DataMotion™ / Whitepaper

How to Securely Exchange Personal Health Information via Email: Secure Messaging for Dentistry

Within the healthcare industry, the electronic exchange of protected health information (PHI) is governed by regulations such as HIPAA and the HITECH Act, which require adequate security be used to protect the information contained in personal health records from accidental or malicious public disclosure. In addition, the regulations seek to encourage electronic health information exchange to both improve the quality of patient care while reducing the cost.

For many disciplines, including dentistry, an email encryption service is a viable and frequently used technology to meet HIPAA security requirements for data in motion. It is also possible to use email encryption services to achieve efficiency in the exchange of dental PHI to improve care and reduce costs.

A modern email encryption solution exhibits the following strengths for use in dentistry:

- Cost effective 'email overlay service'
- Complies with HIPAA regulations
- Works with any email address, email service and email client (including on mobile devices)
- Supports large file attachments including diagnostic images with encryption
- Relatively easy to use for both sender and recipient
- Easy to use for referrals, patient and business associate communications

Unfortunately, current email encryption services have multiple shortcomings that limit its value to the health industry at large, particularly when it comes to sharing clinical information, which is one primary focus of the HITECH act.

- Lack of vendor interoperability
- Lack of identity validation

These limitations reduce the efficacy of email encryption for true health information exchange. These shortcomings were recognized by the US Department of Health and Human Services, and as part of the HITECH Act, the Office of the National Coordinator initiated a new approach, defined as the Direct Project, which developed a standardized email-like method for health information exchange known as Direct Secure Messaging.

New Solution: Direct Secure Messaging (aka 'Direct')

Direct Secure Messaging is a national encryption standard for securely exchanging clinical healthcare data via the Internet. It is also known as the Direct Project, Direct Messaging and just 'Direct'. Developed in 2010 under a part of a federal project for standards-based healthcare communications, the Direct Project specified the secure, scalable and standards-based method for the exchange of Protected Health Information (PHI). As a specific secure messaging technology for healthcare, Direct is designed to go beyond HIPAA compliance, to do much more than proprietary email encryption services to cut costs and deliver improved quality of care.

On the clinical side, Direct can address gaps in transitions of care which have been identified as a significant patient safety issue. Incomplete exchange of patient health information among providers when transitioning from one care environment to another is a point of vulnerability that can compromise the overall quality of care a patient receives.

On the business side, Direct matches the efficiency of generic email encryption by reducing or eliminating the costs associated with fax workflows by transitioning relatively expensive fax communication to less expensive email workflows.

Direct Secure Messaging provides many benefits including:

- One unified standard that all systems and service providers can leverage
- HIPAA compliant security and privacy protection of PHI
- Improved communications between providers
- Easily sent and received referral information
- Efficient report exchange
- Ease of sharing patient information
- Improved practice workflow and related cost reduction

How does Direct Secure Messaging work?

In many ways, Direct is implemented and used just like email. Its benefits for the healthcare industry are incorporated into the methodology and technology within the virtual direct secure messaging network that operates over the internet. Direct can be incorporated into a variety of user interfaces such as an email client, a mobile device, and healthcare IT system portals or as an automated data delivery feed. Any of these interfaces are capable of sending or receiving Direct messages. Healthcare IT systems such as EHRs can also integrate Direct in multiple ways depending on the desired workflow.

But in order to use Direct, both sender and recipient users need a specific Direct Secure Messaging email address, which are provided by a Health Information Service Provider, or HISP (see below). For this reason, traditional email encryption services remain an important and practical tool for email communications in todays dental practice.

Where can you get a Direct Secure Messaging address?

Direct Secure Messaging addresses and services are provided by a Health Information Service Providers or HISP. The term Health Information Service Provider (HISP) has been used by the Direct Project both to describe a function (the management of security and transport for directed exchange) and an organizational model (an organization that performs HISP functions on behalf of the sending or receiving organization or individual).

HISPs responsibilities are also important to understand. They issue Direct Secure Messaging (Direct) addresses and attach certificates that validate sender and recipient identities to those addresses. A HISP also provides the back-end power to make sure your messages are delivered securely to the intended Direct-enabled recipient – similar to a post office delivering the mail.

HISP responsibilities:

- Provide your Direct email address
- Enable backbone transport for HISP to HISP communications
- Publish digital certificates to establish trust
- Package message contents using Direct standards and specifications
- Encrypt content and attachments to secure confidentiality and integrity
- Ensure authenticity of sender and recipient

Since the introduction of the Direct Project, many HISPs have entered the market to facilitate the use of Direct Secure messaging within the healthcare industry. Since Direct was established as a secure messaging standard – every HISP is required to interoperate in order to efficiently exchange secure messages between their respective subscribers. A HISP accreditation process established by the Direct Trust and the Electronic Healthcare Network Accreditation Commission (EHNAC) helps ensure that individual HISPs are in compliance with the Direct Secure Messaging specification and service delivery.

Practical Uses for Direct Secure Messaging in Dentistry

The American Dental Association Standards Committee on Dental Informatics has evaluated Direct Secure Messaging for use in the dental industry. The following use cases have been identified as examples where Direct could be used to meet both HIPAA security regulation, and HITECH efficiency objectives in the area of PHI exchange.

Use Case #1:

A general dentist has taken several radiographic exams of a patient and some preliminary dental examination data. The general dentist wishes to refer the patient to an endodontist for final diagnosis and treatment of an acute pain problem.

Use Case #2:

A general dentist has found a suspicious lesion on the ventral surface of a patient’s tongue. The general dentist has taken several intra-oral photographs and saved them to the office digital imaging system. The general dentist has also performed an excisional biopsy of the area and submitted the specimen to an oral and maxillofacial pathology service.

Use Case #3:

A general dentist has taken a FMX and panoramic radiographic exam. Upon interpretation, the general dentist identifies a suspicious radiolucency in the patient’s mandible. The general dentist would like to send the images to a maxillofacial radiologist for interpretation along with a request that the radiologist also conduct any indicated additional imaging studies.

Use Case #4:

A general dentist has been requested to send all radiographic images for a specific patient to a forensic odontologist to facilitate a post-mortem identification.

Use Case #5:

A periodontist has been referred a patient for surgical placement of an implant. The periodontist has taken a radiographic exam including a panoramic x-ray, individual periapical x-rays of the intended site. The periodontist would like to send these radiographic images to a maxillofacial radiologist for an interpretative report and a CBCT for routine implant planning and surgical guide design.

Summary

The future of healthcare is focused on outcome-based medicine. Positive outcomes are the natural progression of the best minds sharing and interacting to find the best course of treatment for their patients. Healthcare providers who incorporate the Direct Secure Messaging into their workflow gain a secure, interoperable and efficient communication tool to support improved dialog between patients and their care teams, while meeting regulatory requirements, government mandates and in some cases the benefits of financial incentives.

While Direct is the future of ‘email-like’ communications in healthcare, there remains a strong case for traditional email encryption services in today’s dental practices. The simplicity and ubiquity of email encryption services with respect to adoption and use by virtually anyone, along with HIPAA compliance strength, suggest that email encryption services have an important practical role to play as an interim complementary solution to Direct. Vendors delivering both services are best positioned to provide the dental community a well manged, cost effective migration path.

Long term, for dentistry and across the healthcare continuum, the adoption of Direct Secure Messaging can ultimately provide a higher level of care and better outcomes; a scenario that all involved clearly want and are trying to achieve.

ABOUT DATAMOTION

Our mission is to dramatically reduce the cost and complexity of exchanging private health information in a secure and compliant way! Our easy-to-use encryption solutions for Direct Secure Messaging, secure email, file transfer, forms processing and customer contact leverage the DataMotion Platform for unified data delivery. As a provider of secure messaging solutions such as email encryption and Direct Secure Messaging – we are constantly engaged by providers to help them stay in compliance with expanding regulations, including HIPAA and HITECH. We are an EHNAC accredited Health Information Service Provider (HISP), and actively promote the adoption of Direct Secure Messaging across the healthcare industry. DataMotion is privately held and based in Florham Park, N.J.