WHITE PAPER: Electronic Medical Records: Risks and Defenses

The use of Electronic Medical Records (EMRs) and a more digitally integrated medical records system is no longer science fiction, and the task of securing sensitive medical data is a daunting challenge. The threat landscape continues to shift rapidly, and business responses need to keep up.

This whitepaper examines the risks, and outlines steps organizations can take to keep attackers at bay.

1.0 / OVERVIEW / With the technological evolution described above, and an influx of new Knowledge-Based Authentication (KBA) controls to prevent traditional financial fraud, the criminal demand for these records is booming.

The rise in targeted attacks against those who use and store personal medical information is just the tip of the iceberg for the coming risks the medical field will face.

2.0 / ROOTS OF RISK / The earmarking of $19B from the American Recovery and Reinvestment Act of 2009 accelerated the movement towards EMRs, resulting in more and more of American’s Protected Health Information (PHI) being digitally and remotely available\(^1\,^2\,^3\).

This includes everyone from large processors, insurers, and hospitals to small clinics and family practices. Couple this with a stark increase in demand for “Medi Fullz,” or full medical records, by cybercriminals\(^4\,^5\) and you have the makings of a perfect storm.

Examining how easily financial information such as credit card numbers and bank account logins can be changed against how quickly and easily they are burned (flagged by fraud detection), full medical and personal information becomes a much more appealing prospect.

With this data, cybercriminals can open their own bank accounts and credit cards in someone else’s name, but tied to contact information they control. With this data cybercriminals can apply for loans, engage in medical financial fraud or set up businesses and merchant accounts for laundering money -- all with the information typically found in a set of medical records.

Indeed, we have seen a corollary rise in reports of breaches involving electronic medical records and projections predict this trend will continue\(^6\,^7\,^8\). While this recent surge includes accidental and negligent breaches, there has also been a huge uptick in targeted physical and digital theft of PHI and EMRs.

This shift in landscape is accompanied by a change in the way courts and regulatory bodies approach consumer data protection in general. Historically, companies very rarely saw successful punitive action taken against them following a breach. This is no longer the case, as the latest round of breaches and the subsequent legal and financial fallout has shown\(^9\,^10\,^11\).

3.0 / CRIMINAL METHODS AND TARGETS / One money-making scheme involves setting up shop as or working with a clinic or medical practitioner to commit Medicare fraud. This is done by shadow billing, charging for procedures or services that never occurred, or by upcoding, using billing codes that specify the need for expensive procedures.
Medical insurance fraud can also come from the patient side in the form of a criminal posing as another individual to fraudulently receive medical services or prescriptions. Another vector for financial grift takes the form of tax fraud. Using the information found in an individual’s medical records, it is rather straightforward for a criminal to both gain more sensitive information and to steal that person’s tax refund outright.\(^{12,13,14}\)

The data found in EMRs also gives criminals the ammunition to perpetrate more elaborate financial identity theft. With this data they can receive loans, credit cards, and bank accounts under an assumed identity, leaving the victim holding the bag on a tanking credit score and a mob of collection agencies.

The fraudulently created accounts used by these criminals can also open the victim up to criminal proceedings when said accounts are used in the commission of crimes such as wire fraud.

Bank accounts opened by criminals can be used as a dump site or ‘drop’ for funds stolen or laundered by other means. For example, a criminal can set up a merchant account with Paypal, Skrill, Square, or any number of other transaction processors to make charges against stolen credit cards. The money from these transactions can be shunted to the ‘bank drop’ then retrieved via ATM, a money order, or transferred to yet another bank account.

These actions can be performed by the criminal directly or proxied through a set of money mules, individuals recruited to shift the money between accounts they control for a slice of the ill-gotten gains. Such practices are so common among cashout schemes that there is an active underground market for said ‘bank drops’ and third-party payment processors (Figures 1-3).

Furthermore, the information found in these records is often used to form points of verification for opening the payment processor accounts themselves.

![Figure 1: Bank Drops for sale](image-url)
Given this threat landscape, who is being targeted as sources for EMRs by cybercriminals? Medical insurers certainly hold the goods and have indeed been fruitful targets as of late with names such as Anthem, Premera, Community Health Systems, and Excellus making headlines\textsuperscript{14,15,16,17}.

While insurers make tempting marks, it is often easier to hit a medical provider directly. Hospitals, clinics, and doctor’s offices often do not have the security resources and policy enforcement levels that insurance companies do leading to breaches such as those seen by UCLA Health, Lubbock Cardiology, Siouxland Pain Clinic, Pediatric Group LLC, and more\textsuperscript{18}. You can easily find the records pilfered from healthcare providers for sale on the underground market.
Additional sources for EMRs are health information exchange and storage organizations. These are organizations that do not directly provide medical services, but are still in contact with sensitive PHI. There have already been breach reports from groups such as Medical Informatics Engineering (MIE), Metropolitan Atlanta Rapid Transit Authority, and Healthfirst Affiliates. While these types of targets have traditionally seen few breaches do not expect this to remain the case going forward.

There are numerous methods for siphoning out this golden data with varying levels of risk to the criminal perpetrators. Some of the most effective methods employ intentional and targeted research of individuals who have access to EMRs. This information is then used to craft especially enticing communications tempting the targets to divulge sensitive information, click on suspect links, or download malicious software. These are often referred to as ‘Spear Phishing’ communications and employ a level of social engineering skill.

The malicious links or email payloads found in these communications can contain dark surprises such as Remote Access Trojans (RATs), keyloggers, rootkits, credential harvesters, and other nasty forms of malware.

Another option for the attacker is to forgo the social research and specialized communication crafting. They can choose to target weaknesses in the web presence of the EMR holders through other methods. Examples include SQL injection (SQLi), cross-site scripting (XSS), exploiting vulnerabilities in web components, and general site and application security misconfigurations. However, it doesn’t always take an exploitable security hole to gain access to user or admin accounts. Sometimes all it takes is for a person to reuse the same login information on more than one site and for one of those sites to experience a breach.

There are actors actively leveraging password reuse and compromise databases to gain access to accounts across the web. There are even tools developed for this dirty work that make for faster account takeovers while flying beneath the radar of common security mechanisms by rotating account takeover attempts through varied proxy IPs.
Then there are less remote means of nabbing those digital records. Wardriving and warwalking, using a mobile device to hunt for vulnerable wireless networks, can be used to map out and target wireless connections for later exploitation.

Exposed terminals, such as the check-in or a receptionist’s computer, can be attacked with something as small and simple as a malicious PS/2 or USB device surreptitiously plugged into an open port. And, of course, there is the old standby of the physical smash and grab. While less common by the numbers, hardware thefts involving PHI happen often enough and have recently hit entities such as University of California at Los Angeles, Baylor College of Medicine, North East Medical Services (NEMS), and Montefiore Medical Center.

4.0 / DEFENSES / Now that we’ve laid out the threat landscape for U.S. EMRs and the cybercrime underground, let’s look at strategies for defense.

A great place to start is with up-to-date information on Tools, Techniques, and Procedures (TTPs), Indicators of Compromise (IOCs), and general trends relevant to your industry and function. One such forum focused on this type of information is the National Health Information Sharing & Analysis Center (NH-ISAC). Other useful resources include the Medical Identity Fraud Alliance (MIFA), the US Department of Health and Human Services (HHS) and your local State Attorney General's office.

If you are looking to defend against attacks targeting your web presence, you will want to consider an effective and customizable Web Application Firewall (WAF). With a properly feature-rich WAF you can create and deploy customized rules that will alert on or outright block malicious or suspect traffic including SQLi, XSS, CSRF, and more.
A good WAF can also use dynamic thresholds to detect and stop flooding requests from things like brute-force account cracking or takeover attempts, username or email enumeration, automated vulnerability scanning, general fuzzing, and more. It is also advisable to measure baselines for user account activity so you can then detect and respond to anomalous usage.

In preparing a defense against local network attempts remember to monitor, lockdown, and secure access to terminals, Ethernet jacks, laptops, mobile devices, wireless networks, and connected peripherals (medical devices, etc.) anywhere they are exposed to non-authorized persons.

Another important piece of the defense puzzle is a security awareness program that educates your employees, patients, and partners about the specific security threats they face and helps develop an adversarial thinking perspective that allows them to think critically about the potential impacts of the decisions and actions they and those around them engage in.

5.0/ CONCLUSION / Given the rising trend towards dynamic knowledge-based authentication to protect against financial fraud the cybercriminal hunger for extensive and up-to-date personal information will continue to grow.

As Electronic Medical Records are an easily transferable treasure trove of such information they will be eagerly sought by both those wishing to use them for fraud and those wishing to sell them to a growing underground market. This state of affairs makes entities working with and holding EMRs progressively higher-risk targets for larceny.

Existing customers that desire additional information can contact Akamai directly through CCare at 1-877-4-AKATEC (US And Canada) or 617-444-4699 (International), they’re Engagement Manager, or their account team.

Non-customers can submit inquiries through Akamai’s hotline at 1.877.425.2624, the contact form on our website at http://www.akamai.com/html/forms/sales_form.html, the chat function on our website at http://www.akamai.com/ or on twitter @akamai.

6.0/ APPENDIX / Listed below are the sources cited throughout this paper:

1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1560716/
2. http://content.healthaffairs.org/content/early/2012/04/19/hlthaff.2012.0153.abstract
3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4539806/