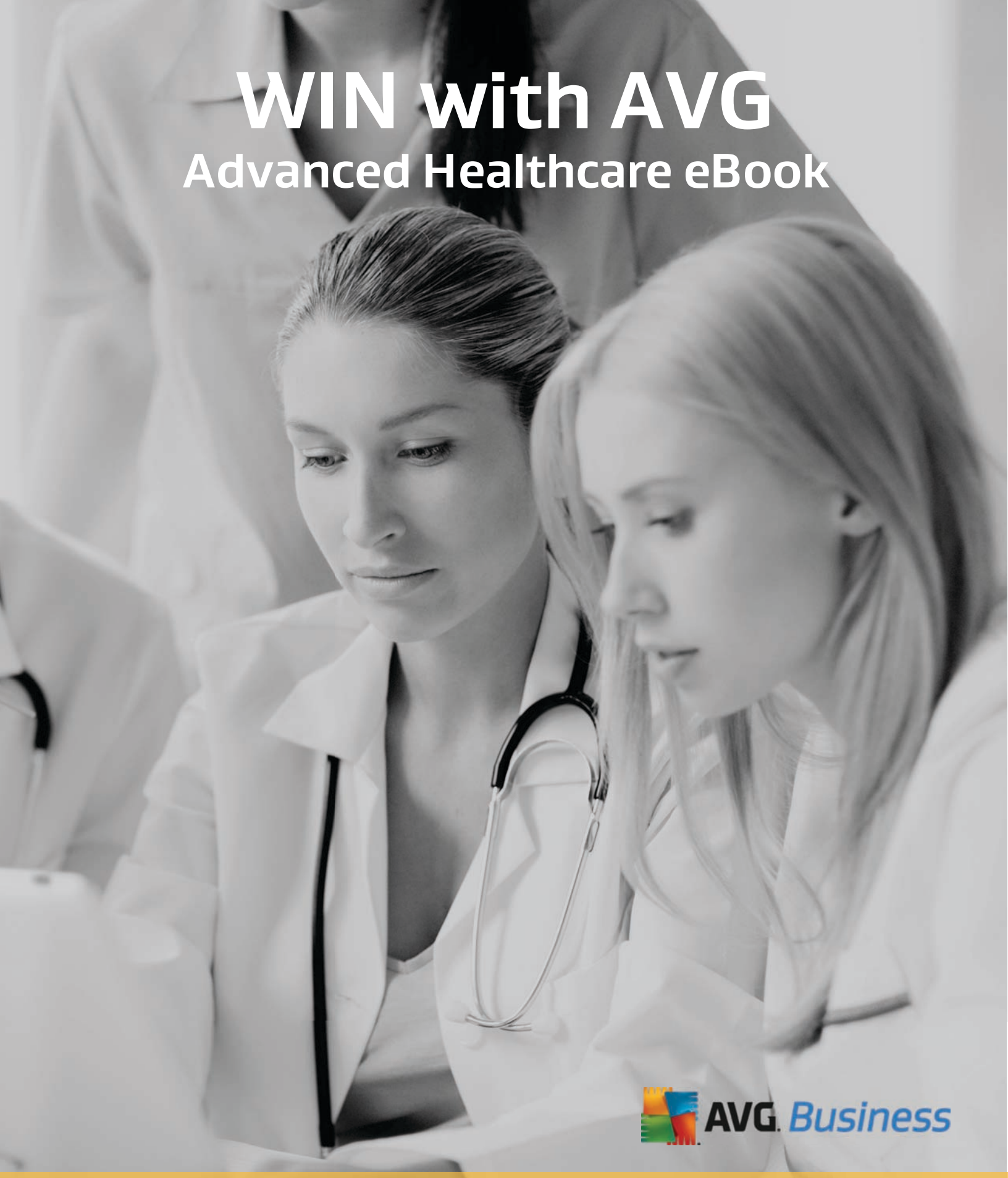
WIN with AVG

Advanced Healthcare eBook



AVG Business

Comprehensive Healthcare Compliance eBook

Table of Contents

AVG Business

Introduction

A significant opportunity for MSPs exists to help maximize profit and grow business.

Healthcare professionals from private practices and hospitals to pharmacies and insurers are becoming increasingly dependent on IT experts to help meet the stringent compliant requirements of the Health Insurance Portability and Accountability Act (HIPAA) as currently enforced by the U.S. Department of Health & Human Services.

To keep up with overwhelming demands of growth, the healthcare industry needs innovative IT solutions to simplify the procedures associated with HIPAA compliance.

AVG can help strengthen your position in the marketplace with high-performance tools that address security, privacy and data breaches.

This guide will serve as an intuitive tool to provide insight into medical compliance issues and AVG solutions geared specifically to help you generate profit for your MSP business.

HIPPA – A Robust Opportunity for Your Business

"Many HIPPA standards require technical solutions. A company can't become compliant with HIPAA without the technology necessary to meet the requirements."

- Gene Geiger, Partner, A-lign, Compliance Solutions Specialists

Since 2000, the U.S. senior population has increased 29% vs. compared to overall population growth of 12% (Forbes Business, Oct 30, 2014). Meeting the increased medical needs of this age group has prompted unprecedented growth in the medical industry. Adding to the surge is a trend of consumers who put off medical treatment during the economic downturn now seeking care. The Bureau of Labor Statistics has projected healthcare as the fastest growing industry overall through 2022.

AVG can help strengthen your position in the marketplace with high-performance tools that address security, privacy and data breaches.

Gartner forecasts that spending by global healthcare providers for IT services will grow by 5.04% to reach $32.16 billion in 2014.

AVG Business

The Demands of HIPAA Compliance

HIPAA is complicated!

In its simplest form, HIPAA compliance requires that all patient data from creation and storage to maintenance be transmitted electronically. This is referred to as electronic protected health information (ePhi) and should ideally occur through the entire lifecycle from the time data is gathered to recording and storage.

Maintaining compliance is a rigorous process and requires ongoing efforts to stay current with regulations and ahead of security challenges. HIPAA requires that specific criteria is met for:

- **Privacy** – Protection of disclosure and the way information is used
- **Security** – Maintaining integrity and confidentiality
- **Data Breaches** – Prevention and communication in the event of a breach

HIPPA requires proof that compliance processes have been clearly defined, instituted and followed.

Compliance expert Geiger explains the need for stringent regulation. The threat of a data breach is real.

"The value of patient data continues to rise. Healthcare information is more valuable on the black market than credit card info."

AVG Business

Who Must Comply?

HIPAA's security rules apply to all Covered Entities (health care and health plan providers and clearinghouses) that electronically transmit health care data.

With changes in the Omnibus Rule of 2013, any person or organization with access to health care information while doing business with a Covered Entity is considered a Business Associate and must adhere to HIPAA security requirements.

MSPs must comply with HIPAA regulations for securing data.

Some studies have shown that Business Associates are being held accountable for almost as many compliance breaches as Covered Entities.

Many MSPs miss out on this tremendous revenue generating opportunity healthcare represents due to liability relating to HIPPA regulations and their business. Savvy MSPs partner with leading technology firms like AVG to provide solutions that enable their healthcare clients, and the businesses supporting them, to achieve HIPAA compliance.

Noncompliance – What's at Risk?

There's a huge fear factor associated with HIPAA and for a good reason.

The consequences for noncompliance are staggering, especially for repeated violations or willful neglect. Fines totaling up to $1.5M per year can be imposed and professional reputations can be damaged beyond repair. Between 2009-2013, with roughly 30% of HIPAA compliance violations resulting in fines, the OCR imposed penalties totaling almost $26M.

Penalties up to $1.5 million per year for HIPAA non-compliance

The Office of Civil Rights (OCR) reports that the most common compliance violations are:

- Impermissable uses and disclosures of protected health information
- Lack of safeguards to secure protected health care information
- Lack of administrative safeguards of electronic protected health care information

According to the OCR, most cases have been resolved by requiring that privacy practices are followed by non-compliant healthcare entities. Penalties can be avoided by ensuring that healthcare entities remain compliant as monitored by appropriate audit and inventory reports.

AVG Business

Noncompliance – What's at Risk?

Four Components of HIPAA Compliance:

- **Administrative Safeguards** – Security management process implementation, security personnel designation, information access management, workforce training & management, and periodic evaluation of all processes and procedures.
- **Physical Safeguards** – Access control, integrity controls, transmission security.
- **Technical Safeguards** – Access control, integrity controls, transmission security.
- **Organizational Requirements** – Specific criteria for contracts and other arrangements between Covered Entities and Business Associates regarding protection of ePhi and breach management.

The technical safeguards required by HIPAA compliance are likely familiar to most MSPs. AVG is uniquely positioned to support you in providing HIPAA-compliant solutions.

Become an MSP Hero in HIPAA Compliance

So, what does this means for MSPs?

HIPAA violations occur every day, yet most can be avoided with the right IT infrastructure implemented, maintained and monitored.

Your role as an MSP is to help improve your healthcare clients' HIPAA compliance efforts. The proper security, assessment and reporting tools can help prevent security breaches and provide proof of compliance.

AVG empowers MSPs to implement and support HIPAA compliant networks by providing products and solutions to address each area of compliance.

Client Reviews

Managed Workplace

Beyond the powerful tools of remote monitoring and management, Managed Workplace offers HIPAA related reports and integrated security solutions.

> "Passwords have proven to be a weak leak in the security infrastructure. SSO strengthens this link by requiring multi-factor authentication and mobile device management. It also simplifies the 'bring your own device' issue"

Backup and Disaster Recovery

Provide clients a single comprehensive solution for the backup, archive and disaster recovery of critical and protected data.

> "HIPAA requires that access to ePHI be maintained in the event of a disaster or disruption in service. A critical step to this requirement is to replicate the data through an offsite storage location"

Single Sign On (SSO)

With centralized control of cloud and mobile apps, one-click authentication of end user and password management capabilities, AVG Business SSO simplifies a company's ability to control and protect confidential data.

> "Managed Workplace is a comprehensive solution to meeting multiple requirements within HIPAA. In addition to increasing efficiency of network management, it layers in the security necessary for compliance."

Managed AntiVirus

With centralized control of cloud and mobile apps, one-click authentication of end user and password management capabilities, AVG Business SSO simplifies a company's ability to control and protect confidential data.

> "Managed Workplace is a comprehensive solution to meeting multiple requirements within HIPAA. In addition to increasing efficiency of network management, it layers in the security necessary for compliance."

All comments above by Gene Geiger

AVG Business

HIPAA Security Standards

HIPPA Citation	HIPPA Security Rule Standard Implementation Specification	Managed Workplace	Single Sign On (SSO)	AntiVirus	Online Backup	Backup & Disaster Recovery	Other (please specify)
164.312(a)(1)	**Access Control** - Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 146.308 (a)(4) [Information Access Management].	✓	✓				
164.312(a)(2)(i)	**Unique User Identification** - Assign a unique name and/or number for identifying and tracking user identity.		✓				
164.312(a)(2)(ii)	**Emergency Access Procedure** - Establish procedures for obtaining necessary electronic protected health information during an emergency.		✓				
164.312(a)(2)(iii)	**Automatic Logoff** - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	✓					
164.312(a)(2)(iv)	**Encryption and Decryption** - Implement procedures that specify a mechanism to encrypt and decrypt ePHI.	✓					
164.312(b)	**Audit Controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	✓					
164.312(c)(1)	**Integrity** - Implement policies and procedures to protect ePHI from improper alteration or destruction.						
164.312(c)(2)	**Mechanism to Authenticate Electronic Protected Health Information** - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.						
164.312(d)	**Person or Entity Authentication** - Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.		✓				
164.312(e)(1)	**Transmission Security** - Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	✓				✓	
164.312(e)(2)(i)	**Integrity Controls** - Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.						
164.312(e)(2)(ii)	**Encryption** - Implement a mechanism to encrypt ePHI whenever deemed appropriate.	✓				✓	

AVG Business

Conclusion

The healthcare market is primed for MSPs prepared to facilitate the challenges of HIPAA compliance.
Learn more about how AVG can power your profitability with specialized solutions, support and expertise.
Partnering with AVG is a win for you and your clients.

AVG Business