A Prescription for Secure Physician Communications

Meaningful Use Stage 2 (MU2) requires physicians to use the Direct Project to securely exchange health information over the Internet. The goal is to create a standards-based approach to communication that facilitates interoperability and collaboration among providers. That means identifying the underlying secure messaging technology that will enable a medical practice to demonstrate data transmission capabilities and integrate with the Direct Project protocols.

Sounds complicated? Actually, there's no need to panic, much of the legwork has already been done.

The key is to look for secure messaging technology that seamlessly integrates with existing EHR technologies – so physicians, nurses and other staff can use tools they already know. Naturally, physicians and their staff don't want to learn another complex system.

Andy Nieto is a health IT strategist for DataMotion, a health information service provider (HISP) with 15 years of experience in secure data delivery. DataMotion was founded in 1999, and today, millions of desktop, tablet and mobile users leverage its cloud-based data delivery platform to securely transmit protected health information.

Enter Direct Secure Messaging

One of the key advancements from Meaningful Use Stage 1 (MU1) is the introduction and use of Direct Secure Messaging (Direct); an email-like technology that uses Direct Project protocols and allows providers/practices to share information in a secure manner. The MU2 measure is based upon, but not limited to, transitions-of-care events: provider referrals, provider-to-hospital intakes and hospital-to-provider discharges.

Direct can be readily integrated into most EHRs by an EHR vendor. Other connectivity resources include web and mobile device interfaces. It is expected that EHR vendors will initially deploy Direct resources solely for the transition-of-care measures. Direct, however, is capable of much more versatile use due to its recognizable structure and secure functionality. General messaging — provider to patient and patient to provider — are just a couple of the communication pathways possible. Direct provides a HIPAA-secure method of sending electronic messages, and ensures its delivery to the desired recipient.

This ability to communicate is provided by health information service providers (HISPs), which offer message encryption, identity validation and message transition between providers. You needn't be overly concerned about the technology involved. There are some basic traits to look for, and resources that can guide you to selecting the right HISP.

Selecting a HISP

DirectTrust.org, Direct's governing body, has actively worked to make this technology secure, easy-to-use and available. Full accreditation by the Direct Trusted Agent Accreditation Program (DTAAP) for HISPs from DirectTrust.org, and the Electronic Healthcare Network Accreditation Commission (EHNAC), ensures compliance with industry-established standards, HIPAA regulations and the Direct Project. Simply put, this accreditation is not only vital for selecting a worthy HISP, it makes finding one simple and safe.

A strong, experienced HISP will be able to clearly explain and demonstrate the use of Direct and should provide tools/services that have been proven in the field over a period of time. As these have matured, naturally, ease-of-use will have developed accordingly. Remember, what you need is tools/services that meet real-world communications needs.

Another proof-point to look for is how that HISP has helped EHR systems to achieve 2014 ONC-ACB certification using Direct as "relied upon software." With integration of Direct, EHR vendors are now enabling healthcare providers to attest for MU2 and qualify for financial incentives from the Centers for Medicare and Medicaid Services. If a HISP can show that they're helping EHR vendors to help healthcare providers, you can work with them directly to easily attain your goals.

The prescription for secure physician communications is actually readily available: accreditation, experience in secure data delivery, field-proven tools, and a demonstrated ability of helping others in the industry. Check each of those "boxes" and you'll be in good hands.

*A variation of this paper was previously published in *Medical Practice Insider*, March 4, 2014.

ABOUT DATAMOTION

DataMotion enables organizations to dramatically reduce the cost and complexity of delivering electronic information to employees, customers and partners in a secure and compliant way. The company's easy-to-use solutions for secure email, file transfer, forms processing, customer contact and Direct Secure Messaging leverage the DataMotion Platform for unified data delivery. In 2012, DataMotion expanded operations as a health information service provider (HISP) with its DataMotion Direct secure messaging service, allowing healthcare organizations to meet emerging Meaningful Use Stage 2 (MU2) requirements. Millions of users worldwide rely on DataMotion to transparently improve business processes and reduce costs, while mitigating security and compliance risk. DataMotion is privately held and based in Morristown, N.J. For the latest news and updates on DataMotion, visit www.datamotion.com, like DataMotion on Facebook® or follow DataMotion on Twitter® @datamotion.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 200 Park Ave Florham Park New Jersey 07932