ARMOR™

BETWEEN YOU AND THE THREAT

Patients, privacy & healthcare's eroding trust

CISO VANTAGE POINT

KURT HAGERMAN | **CHIEF INFORMATION SECURITY OFFICER | ARMOR**

Real patients behind healthcare data

We often think of cybersecurity as an internal healthcare IT concern. From CISOs to system administrators, we assume that we're the only ones worrying about breaches and contemplating the benefits of ePHI and eHR.

And while HIPAA compliance requirements have given hospitals, healthcare IT organizations or anyone who stores, uses and manages electronic medical records plenty to be concerned about, we often forget that there are real patients at the core of these dialogues.

The Office of the National Coordinator (ONC) for Health IT, via a two-year study, found that privacy and data loss are very much on patients' minds — and those attitudes have the potential to impact both treatment outcomes and organizational reputations.

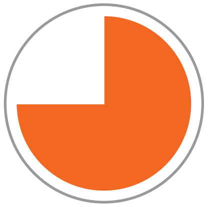
> "We often forget that there are real patients at the core of these dialogues."
>
> Kurt Hagerman
> Chief Information Security Officer | Armor

Through the patients' lens

In 2014, the ONC surveyed more than 2,000 respondents on their feelings about the privacy and security of electronic health records. The answered provided interesting results:

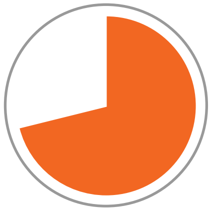
- 75 percent of patients were somewhat or very concerned regarding the privacy of their medical records; 69 percent were somewhat or very concerned regarding the security of their medical records
- Patients were particularly concerned about sharing records via fax or online, with 60 percent worried about electronic transmission and 63 percent worried about fax transmission
- 10 percent withheld information from healthcare providers over privacy and security concerns
- Despite those concerns, 76 percent wanted providers to use EHR and 70 percent wanted them to share those records

LOSING TRUST



75%

Very or Somewhat Concerned about Medical Record Privacy



69%

Very or Somewhat Concerned about Medical Record Security

The Office of the National Coordinator (ONC) for Health IT found that the strong majority of Americans have concerns about both the privacy and security of their medical records.

So, what does this tell us? For starters, we know that patients do appreciate the convenience offered by digital records. At the same time, they're concerned about privacy and security in almost equal numbers.

This concern is understandable given that a patient record can typically include a name, social security number, address, birthdate, employer, spouse name, credit card data/bank account data and family medical history. Just one breach represents a massive invasion of privacy for a patient.

Optimizing patient care through trust

That apprehension is also not terribly surprising, given how many breaches have been in the news. Overall, these numbers point to the urgent need for a strong security posture in healthcare organizations — not only to prevent attacks but also to foster patient trust.

After all, optimizing patient care depends on positive relationships between patients and providers. The fact that 10 percent of responding patients have withheld information from providers because of security fears is disturbing. (A 2013 Harvard study found that more than 12 percent of patients had withheld medical information for the same reason.)

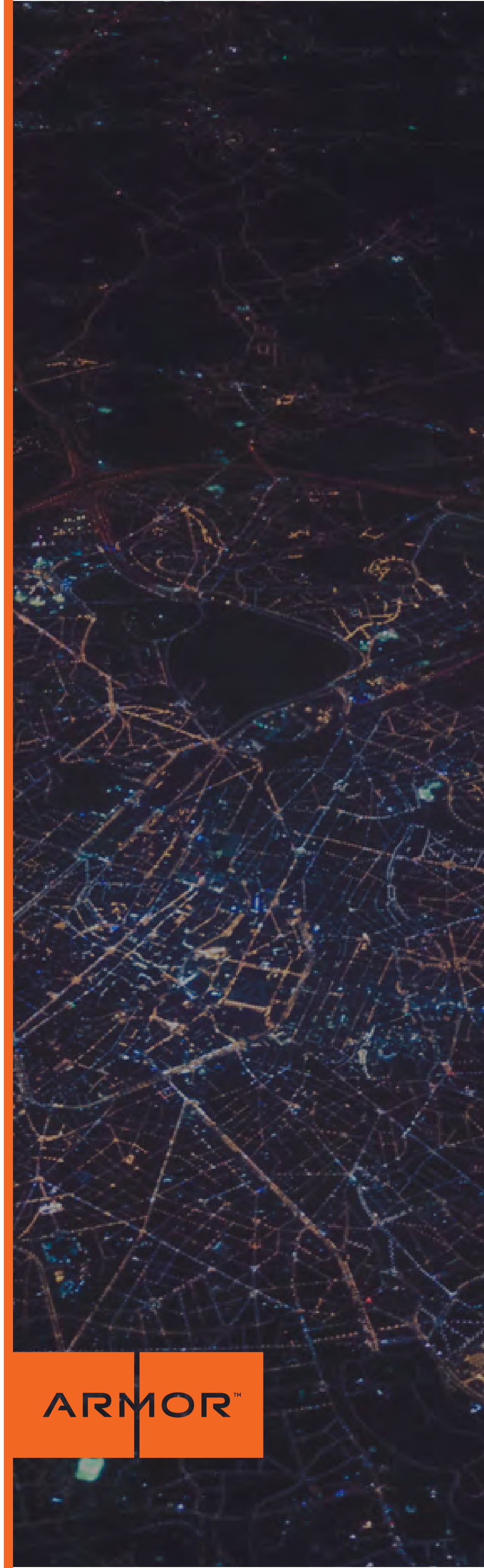
To be fair, the number of patients who'd withheld information from providers using paper records was 6 percent, which isn't much of a difference.

Regardless, it's obvious that organizations must allay patient fears by offering a strong security posture. Healthcare providers need as much accurate information as possible to make the best possible treatment decisions.

> "These numbers point to the urgent need for a strong security posture in healthcare organizations — not only to prevent attacks but also to foster patient trust."

Kurt Hagerman

Chief Information Security Officer | Armor



Defining HIPAA administrative safeguards

Security Management Process

A covered entity must identify and analyze potential risks to ePHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel

A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Information Access Management

Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the “minimum necessary,” the Security Rule requires a covered entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient's role (role-based access).

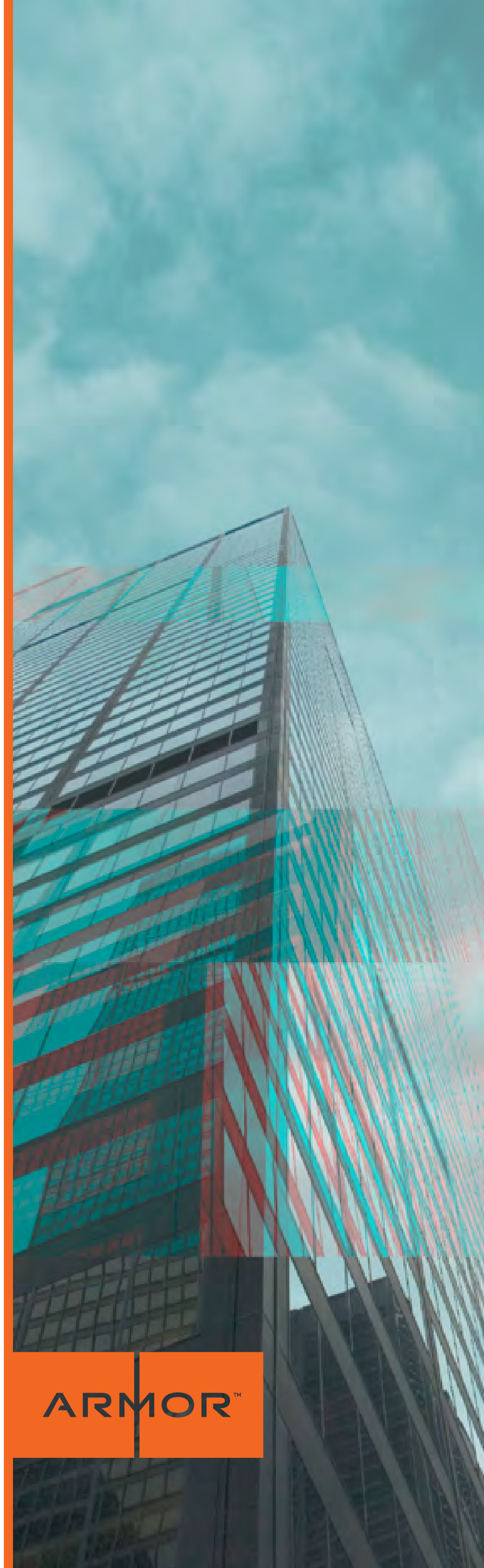
Workforce Training & Management

A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation

A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

— U.S. Department of Health & Human Services



Healthcare IT organizations confused about BAAs

Trust is further weakened when confusion about risk ownership is discovered. In March 2015, New Jersey-based DataMotion published a report highlighting some confusion by business associates (BA) about business associate agreements (BAA).

The encryption and healthcare information service provider polled some 780 IT and business decision-makers in North America. The survey focused on professionals who manage, oversee or work with compliance mandates and sensitive data.

While the effort did span several industries, Healthcare IT News noted some of the more alarming findings:

- Nearly 70 percent of responding organizations have a business relationship with a healthcare entity and also process protected health information (PHI)
- However, more than a quarter admitted they were either not a BA or were unsure if they were
- Of those processing PHI, 40.5 percent had either not been asked to sign a BAA or were unsure if they had signed one

If healthcare IT organizations are going to rebuild or establish greater trust with end-user patients, they must understand and follow the established guideless to help protect the very information they're entrusted.

> "If healthcare IT organizations are going to rebuild or establish greater trust with end-user patients, they must understand and follow the established guideless to help protect the very information they're entrusted."

Kurt Hagerman
Chief Information Security Officer | Armor

Reassuring patients, securing EHRs

So, what should organizations do? Clearly, just locking down EHRs and calling it a day isn't sufficient. Security is not just a matter for the IT team but for the entire organization. Providers and office support must proactively address security concerns when communicating with patients, rather than waiting for questions.

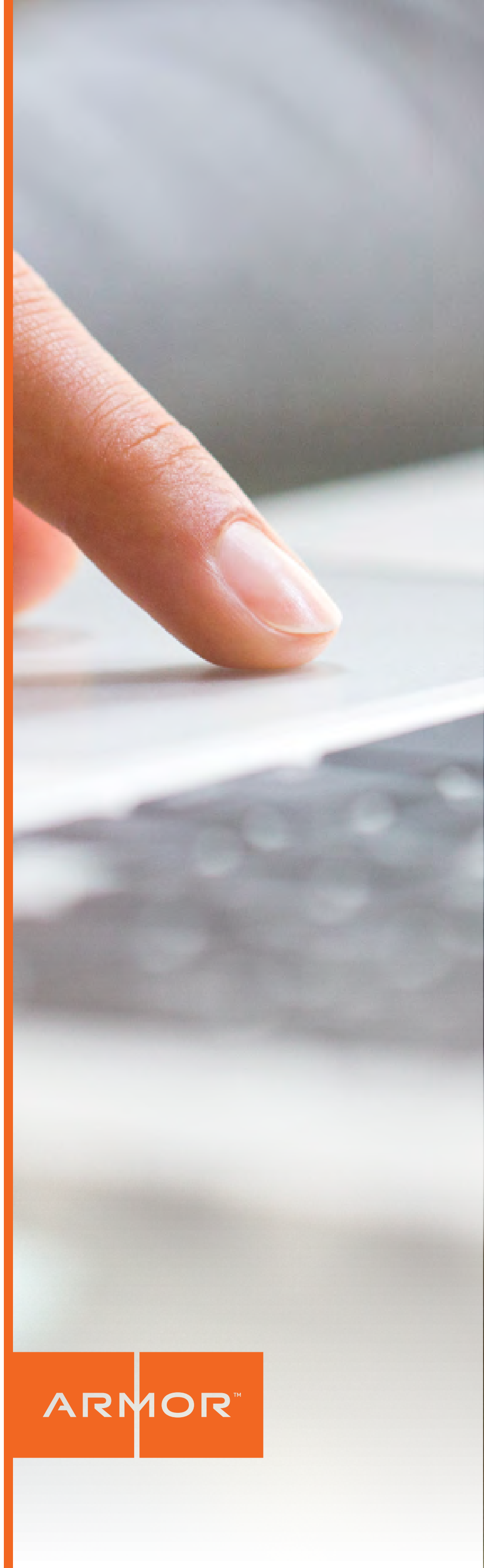
Organizational content — such as websites, instruction packets, brochures and other literature — should assure patients of their data protection and stress the point that withholding information can hinder good medical care.

Currently, when a patient arrives for an appointment, they're asked to sign a paper authorizing the provider to share their medical records. And usually, that's it.

There's rarely anything that says, "We're committed to protecting your data." And, of course, the patient never sees the IT staff working diligently behind the scenes.

The ONC survey shows that it's time to change. To optimize both their reputations and patient outcomes, organizations must build rock-solid security programs — and let patients know that their privacy is valued as highly as their health.

> "To optimize both their reputations and patient outcomes, organizations must build rock-solid security programs — and let patients know that their privacy is valued as highly as their health."
>
> Kurt Hagerman
> Chief Information Security Officer | Armor



About Kurt Hagerman

Hagerman serves as chief information security officer (CISO) for Armor. He is responsible for the governance, risk and compliance for both corporate- and customer-facing security solutions and products. Hagerman leads Armor's information security team, serves as the risk officer and ensures Armor maintains its PCI, HITRUST (HIPAA), ISO 27001 and other certifications.

Hagerman regularly consults with Armor prospects and customers on PCI, HIPAA and financial services regulations to help them understand how these regulations impact their business and how Armor can help them meet their regulatory responsibilities.

Hagerman is an active industry speaker and author on information security topics in the payments and healthcare spaces, as well as cloud security. He holds CISA and CISSP certifications and is an active participant with local chapters of ISACA, CSA and ISSA.

Prior to joining Armor, Hagerman was a managing director and national PCI practice director for Coalfire Systems Inc., a leading IT security GRC company. Hagerman has conducted hundreds of security reviews and audits across a number of industries, including the payment space, healthcare, financial services and higher education.

During his 25-plus years in the field of information technology, he has held a wide number of positions encompassing many IT and security disciplines, including network, systems and security engineering, IT/security auditing and compliance.

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

CISA® Certified Information Systems Auditor®
An ISACA® Certification

ARMOR™

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™

BETWEEN YOU AND THE THREAT