MedAllies

Two sides, same coin:
Security must support, not impair, EHR interoperability

The Internet is a dangerous place, especially for health records. Privacy and security threats abound, and each breach has the potential to chill the future of health IT. Inadequate security—perceived or real—and the ensuing lack of trust could doom interoperability efforts, and ultimately stall health care transformation.

The Identify Theft Resource Center—which has identified 353 breaches in the first half of 2014 across industries it tracks—reports about half occurred in the health sector.[1] Criminal attacks on health data have doubled since 2000.[2] In June, the Department of Health and Human Services' Office for Civil Rights reported 236 breaches of personal health information which affected more than 500 people in 2011, and 222 in 2012. The 236 breaches in 2011 affected 11.4 million individuals, while 3.3 million were affected in 2012.[3]

Underscoring these incidents is the value of the data. Robert Wah, MD, president of the American Medical Association, estimates a patient's health record is about 15 to 20 times as valuable as a stolen credit card.[4] Politico recently reported that a full identity profile contained in a single record could fetch $500.[5]

Privacy and security are at risk, putting health care transformation at risk as well.

The future of interoperability—and therefore, the future of health care transformation—depends on getting security and privacy

> *The future of interoperability—and therefore, the future of health care transformation—depends on getting security and privacy right. "If we fail at that, we fail. Period."*
>
> **A. John Blair, III, MD, FACS, CEO of MedAllies**

Issue Brief
AUGUST 2014

[1] "Big cyber hack of health records is 'only a matter of time,'" *Politico*, July 1, 2014

[2] The Fourth Annual Benchmark Study on Patient Privacy and Data Security, Ponemon Institute, March 12, 2014

[3] Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2011 and 2012

[4] Interview with Robert Wah, MD, president AMA. *H&HN Daily,* Feb. 26, 2014

[5] "Big cyber hack of health records is 'only a matter of time,'" op.cit.

right. “If we fail at that, we fail. Period,” says A. John Blair, III, MD, FACS, CEO of MedAllies.

On the other side of the equation is the need for data to flow between clinicians, and between clinicians and health care organizations. The Triple Aim[6] of better care, improved health and reduced costs isn’t achievable without data access and fluidity. Data must flow, but it must flow securely. Providers must be confident that sensitive information is going only to its intended recipient and remains encrypted until it arrives. Data and information need to follow the patient, so it gets to the right person at the right time.

“You cannot pit one against the other. Once you frame security and data access as competing goals, you’ve lost the game,” Blair warns.

> *“You cannot pit one against the other. Once you frame security and data access as competing goals, you’ve lost the game.”*
>
> **A. John Blair, III, MD, FACS, CEO of MedAllies**

This explains why MedAllies’ approach, through its national Direct network and MedAllies Direct Solutions™, ensures data security *and* its fluidity. MedAllies’ technical infrastructure enables providers to securely, accurately and instantly transfer vital clinical information in support of clinicians, improving the care and outcomes of their patients, and achieving Meaningful Use requirements.

Accreditation: Know your partner

MedAllies has earned triple accreditation for Certificate Authority (CA), Registration Authority (RA) and Health Information Service Provider (HISP) from DirectTrust.org and the Electronic Healthcare Network Accreditation Commission (EHNAC). “This validates our very high standards of privacy, security and trust-in-identity, and confirms we are adhering to the security ‘rules of the road,’” Blair says.

Providers need to know that. “These accreditations give an important assurance to MedAllies’ customers, but also to its information trading partners—vendors and providers—who know they can trust and rely on MedAllies,” explains David C. Kibbe, MD, MBA, president and CEO of DirectTrust, and senior advisor, American Academy of Family Physicians.

Physicians want to reach—that is, to connect with via Direct—colleagues across the country. EHNAC/Direct Trusted Agent Accreditation Program (DTAAP) recognition virtually guarantees them this will happen. The reason: Every EHNAC-/DTAAP-accredited network has the identical reach of every other accredited network. Accreditation also assures physicians their Direct-enabled system complies with Stage 2 Meaningful Use requirements—Direct exchange capability that is easy to use, secure and reliable, with little or no delay or interruptions in service. (See sidebar.)

So when Dr. Smith in Texas on an accredited network sends confidential information to

[6] Developed by the Institute for Healthcare Improvement

> *"These accreditations give an important assurance to MedAllies' customers, but also to its information trading partners—vendors and providers—who know they can trust and rely on MedAllies."*
>
> **David C. Kibbe, MD, MBA, president and CEO of DirectTrust**

Dr. Lopez in Oregon on an accredited network, each knows—with certainty—the other is not a fraud. Dr. Smith knows what network accreditation means, so she knows she's sending the data to the right person. And Dr. Lopez knows the information he is receiving is legit. Simply put, they are interacting with known, trusted providers.

Kibbe put it this way in the DirectTrust blog:

> *"There are, of course, times and circumstances when you don't want anyone to 'know you're a dog on the Internet,' as the famous* New Yorker *cartoon had it. But for health information exchanges, you really do want to know if you're talking with a dog! And health care providers and their patients can't and won't tolerate threats to their privacy. They'd rather abstain from the communications altogether."* [7]

Abstinence is not an option.

Leading the way

MedAllies is among a handful of organizations to achieve triple accreditation, but its commitment to privacy and security goes beyond that. It distinguishes itself even further by not only complying with the rules of the road, but being involved in their development.

Cultivating consumer trust

As providers communicate with each other, patients need to be confident their privacy and the security of their records are maintained. And they are already skeptical. Consumers' health care decisions will be influenced by their perception of security. But most Americans (83 percent in a 2013 Xerox-sponsored survey[†]) have significant concerns about EHRs—largely centered on privacy and security. Only 32 percent even want their records digitized.

On the other hand, 62 percent say EHRs will reduce overall health care costs, and 73 percent say they'll improve the quality of service they receive from their provider. A 2014 survey paints a somewhat brighter picture. *The Morning Consult* found 83 percent of respondents *expect* hospitals to use EHRs, but only 53 percent think the information in the EHRs would be safe; 39 percent are actively "worried."[‡]

"If they are going to keep trust with the patient, providers themselves must be confident that the patient's information is being kept secure. We provide that confidence," says Blair.

[7] DirectTrust blog, Aug. 24, 2012

[†] "Patients still ill-informed about EHRs," *Healthcare IT News,* Sept. 30, 2013 http://www.healthcareitnews.com/news/patients-still-ill-informed-about-ehrs

[‡] "Poll: Large Majority Expect Hospitals To Use EMRs," *The Morning Consult,* May 29, 2014

"Our team is deeply involved with Direct Trust, and we demonstrate our leadership in and grasp of security issues by participating in their creation. We also work directly with the providers to ensure security is addressed at the individual level," says Pete Palmer, CISSP, MedAllies' chief security officer. "It gives us unique insight into and comprehension of just what's required. We understand the security standards because our leaders helped build them."

What MedAllies provides

MedAllies' suite of services, MedAllies Direct Solutions, provides a secure, scalable, standards-based way for participants to send authenticated, encrypted personal health information to other providers, whether they are across the street or across the country. It ensures clinically relevant data can be exchanged between providers—using disparate EHR systems—seamlessly and in a manner completely consistent with existing EHR workflows. This approach supports Stage 2 Meaningful Use and the patient-centered medical neighborhood.

> *"We understand the security standards because our leaders helped build them."*
>
> **Pete Palmer, CISSP, MedAllies' chief security officer**

Importantly, in terms of security and workflow, MedAllies' team includes physicians and security experts. MedAllies leverages an expert clinical process redesign team to ensure the Direct-enabled solution is aligned with the practice's clinical workflow.

MedAllies operates a leading national Direct network, but its implementation focus is clinically and community centered. MedAllies Direct Solutions builds on existing EHR-based workflows. "We engage directly with the clinical staff to incorporate Direct exchange of information into each organization's regular stream of work," Blair explains. Its proven three-phase, three-track onboarding process covers the technical, administrative and clinical aspects—and each track thoroughly addresses security, not as an abstract concept or a complicated add-on, but as a fundamental part of the onboarding process.

Relevance, efficiency and security

MedAllies' security team works directly with provider organizations to address security down to the individual level, verifying each person attached to an address is who she

Accreditation and reach

Accreditation enables HISPs to exchange messages without having to make separate trust and security agreements with each other. No accredited HISP has any greater reach than any other HISP, because they're all connected to the national network, Blair explains. Any provider organization can communicate with any other provider organization if each has certified EHR technology and is using an accredited network, even if the networks are different. Think about how national cellular networks work: A person on AT&T can reach everyone on Verizon and a person on Verizon can reach everyone on Sprint.

says she is, Palmer explains. This hands-on approach, this attention to workflow, isn't just "nice to have." It's essential. Security must support the flow of data, not impede it.

Security and privacy cannot be the only considerations when advancing health information technology. Ultimately, where health IT succeeds or fails is in the practice or at the hospital. It comes down to functionality and clinical relevance. Any effort to advance health information exchange must be clinically relevant and enhance—not impair—provider efficiency.

That's because on the provider side, productivity and workflow are just as important as security. "If providers believe changes to enhance security will improve care and efficiency, interoperability will advance rapidly. If the providers do not believe this, it will stall. Physicians want secure systems, but not at the expense of patient care or operational efficiency," says Blair.

This hands-on approach, this attention to workflow, isn't just "nice to have." It's essential. Security must support the flow of data, not impede it.

Productivity and security need not be competing aims; in fact, they are complementary goals. "You hear a lot of talk about the tension—even the conflict—between security and convenience, but I don't see that," Palmer says. "They serve each other. They are partners, not competitors."

It comes back to workflow, says Blair. A good example of this is two-factor authentication. This approach to security is commonplace in the retail world. It requires "something you know" (such as a password or PIN) and "something you have" (a cell phone, ATM card, retinal scan, fingerprint, etc.). "We need a mindful approach to two-factor authentication. What will be the impact on provider workflow and productivity? The issue isn't whether to take this approach, but how to accomplish it," says Blair. For instance, will the provider have to authenticate at each transaction or at each session? "Each approach has a markedly different impact on provider workflow—and thus, provider willingness—or unwillingness—to use it. This could have a profound impact on adoption and use of EHR functionality related to interoperability."

It's not that providers prefer functionality over security. They don't; they want both. "The more thoroughly we address workflow functionality, the less resistance we encounter and the faster we can move to two-factor authentication."

With the MedAllies approach, security and productivity *do* complement each other. MedAllies is working with provider entities, vendors and others to advance workflow processes that will support the evolving security requirement for providers. "The real distinguishing feature of a HISP will be the service it provides, including the efficiency of onboarding providers, and its ability to get adoption and usage across communities," Blair explains. "That's MedAllies' strength." MA

A. John Blair, III, MD, F.A.C.S., CEO of MedAllies

BLAIR is a health care and technology executive with broad experience across the health care industry. MedAllies facilitates provider adoption of health information technology and integrates the health care community to facilitate care coordination and patient-provider communication. In 2011, MedAllies was selected by the Office of the National Coordinator (ONC) to provide the MedAllies Direct Solutions software platform for one of the seven Reference Implementations of Direct. In 2012, the New York eHealth Collaborative (NYeC) chose the MedAllies software platform to run the Direct Network portion of the Statewide Health Information Network of New York (SHIN-NY).

MedAllies went live as a National Direct Health Information Service Provider in 2013; it has achieved full EHNAC/Direct Trust accreditation. Today, MedAllies runs one of the leading national Direct networks.

Blair also serves as president of Taconic IPA (TIPA), a 5,000-member physician organization at the forefront of transforming health care delivery in New York's Hudson Valley through meaningful use of health IT and pay-for-performance incentives.

Blair is chair of the DirectTrust board and serves on the Governance Subgroup of the Interoperability and HIE Workgroup of the ONC Federal Advisory Policy Committee.

He is a member of various committees and boards, including the NCQA Committee on Performance Measurement.

A board-certified general surgeon, Blair spent 15 years in academic medicine and private practice before becoming president of TIPA. He received his medical degree from Rush Medical School in Chicago and completed his surgical training at the University of Texas Medical Center in Dallas. He performed a gastrointestinal fellowship at the Middlesex Hospital in London, England.

Peter Palmer, CISSP, CPHIMS Chief Security Officer of MedAllies

PALMER has more than a decade and a half of experience designing and implementing security and identity management systems in the health care industry. He currently chairs the Kantara Initiative's Healthcare Identity Assurance Work Group and Leadership Council. He is active with DirectTrust.org, the standards and accreditation organization for Health Information Service Providers. He has expertise in the areas of health information technology, information security, audit and compliance, public key infrastructure, health data standards and identity management. He has led organizations to ISO 27001, EHNAC, and Federal Bridge PKI accreditations.

Palmer has previously participated in various HIMSS work groups and task forces in the areas of privacy and security, and served on the local chapter board for six years. He has written whitepapers and articles in publications such as *Healthcare IT News, Health Management Technology* and *Business Communications Review.*

David C. Kibbe, MD, M.B.A., president and CEO of DirectTrust

KIBBE leads DirectTrust, the nonprofit industry alliance whose goal is to serve as a forum and governance body for persons and entities engaged in Directed exchange of electronic health information as part of the Nationwide Health Information Network. DirectTrust is a standards development organization whose Security and Trust Framework is the basis for the voluntary accreditation of service providers implementing Directed health information exchange. He is also senior advisor to the Center for Health IT at the American Academy of Family Physicians, where he has worked in either a full-time or part-time capacity since 2003. In late 2007 he started a sole proprietorship consulting firm, The Kibbe Group LLC. He is a leader in the Health 2.0 movement that seeks active participation by patients and consumers in the uses and management of their own personal health information.

About MedAllies

MedAllies, founded in 2001, has extensive experience with EHR implementation and workflow redesign to improve clinical care. It provides unmatched expertise in interoperability, Meaningful Use 2 compliance and Direct services. As one of the ONC Direct Reference Implementation vendors, MedAllies has provided Direct services since the Direct Project's inception; it now runs a leading national Direct network. MedAllies' product suite, MedAllies Direct Solutions™ builds on existing technology to achieve interoperability. Physicians use their current EHR systems, allowing information to flow across disparate EHR systems in a manner consistent with provider workflows. MedAllies Direct Solutions is a tool to advance primary care models that emphasize care coordination and improved care transitions, and support patient-centered care.

Fully-accredited Direct HISP

DirectTrust EHNAC ACCREDITED DTAAP CA

DirectTrust EHNAC ACCREDITED DTAAP HISP

DirectTrust EHNAC ACCREDITED DTAAP RA

Do you want to learn more?

Call us at (845) 896-0191 ext. 3076 or send us a request through our website,
www.medallies.com/Contact_Us