



AirPatrol Case Study – US Multi-State Health Maintenance Organization

March 2009



www.airpatrolcorp.com

A Customer Profile

The customer used as the model for this report is one of the largest multi-regional HMOs in the United States. This HMO is headquartered in Pennsylvania, and employs more than 1,400 employees and comprises the largest multi-state Medical Assistance managed-care organization in the country, serving 6.2 million members nationwide.

The Issues

Common Risks to This Market

Unauthorized Use of Wireless Devices to Obtain Patient Confidential Information – Breach of HIPAA, Privacy Laws

An alarming number of incidents have occurred recently wherein wireless devices have been used in healthcare facilities to obtain PHI without the consent of patients.

http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

Breaches have included the taking of photographs with cellular phones - by patients, visitors and even healthcare facility employees - of patients, medical records and X-Rays. Some images were even posted on social Web sites.

With the sophistication of electronic devices, coupled with the storage and transmission by healthcare facilities of medical data by electronic means, PHI can be transmitted by calls, emails, electronic Instant Messaging or even texts. Without the proper surveillance, the cellular phone or Wi-Fi device holder may even gain wireless access to those records inadvertently or intentionally.

Regardless if a facility is completely wired, completely wireless or a combination of both, it is not safe from wireless intrusion without a wireless surveillance system in place. Because wireless technology does not require physical connectivity for data to be transferred, it effectively renders useless many of the conventional means that have traditionally been deployed to secure networks and information. As a result, sensitive data and proprietary networks have been left vulnerable to both internal breaches and external wireless attack. Such exposures could lead to breach of patient photographs, records and other PHI, as well as confidential information regarding the facility.

To protect mission-critical operations, facilities should choose to enforce no-wireless policies or to allow wireless in very limited areas. However, establishing policies without a means of enforcement is not sufficient to mitigate the security risks. To effectively enforce no-wireless policies and to prevent exposures, enterprises must be able to accurately detect and locate all popular cellular and Wi-Fi technologies, on all bands.

Rogue Access Points

When an eager employee - unaware of the dangers - connects an access point within their personal office space in order to facilitate mobility, he or she can open up a completely unrestricted entry point into a facility's wired network. Potentially more damaging can be the

rogue access point that is *intentionally* installed by any third party that temporarily has access to your facilities (think sanitation personnel, contractors, visitors, etc), giving anyone the ability to roam your wired network at will. To prevent these types of vulnerabilities, facilities simply must have reliable wireless intrusion detection systems in place, regardless of whether they have or do not have a wireless network installed.

Wireless Client Promiscuity

Most popular wireless clients and operating systems will continue to try and automatically connect to any wireless network to which they have been previously connected. Any third party can instantly establish a completely trusted connection to any wireless laptop in your organization, *simply by guessing the name of a wireless network they have connected to in the past!* This is known as **WiPhishing**. Once connected, numerous attacks against the laptop are possible, and even against the wired network if the attacker is knowledgeable enough to tunnel through the compromised laptop. These risks are present even if you have no wireless network within your organization. Any mobile device that has been used wirelessly outside of the facility is at risk of being WiPhished and compromising your network.

Intentional Circumvention of Network Controls

Users often find Network Controls (Internet usage monitoring, website filtering, email filtering and monitoring, network level antivirus/antispam filtering, etc) at best an inconvenience. Worst case, some users may consider these types of Network Controls something desirable to circumvent. Any available wireless connectivity option, such as the “free WiFi” signal floating in through the window, or the Cellular 3G network card in their brand new laptop, provide the unscrupulous employee trivially simple means to get around any Network Controls you have installed in your facility’s network. If these same employees have access to PHI, the risks can be extreme.

Viruses and Malware

Employees often ignore documented policies and best practices, including use of firewalls and antivirus protection either because they don’t understand the risks involved or perhaps just don’t care—favoring efficiency over security. When employees with mobile devices, which have been exposed to the Internet in the wild, return to the facility and connect an infected device to the network, they can inadvertently expose the network to malicious codes such as software viruses, Trojan horses or worms. To protect networks, enterprises must be able to secure the endpoints, enforce the presence of endpoint firewalls, and prevent the use of unauthorized devices within the corporate campus.

Insecure Wireless Networks

A wireless network is basically an implicitly trusted but typically insecure medium, just like the Internet. Unlike a wired network, where information travels through a network cable, a wireless network allows information to travel everywhere throughout a broad geographical area, where the information can be intercepted from the air *by anyone with a WiFi card in their laptop*. Employees who use open, unencrypted Wi-Fi access points and don’t use

encryption or Virtual Private Networks (VPNs), place corporate data at risk to numerous security exploits. The simple act of checking your email while sitting in your local coffee shop can potentially give anyone within listening range your email account's password! To protect sensitive data and meet compliance mandates, client policy enforcement software must be used to ensure that employees only connect to authorized types of Wi-Fi networks and force users to utilize adequate levels of security including VPN, encryption, and personal firewalls.

Interference with Hospital Equipment

Although it there have been mixed opinions regarding the potential interference of cellular phones and Wi-Fi devices with medical equipment, there exists a healthy argument against the use of such devices in the event interference does occur. The risk to the patient is simply too great to allow such devices to be used where medical equipment, electronic medical records, etc. are present. This is especially true in light of the fact that such devices should be banned to comply with HIPAA, state privacy laws, Sarbanes-Oxley, and other regulations. Simply putting up a sign instructing visitors to "please shut off your cellular phone" does not adequately mitigate these issues – reliable detection of these devices does.

Specific Concerns of This HMO

With the proliferation of wireless infrastructures everywhere, a major concern for this multi-regional HMO is to manage the connectivity resources of their laptops, thereby enhancing the security of their wireless LAN with an endpoint management solution.

Because this model health plan provider has several buildings located on major interstates, they are concerned about the threat caused by "WiPhishing" attacks from hackers sitting on the edge of the highway with an inexpensive wireless access point.

Within a matter of minutes, if one of the HMO's employees has ever used a WiFi connection at a hotspot using well-known wireless SSIDs, his laptop would automatically connect to that SSID, and an Attacker could easily access the confidential information on the laptop.

Without proper wireless threat management protection, healthcare organizations are in danger of violating key regulatory policies. In order to maintain compliance with laws such as the Health Insurance Portability and Accountability Act (HIPAA), and to avoid costly and embarrassing lawsuits resulting from loss of confidential patient or partner data, this HMO would require technology which could enforce its existing wireless security policy. It needs to be able to detect, locate and stop unauthorized cellular phone and other Wi-Fi device communications in order prevent breaches of established policies and regulations, as well as to maintain patient safety and a sound reputation for confidentiality.

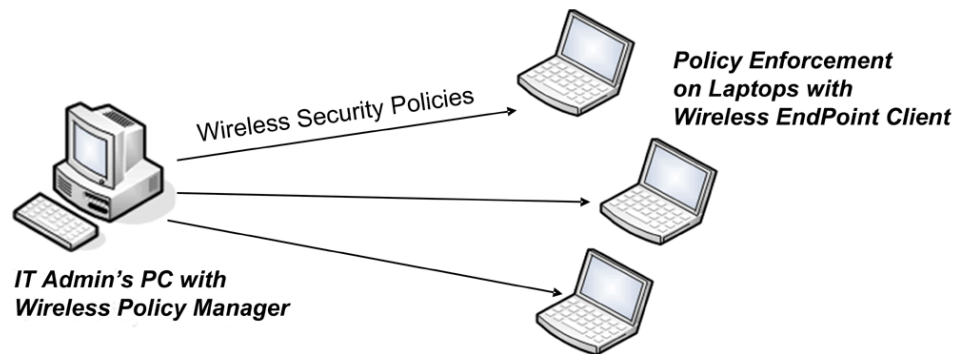
The Resolution

AirPatrol provides a solution that secures wireless endpoints and effectively removes WiPhishing threats.

Integrated Wireless Client / Policy Management

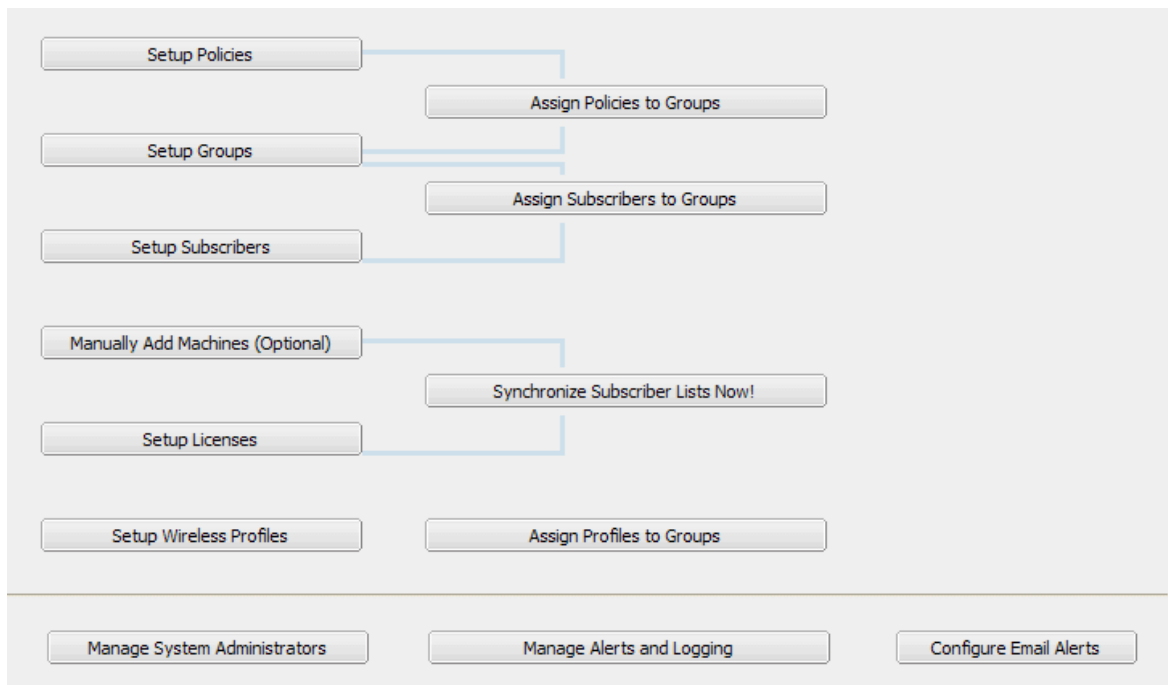
Wireless EndPoint Client (WEC) protects wireless endpoints against known and unknown threats without inhibiting users or slowing performance. It also simplifies the integration and implementation of wireless threat management into existing legacy wired security infrastructures by preventing dual-homing or routing from wireless interfaces through to a wired connection.

AirPatrol's **Wireless Policy Manager (WPM)** offers a comprehensive management interface for the centralized administration of all Endpoint Client policy configurations and an ability to push the policies on a dynamic basis to all managed laptop endpoints.



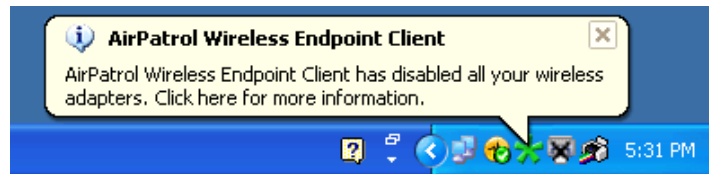
Centralized Wireless Policy Management

AirPatrol's **Wireless Policy Manager** allows Wireless Network Administrators to control how, when and if users can connect to wireless networks.



Prevent Wireless Intrusion & Hacking

To prevent wireless hacking at its source, Wireless EndPoint Client automatically turns off the wireless adapter whenever a laptop is connected to a wired network port.



This capability addresses the security deficiencies in standard Windows® XP and Vista wireless clients, and prevents WiPhishing attacks that enable a hacker to bridge the connection between a wireless laptop and the corporate wired network.

By enforcing the wireless connectivity policies defined using Wireless Policy Manager, Wireless EndPoint Client seamlessly protects business communications, critical information, and IT infrastructure. As a further precaution, Wireless EndPoint Client limits wireless connectivity to the office network whenever it is within range – completely eliminating the possibility of users connecting to a rogue access point or other non-sanctioned wireless networks while at work.

Cellular Card and Modem Control

Wireless EndPoint Client can also disable and enable a cellular card or modem whenever it detects wired or wireless connections. When the cellular card or modem is active, Wireless EndPoint Client will automatically disable the wireless adapter.

Control Connections with Location Aware

Using Location Aware, when a Wireless EndPoint Client is within range of one of corporate access points, it will only connect to that access point - not to any unknown access points which may also be in range. This prevents users from connecting to unknown outside access points whenever they are near the corporate wireless network.

Intelligent USB Device Management

USB is rapidly become the standard for all peripheral connectivity to PCs and laptops worldwide. In addition, one of the fastest growing exploits and modes of propagation for malware is USB flash drives. These cheap and easily obtainable devices also represent the most pervasive method of malware intrusion, but also information extrusion (see article in IT Business).

Summary

AirPatrol Corporation can assist healthcare facilities in complying with the strict industry regulatory requirements and privacy rules. With IT being integral to the electronic PHI, as well as to the financial accounting, tracking and reporting of financial information of facilities, it follows that a facility should ensure that it has a secure wireless threat management system in place.

As a centralized wireless network policy management system, AirPatrol's Wireless Policy Manager and Wireless EndPoint Client provide definitive assurance that your mobile workforce will remain safe, whether within your facilities or when removed from your

workplace. The AirPatrol solution allows your Wireless Network Administrator to take control of how, when, and where your workforce connects their mobile devices - dictating and enforcing safe practices, instead of leaving it up to the employee to decide what is safe.

About AirPatrol Corporation

As the most trusted authority on wireless threats to wired and wireless networks, AirPatrol Corporation delivers the security and network management capabilities today's businesses and government agencies require to solve the industry's most pressing wireless security and network management issues. By offering a comprehensive suite of wireless threat management solutions, AirPatrol enables entities to keep pace with the expanding requirements of a mobile world while complying with pertinent regulations and protecting communications, critical information, and IT infrastructure against present and future wireless threats. Customers and partners include leading network infrastructure and wireless vendors, Fortune 100 enterprises and high-profile government agencies around the globe.

For more information about the contents of this white paper, AirPatrol Corporation products or our company, please contact us at info@airpatrolcorp.com or call us at +1-866-430-4227.