiple can occur in any given situation).

Violation Tier	Description	Minimum Penalty per Violation	Maximum Penalty per Violation
Tier 1	Unawareness of violation; would not have known with reasonable diligence.	$141	$71,162
Tier 2	Reasonable cause; not due to willful neglect.	$1,424	$71,162
Tier 3	Willful neglect; corrected within 30 days.	$14,232	$71,162
Tier 4	Willful neglect; not corrected within 30 days.	$71,162	$2,134,831

CASE IN POINT: PLASTIC SURGERY ASSOCIATES OF SOUTH DAKOTA

In 2017, Plastic Surgery Associates of South Dakota faced a ransomware attack compromising PHI of 10,229 patients. HHS identified HIPAA violations, including insufficient risk analysis and safeguards. The organization settled for $500,000 and implemented a corrective action plan involving risk analysis, risk management, and updated breach notification policies.

The increasing sophistication of threats, coupled with stringent regulatory requirements and the operational risks of service disruptions, makes it critical for healthcare providers to adopt a proactive security strategy. As IT ecosystems grow more interconnected with electronic health records (EHRs), Internet of Medical Things (IoMT), and hybrid infrastructures, organizations must strengthen their defenses to protect sensitive information, ensure compliance, and safeguard patient trust.

SOLUTION: SDG HEALTHCARE SECURITY ADVISORY PROGRAM

The SDG Healthcare Security Advisory Program is a structured cybersecurity and compliance program tailored to healthcare organizations. Whether you're a small clinic or a multi-region network, this program helps you:

- **Manage Risk Proactively:** Identify vulnerabilities and address them before they are exploited.
- **Ensure Compliance:** Align operations with HIPAA and other regulatory standards.
- **Build Resilience:** Prepare for and recover quickly from cyber incidents.
- **Evolve Continuously:** Adapt to new threats and industry advancements.

SDG Health Care Security Advisory: Service Details

HIPAA Security Risk Assessment

Purpose: Evaluate adherence to HIPAA Security Rule requirements.

Deliverables:

- Comprehensive risk assessment report.
- Compliance gap analysis.
- Prioritized remediation recommendations.

Network Security Assessment

Purpose: Identify vulnerabilities in your IT infrastructure and ensure robust network segmentation.

Deliverables:

- Vulnerability scan results.
- Segmentation validation report.
- Penetration testing findings (if applicable), with actionable steps.

Policy & Procedure Review

Purpose: Align organizational policies with regulatory requirements and cybersecurity best practices.

Deliverables:

- Precise updates required of security policies and procedures.
- Compliance gap matrix.

Optional Add-Ons

- **Third-Party Risk Assessment:** Evaluate vendor compliance and manage external risks.
- **Microsegmentation:** Advanced testing to isolate sensitive data and limit threat exposure.
- **Tabletop Exercises:** Simulated scenarios to test and refine incident response plans.
- **Ransomware Readiness Review:** Assess preparedness to prevent, detect, and respond to ransomware threats.

WHY SDG?

Choosing SDG's Healthcare Security Advisory Program means partnering with a team that understands the unique cybersecurity challenges facing healthcare organizations. With 30+ years of deep expertise in regulatory compliance, risk management, and cutting-edge security solutions, SDG helps you stay ahead of cyber threats while ensuring HIPAA and industry compliance. Our proactive approach identifies vulnerabilities before they become breaches, safeguarding patient data, minimizing operational disruptions, and protecting your organization's reputation.

- **Healthcare Expertise:** Designed specifically to address the unique challenges of healthcare organizations.
- **Tailored Solutions:** Customizable to your size, complexity, and budget – including bespoke efforts.
- **Actionable Insights:** Clear, prioritized recommendations for immediate and strategic improvements.
- **Trusted Professionals:** Certified experts with a proven track record in cybersecurity and compliance.

CONCLUSION

In an era where cyber threats are becoming increasingly sophisticated and regulatory pressures continue to rise, healthcare organizations cannot afford to take a reactive approach to cybersecurity. SDG's Healthcare Security Advisory Program provides the expertise, tailored solutions, and proactive strategies needed to safeguard patient data, ensure compliance, and strengthen cyber resilience.

By partnering with SDG, your organization gains a trusted advisor with a deep understanding of healthcare security challenges and a commitment to delivering actionable insights and long-term protection. Don't wait for a breach to expose vulnerabilities—take control of your cybersecurity strategy today with SDG.

ABOUT SDG

With more than 30 years of experience partnering with global brands on complex business and IT challenges, SDG is a proven leader in advisory, transformation, and managed services that enable leaders to confidently execute AI, identity, threat, and risk management solutions that protect assets and provide business value. To learn how SDG can help your organization, visit sdgc.com or call us at +1 (203) 866.8886.

For more information on SDG's Healthcare Security Advisory Program, please contact us today at +1 (203) 866-8886 or email us at solutions@sdgc.com.

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com