Spyware Meets HIPAA
by Kate Borten, CISSP, CISM
# Table of Contents

- **Introduction** .................................................................................................................. 3
- **Spyware Mutates** ............................................................................................................ 4
- **Using HIPAA’s Security Rule as a Prescription to Fight Spyware** ................................. 5
- **About the Author** ............................................................................................................. 6
INTRODUCTION

The mission of healthcare has always been to combat disease and illness. In today’s world that mission extends to fighting electronic “diseases” that can threaten quality of care and privacy of patient information.

The Health Insurance Portability and Accountability Act (HIPAA) is broad federal legislation requiring, among other things, that healthcare providers and payers implement electronic safeguards to protect patient data confidentiality, integrity, and availability. Through HIPAA’s Security Rule healthcare organizations are instructed to identify and mitigate security threats and vulnerabilities. One type of threat recognized by the Security Rule is the threat of malicious software or malware. And one form of malware is spyware.

The Security Rule requires each organization to assess its risks and to take appropriate action. As risks such as spyware change and grow, healthcare organizations must constantly manage those risks to protect individually-identifiable health data from unauthorized disclosure and to ensure the data’s availability when needed. Hence, implementing an anti-spyware program is both good business practice and helps ensure regulatory compliance.
Once considered relatively benign, spyware has become increasingly invasive and damaging, presenting a serious challenge for healthcare providers and payers in today’s highly-networked world. Spyware prevention tactics have become a necessity across all organizations.

In its more benign forms spyware consumes large amounts of computer memory, directly impacting performance of workstations and, thus, users. In situations where patient care is dependent on rapid response, spyware can have troubling consequences for care delivery. In some circumstances slow response time can also lead to duplication of tests which adds to the cost of health care.


So how does spyware get onto a computer? Responding to spam email, being redirected to “bad” web sites with hidden code or web bugs, and downloading software containing hidden code or a Trojan horse are common ways that computers become infected. The CERT® Coordination Center at Carnegie Mellon University even reports that some web sites offer spyware detection tools that are actually spyware themselves.

Recovering from spyware drains technical staff productivity. Spyware is not likely to be removed through a convenient “uninstall” feature. Sometimes spyware is embedded in code a user intentionally downloaded such as a screen saver, so deleting the spyware also deletes the desired software. And spyware is often difficult to eliminate completely. Like trick birthday candles that reignite after being blown out, some spyware reinstalls itself even after it appears to have been removed.

Those are the visible effects of spyware, but what about the more subtle and potentially more dangerous risks? Spyware can result in the loss of all three of the prime components of information security: confidentiality, integrity, and availability. Spyware-related privacy and security breaches in the form of unauthorized disclosure of confidential data – personnel data, legal advice, business strategies, and Protected Health Information or PHI (as defined by HIPAA) of patients and health plan members – can lead to public embarrassment, lawsuits, and regulatory non-compliance penalties for the affected organization.

Spyware-related breach of patient confidentiality in a healthcare organization can seriously affect targeted patients as well. Such breaches can lead to embarrassment, mental anguish, job loss, financial loss, and even physical harm.

Furthermore, in a healthcare provider organization the spyware-related loss of PHI or access to it (the availability component of security), even temporarily, can affect the cost and quality of patient care, as can the loss of PHI integrity.
USING HIPAA’S SECURITY RULE AS A PRESCRIPTION TO FIGHT SPYWARE

With the advent of HIPAA, security is no longer an option for healthcare organizations. Instead, the questions today are related to how much security is enough and where to focus security efforts.

By law all PHI must be secured. Implicitly Covered Entities’ security programs must encompass their full electronic environment, not just PHI, since PHI systems are not isolated islands. It is also increasingly clear that individually identifiable non-healthcare data held by any type of organization, including healthcare providers and plans, should be protected from misuse for identity theft and financial fraud.

Organizations with the most effective security programs recognize the broad scope of the security challenge, and they routinely allocate resources for security infrastructure strategies such as widely-deployed network and desktop controls including anti-malware protections. HIPAA’s security rule provides several standards and implementation specifications that logically encompass anti-spyware strategies.

First, the security rule requires workstation use policy and procedures that “specify the proper functions to be performed.” Policies and network controls that limit the workforce’s use of the Internet, for example, by prohibiting access to known spyware sites, reduce the risk of malware infection. Policy and procedures requiring all new software to be approved before loading (downloaded from the Internet or introduced via physical media such as a CD) also reduce the risk. These policy points are often clustered together in a computer and network “acceptable use” policy for the workforce.

Second, the rule requires security incident policies and procedures “to address security incidents,” that is, to identify, respond to, and mitigate the harmful effects of security incidents – including malware attacks. Organizations should install anti-virus and anti-spyware software that can identify and deflect malware attacks. There should be processes for monitoring and updating the anti-malware software. And as part of the response and mitigation plan, there should be documented procedures for removal of malware including spyware.

Other sensible technical measures to reduce the risk of malware infection include hardening the workstation configuration, including the browser configuration, as well as promptly applying security patches to all networked devices.

Finally, HIPAA’s security rule requires workforce training on security. Workforce training programs should discuss acceptable and unacceptable uses of computers and the organization’s network, based on organization policy. To meet the implementation specification regarding protection from malware, training programs should describe the symptoms of an infected workstation; those might include newly persistent slowness and an unexpected change in appearance or functionality. Additionally, training should inform the workforce of the procedure for reporting suspected malware.
While HIPAA’s security rule is high-level and technology-neutral, it is clear that in today’s networked world, healthcare organizations are expected to take all reasonable measures to protect their PHI and other information assets from the dangers of spyware and other types of malicious software.

ABOUT THE AUTHOR

Kate Borten, president and founder of The Marblehead Group, Inc. brings to clients a unique combination of expertise in information security, privacy, and IT from over twenty years inside the healthcare industry. She led the first corporate-wide information security program at Massachusetts General Hospital, and she is the former Chief Information Security Officer at CareGroup, a major healthcare system based in Boston.

Ms. Borten is a nationally-recognized expert on HIPAA and health information privacy and security, and a frequent speaker on the topic. She is a contributing author to Auerbach Publications’ Information Security Management Handbook; author of HIPAA Security Made Simple (HCPro, Inc. 2003) and Guide to HIPAA Security Risk Analysis (HCPro, Inc. 2004); contributor to newsletters on HIPAA privacy and security; and three-year chair of HealthSec, the premier annual conference on information security in healthcare.

Sources


