# Blog for BAI Security

***https://baisecurity.wordpress.com/2014/11/19/protecting-electronic-healthcare-data-the-new-realities/***

## Protecting Electronic Healthcare Data: The New Realities

Posted November 19, 2014

Almost half of all identity thefts in the U.S. are now stolen medical records, as reported by USA Today.

While breaches of credit card data may grab the headlines (like last year's fiasco at Target stores), a stolen credit card number usually reflects fraud quickly and can be cancelled rapidly. By contrast, a single patient's full electronic medical record (EMR) typically includes the "identity theft trifecta"—birth date, Social Security number and home address—as well as their detailed medical history, which can be discreetly used (over months or years) to bill bogus medical charges or obtain prescription drugs which are regularly trafficked on the black market. As a result, the estimated "street price" of stolen EMRs can now be as much as ten times higher than 16-digit credit cards.

Medical data is particularly vulnerable, because many healthcare organizations are still dependent on applications and equipment designed exclusively for Windows XP; Microsoft, however, officially discontinued all support (including security patches) over six months ago. Because of the wide range of technical devices spanning modern medicine, it's harder for a hospital to upgrade its entire IT infrastructure around a new OS. Meanwhile, legions of malicious hackers around the world are searching for any exploitable flaw within that final update of XP.

The first line of defense against medical data breaches is compliance with Title 2 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protects the privacy of specific patient data. While the technical safeguards mandated by HIPAA are outlined in this 17-page document from the Department of Health & Human Services (HHS), it places broad responsibility on the healthcare organization to devise "reasonable and appropriate" safety measures based upon the organization's size and scope; a nationwide HMO (health maintenance organization) would require a different compliance program than a local dental practice.

What’s the real cost of sloppy HIPAA compliance or an all-out medical data breach? HHS can impose a civil fine ranging from $100 to $50,000 per incident, though total punitive class action damages could approach as much as $100 million, as currently faced by Tennessee-based Community Health Services after 4.5 million EMRs were reportedly hacked this past August. Or for any incident involving as few as 500 EMRs, it also could mean a permanent inclusion on HHS’s Breach Notification site, or what healthcare circles commonly refer to the “Wall of Shame.” In an age where consumers can easily monitor the online reputation of any business from a major retailer to a corner hot dog stand, a spot on the Wall of Shame may raise some anxiety.