



HIPAA Data Security Compliance Services

In the Past Five Years, Few Industries have undergone a more dramatic change in the nature of their compliance and monitoring activities than healthcare providers,

Under HIPAA, Covered Entities must develop and implement policies and procedures for authorizing Electronic Protected Health Information (EPHI). Of utmost concern is the number of security breaches that have occurred due to the use of portable media, such as USB flash drives, and the use of laptop computers, PDA's, home computers and other storage devices outside of the organization's physical domain. The review of these policies and procedures generally occurs on an annual basis in order to comply with the HIPAA Security Rule.

ALP-Consulting is a professional IT auditing & security firm. Our auditors have a diverse background that provides the experience necessary to ensure coverage of your key HIPAA compliance areas, including those you might not have experience with:

- ◆ Protection of Logon Passwords
- ◆ Controls Over EPHI Data Access
- ◆ Remote Workstation Termination
- ◆ Viruses, Malware & Spyware
- ◆ Laptop Data Encryption/Storage
- ◆ Use of Portable Data Storage Devices
- ◆ Use of Wireless Networks
- ◆ Transmission Standards for EPHI Data
- ◆ Non ISO 17799 Compliance Techniques

Areas of Compliance

1. Protection of Logon Passwords

- Password encryption
- Unique login identifiers
- Strong Passwords; Frequent Rotation; Single-User,Single-Login Protocol

2. Controls Over EPHI Data Access

To be compliant, health plan providers MUST disclose only the minimum information necessary. We review and test your procedures, including user profiles, activity logging, and audit trails

3. Remote Workstation Termination

We evaluate compliance with HIPAA's workstation timeout requirements, password-protected screensavers, and other security measures.

4. Viruses, Malware & Spyware

We evaluate the use of firewalls, anti-spyware protection, port restrictions and other techniques designed to minimize disruption from viruses and spyware.

5. Laptop Security & Data Encryption/Storage

Laptops must be secure from theft and two factor authentication and hard drive encryption are recommended. EPHI Data stored on and transmitted from laptops must be encrypted.

6. Use of Portable Data Storage Devices

Portable storage devices should be eliminated to the extent possible. We ensure you have a policy in place, evaluate its appropriateness, enforceability and the extent to which it is followed.

7. Use of Wireless Networks

We evaluate the use of wireless networks to transmit EPHI data, complete penetration tests of access points, look for VPN connections between remote workstations and central host, and data encryption

8. Transmission Standards for EPHI Data

Do policies and procedures require encryption and decryption of transmitted EPHI data and are the policies being followed. Are the minimum number of individuals provided with EPHI data? Are networks over which data is transmitted secure?

9. Non ISO 17799 Compliance Techniques

ISO 17799 can be used as a framework for HIPAA compliance, but other methods are also available. Complying with ISO 17799 is difficult unless you have an automated system and are constantly monitoring changes. We identify best practices for information security and HIPAA compliance, without requiring strict adherence to ISO 17799, saving you time and money, without compromising any sensitive HIPAA data.

THE ALP ADVANTAGE

- We ARE Network Security Experts - and Professional Hackers
- Extensive HIPAA Audit and Security Experience for both healthcare providers and third party insurers
- Knowledge of HIPAA's Security Standards and Practical Implementation Techniques to Ensure Compliance
- Extensive Knowledge of the Healthcare Industry
- Expertise in Establishing Comprehensive Strategies for Addressing Risk Mitigation, Regulatory Compliance, and Identifying Network Vulnerabilities

The IT Professionals Group

ALP-Consulting • Unlimited Technology Solutions (UniTech)

Partnership with Integrity

ALP TEAM KEYS TO YOUR SUCCESS

Assisted by ALP, co-sourcing will work for you. ALP can complete security reviews and conduct audits of highly technical and sensitive areas. Clients call on us when they need specialized expertise but cannot justify the permanent costs or are unable to meet peak demands

Led by IT and internal audit experts having CISA, CISSP, CIA, CPA, and other technically certified designations, our engagements are managed by individuals with more than fifteen years of IT security and audit experience

Professional IT audit capabilities set us apart. We've completed HIPAA IT & IT security compliance reviews for healthcare providers and 3rd party insurers.



HIPAA Security Compliance Services

ALP-CONSULTING

“The IT Auditing & Security Professionals”®



SOUTH BEND
(574) 532-9414

FORT WAYNE
(260) 399-6398

TOLL FREE
(877) 312-6547

Visit Our Web Page
<http://www.alp-consulting.net>

We help protect your most sensitive resources