

Health Insurance Portability and Accountability Act Compliance Report

Designated Official: _____

Time Period: 09:51:31 Thursday, July 07, 2005

What is HIPAA?

HIPAA stands for Health Insurance Portability and Accountability Act, which was passed by US Congress as an attempt at incremental healthcare reform. HIPAA stipulates the security standards and requirements for the maintenance and transmission of health information that identifies individual patients.

Which of the HIPAA Security Standards Final Rule applies to the wireless network?

Section 164.312, Technical Safeguards, of the HIPAA Security Standards Final Rule that went into effect on February 21, 2003 establishes the general guidelines to ensure the confidentiality, security and integrity of electronically stored and/or transmitted health information, and has a direct impact on wireless networks that

To whom does the HIPAA regulation apply?

The HIPAA Security Standards Final Rule applies to entities in the following four categories:

- Health Care Providers;
- Health Plans;
- Health Care Clearinghouses;
- System Vendors who provide computer software applications to health care providers and other billers of health care services.

What are the primary compliance obligations of a covered entity in

The Technical Safeguards of the HIPAA Security Standards Final Rule contains the following security requirements for wireless networks used to transmit PHI:

1. Access Control [§ 164.312 (a) (1)]: Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software applications that have been granted access.
2. Audit Control [§ 164.312 (b)]: Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.
3. Integrity [§ 164.312 (c) (1)]: Implement policies and procedures to protect electronic PHI from improper alteration or destruction during transit.
4. Person or Entity Authentication [§ 164.312 (d)]: Implement procedures to verify that a person or entity seeking access to electronic PHI is the party claimed.
5. Transmission Security [§ 164.312 (e) (1)]: Implement technical security measures to guard against

AirMagnet HIPAA Compliance Reports

The HIPAA Security Standards Final Rule requires that PHI transmitted over public networks be encrypted. Since wireless networks broadcast data over the air, they are a type of public network, and, therefore, must meet the encryption requirements in order to comply with HIPAA Security Standards Final Rule. This report details your wireless network policies in terms of encryption requirements for each access point. It also shows the security violations that have occurred within the specified time frame. The report is backed by AirWISE - AirMagnet's leading network analysis engine which is not only capable of automatically analyzing more than 40 unique security vulnerabilities and attacks on a constant and real-time basis, but also provides technical solutions (expert advice) for IT staff to tackle the identified issues.

1/ System Level Compliance Report

This report summarizes your network's overall compliance with the HIPAA Security Standards Final Rule on a per-policy basis.

HIPAA Security Standards Final Rule	Compliance %
"Audit Control [§ 164.312 (b)]: Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI."	100%

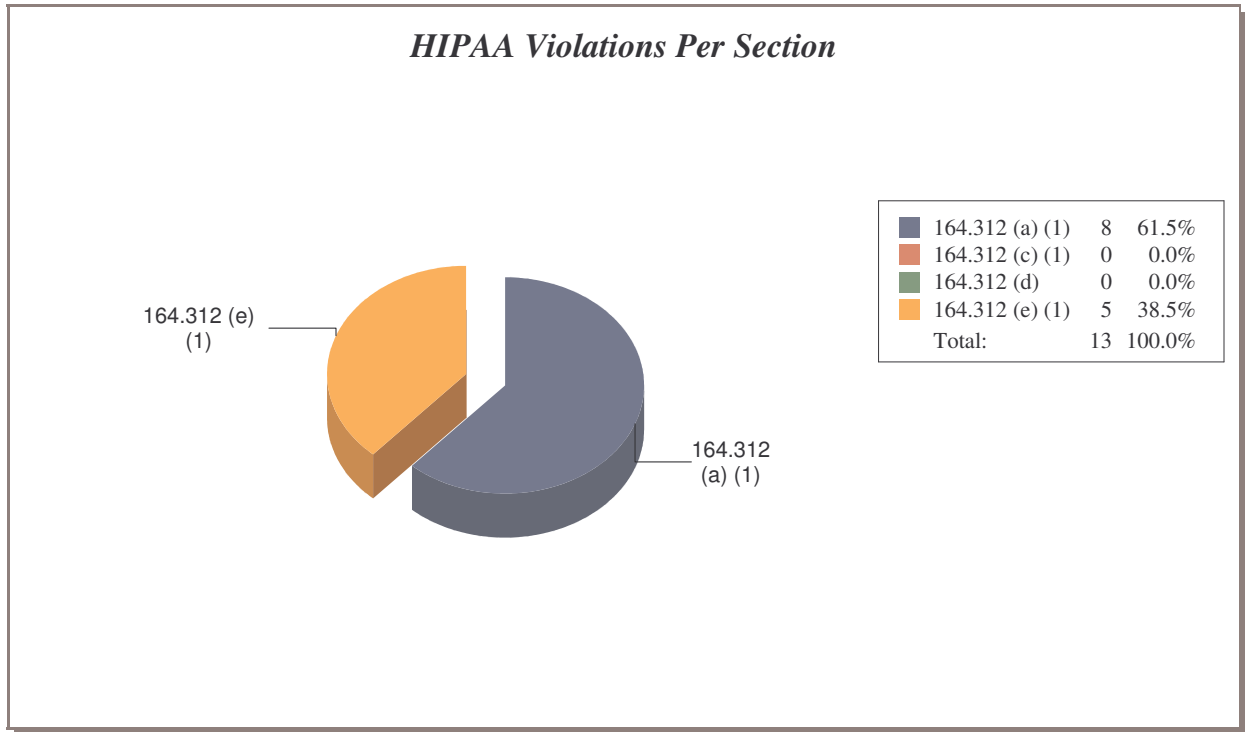
Notes:

Section 164.312 (b) Audit Control requires that wireless networks have auditing tools in place to provide early detection of intrusion to minimize damage. As the industry's leading IDS system, AirMagnet provides the most comprehensive intrusion detection. To comply with this HIPAA regulation, all AirMagnet alarms must be activated. De-activating any of AirMagnet's security alarms violates the Audit Control [§ 164.312 (b)].

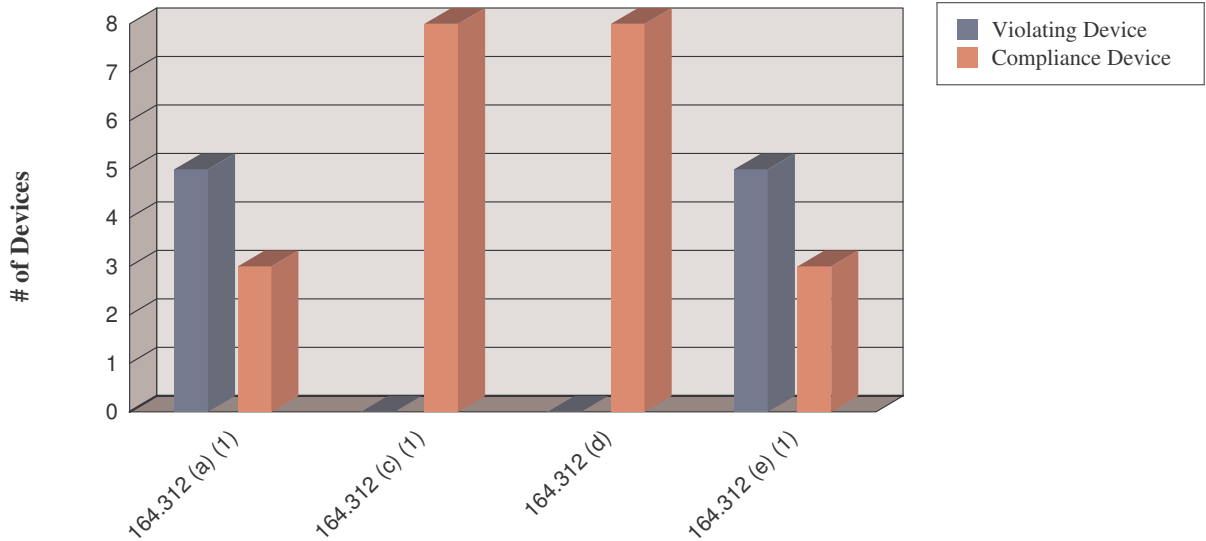


2/ Policy Level Compliance Report

This report summarizes your network's compliance on a per-policy basis, showing you the total number of devices that are in compliance or violation of each and every policy in the HIPAA Security Standards Final Rule.



HIPAA Violating/Compliant Devices Per Section



HIPAA Security Standards Final Rule	Policy Violation	# Violating Devices	# Compliance Devices	Compliance %
Access Control [§ 164.312 (a) (1)]: Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software applications that have been granted access.	8	5	3	37.50%
Integrity [§ 164.312 (c) (1)]: Implement policies and procedures to protect electronic PHI from improper alteration or destruction during transit.	0	0	8	100.00%
Person or Entity Authentication [§ 164.312 (d)]: Implement procedures to verify that a person or entity seeking access to electronic PHI is the party claimed.	0	0	8	100.00%
Transmission Security [§ 164.312 (e) (1)]: Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communication network.	5	5	3	37.50%

HIPAA Security Standards Final Rule			
AirMagnet Alarms	# Violating Devices	# Compliance Devices	Compliance Status
Access Control [§ 164.312 (a) (1)]: Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software applications that have been granted access.			
Rogue AP by MAC address (ACL)	3	5	62.50%
AP broadcasting SSID	5	3	37.50%
Transmission Security [§ 164.312 (e) (1)]: Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communication network.			
WEP IV key reused	1	7	87.50%
AP with encryption disabled	3	5	62.50%
Device unprotected by TKIP	1	7	87.50%

Notes:

- 1) By default, your network fails to comply with the Health Insurance Portability and Accountability Act (HIPAA) if one of the devices violates any of its policy sections.
- 2) Channel specific policy violations will not be included in the Device-Specific Compliance Report.

3/ Device-Specific Compliance Report

This report contains detailed information about devices in compliance or violation of HIPAA. It checks the devices against each and every provision in the Directive to show what policy provisions are violated or upheld to. It lists all wireless devices deployed on your WLAN.

Device Information	Policy Sections				Compliance %
MAC Address - Type Channel SSID Vendor	164.312 (a) (1)	164.312 (c) (1)	164.312 (d)	164.312 (e) (1)	
00:02:6F:20:B3:F7-a Channel 56 5354a	F	P	P	P	80.00%
00:02:6F:04:88:6A-b Channel 1 1d2d70	P	P	P	F	80.00%
00:0F:66:42:D2:B5-b Channel 11 kassandra	F	P	P	F	60.00%
00:02:6F:09:3E:2B-b Channel 1 1d2d70	F	P	P	F	60.00%
00:02:6F:20:B3:F8-b Channel 11 5354g	F	P	P	F	60.00%
00:02:6F:34:A1:59-b Channel 6 3054g	F	P	P	F	60.00%

Notes:

- 1) P = Pass; F = Fail
- 2) A device is considered to have failed to comply with HIPAA if it violates any of the policy provisions.



