# Keep Patient Data Secure

## Simple Actions for a Digital World

By **Andy Slavitt**, CEO of OptumInsight,
**Mark Crockett, M.D.**, Senior Vice President of Clinical Solutions, OptumInsight
**Ray Scott**, Senior Vice President of Product Strategy, OptumInsight

As a practicing physician, you are already familiar with the Health Insurance Portability and Accountability Act (HIPAA) and its security and privacy standards. Your practice has no doubt put into effect policies and procedures to safeguard the privacy of protected health information (PHI) and to meet patients' rights, under HIPAA, to access their own personal health information.

While most practices are adept at protecting PHI with paper records, hospitals, physicians, and health plans are increasingly taking advantage of technology to improve efficiency and provide better patient care.

If your practice does not currently use an electronic health record (EHR) system, the chances are that it soon will. Initiatives such as the American Recovery and Reinvestment Act of 2009 (ARRA) are promoting the use of EHRs by providing incentives to health care providers who convert from paper medical files to an EHR system.

The combination of ARRA incentives and benefits such as real-time access to legible patient data, improved continuity and quality of care, increased productivity, and greater patient and staff satisfaction make an overwhelming case for adopting an EHR. ARRA also provides funding for communities to establish health information exchanges (HIEs) to enable health care providers and health plans to share medical information as permitted by their patients.

As we share growing volumes of clinical information electronically, it is even more critical for physicians to take appropriate measures to protect patient rights and safeguard their information, and to meet HIPAA requirements. OptumInsight™ (formerly Ingenix) offers the following advice as a how-to guide to sharing and protecting health information in today's connected health communities.

### Highlights

- Securing the electronic health record and participating in a health information exchange
- Communicating with patients, consulting with fellow physicians and managing referrals
- Working with Business Associates
- Understanding de-identified information
- Creating a culture of respect for privacy
- Making security and privacy a priority
- Protecting your own privacy

### Securing the electronic health record and participating in a health information exchange

When selecting an EHR system, look for technology certified by organizations such as the Certification Commission on Health Information Technology (CCHIT), which verifies that EHRs have built-in functionality to ensure security of PHI. More information about CCHIT is here: http://bit.ly/m5fcAl.

While widespread adoption of EHR systems improves the flow of information within your practice, more meaningful connectivity with other providers and stakeholders in the health system should occur through an HIE. A robust HIE makes it possible for physicians to access critical patient data from other health care providers, hospitals, laboratories, radiology departments, emergency departments and other sources.

Both HIPAA and ARRA require that you take reasonable steps to secure the integrity and confidentiality of PHI. This means that it is important for you to understand where your patient information is stored, who has access to it and how it moves around your organization as well as outside of your practice, regardless of whether it is on paper or in electronic form. Understanding this flow will help you develop policies and procedures to ensure that your practice is complying with regulations that protect patients.

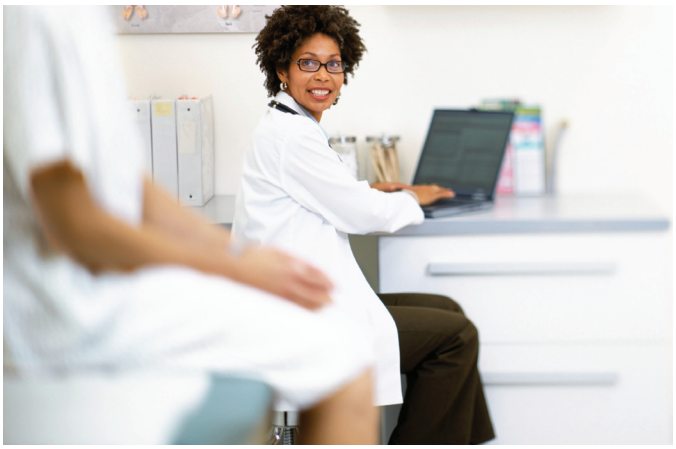
You also need to ensure your hardware and software are both secure. Following is an essential checklist of actions you can take to secure patient data:

- ☐ Use strong passwords to protect computers and electronic devices. A strong password is at least eight characters long, does not contain a complete word, is significantly different from prior passwords and contains a combination of upper case and lower case letters, numbers and symbols.
- ☐ Install encryption software on all laptops and desktops that contain PHI. This is important, as an theft or accidental loss of secure, properly encrypted information is not a considered a "breach" under HIPAA.
- ☐ Install antivirus and malware detection software on all computers.
- ☐ Implement password protection on databases containing PHI.
- ☐ Physically secure hardware that stores PHI. For example, laptops should have locking cables and disks should be stored in locked cabinets.
- ☐ Remove all PHI from electronic computing and communication devices before disposal or reuse.
- ☐ Always log off when leaving your computer. Don't leave medical files on a computer screen when you leave your desk. As an additional safeguard, set your computer to automatically password protect access after 10 minutes of non-use.
- ☐ In public areas, arrange workstations so that people walking by cannot view information on the screen.

## Communicating with patients, consulting with fellow physicians and managing referrals

Online communication with patients, especially though email, is becoming increasingly popular. A 2010 Manhattan Research report found that approximately 39 percent of physicians engage in electronic communication of some kind with patients, a 14-point increase since 2006. Physicians using email to communicate with patients have found that email improves patient, physician and staff satisfaction; increases efficiency; and strengthens the doctor-patient relationship.

However, email is just the start. Increasingly, peer consultation and referrals of patients to specialists are managed electronically on social networking sites such as Sermo, an online community for physicians, and via health IT services such as EHRs. ARRA provisions for demonstrating meaningful use of an EHR system also require physicians who refer a patient to another provider of care to share a summary care record for each transition of care or electronic referral.



Before adopting email or other forms of online communications for clinical purposes, you need to establish policies and procedures to safeguard patient information. Specifically:

- Prohibit the transmission of PHI via instant messaging or other peer-to-peer software.
- Always validate the email address of the recipient and be certain emails containing PHI are properly encrypted, pursuant to HIPAA
- Establish *informed consent* before communicating electronically with a patient. Including a "privacy policy for messages" in your HIPAA Notice of Privacy Practices form can fulfill this requirement.

## Working with Business Associates

HIPAA defines a "Business Associate" as any company or person outside of your practice that: (1) performs services on your behalf, and (2) requires the use or disclosure of PHI in order to complete the tasks they are contracted to execute for you. This can include consultants, lawyers, accountants, transcription agencies, billing companies and computer support personnel.

Companies such as OptumInsight contract with physician practices to provide technology applications and services. In many cases, this requires access to clinical and administrative data—in other words, PHI. As you contract with Business Associates, it is important to be sure that these individuals and organizations have processes and protocols in place to protect the PHI of your patients. In addition, it is important to understand how Business Associates use information from your practice, including de-identified information.

OptumInsight's clinical data philosophy is simple and clear. We believe that we have a responsibility to manage and protect your data and that of your patients. We do not sell client PHI, and do not share or use your information without explicit approval

### Understanding de-identified information

Like PHI, the use of de-identified information is also governed by HIPAA. De-identified information is "health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual." De-identified information is not PHI under the HIPAA Privacy Rule. As a result, de-identified information may be shared without restriction.

De-identified information has many uses such as research into the comparative effectiveness of certain medical procedures, where it is beneficial to compare test populations to control groups of individuals not in the study. Other applications include quality improvement, public health and research.

As a steward of your patients' information, it is important for you to understand acceptable use of de-identified information, whether by your practice or by one of your Business Associates.

HIPAA defines two routes by which a Covered Entity may properly de-identify data:

(1) the "Safe Harbor" method, and (2) through professional statistical analysis. Using the Safe Harbor method, 18 specific identifiers must be removed, including all geographic subdivisions smaller than a state; all elements of dates, except the year; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web addresses; IP address numbers; biometric identifiers, including finger- and voiceprints; full-face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.

Removing all 18 of these identifiers, as specified by the Safe Harbor method, makes the data much less useful for analyzing health trends over time or for surveillance of health conditions, such as influenza outbreaks or cancer clusters that occur in smaller geographic areas.

The second method of de-identification permitted under HIPAA requires that a qualified statistician determine and certify that the likelihood of conclusively re-identifying any single person in the data set is "very small" (less than 4 percent) using the information alone or in combination with other reasonably available information. These findings must be certified by a statistician who has appropriate knowledge and experience of generally accepted scientific principles and methods for rendering information not identifiable.

from you. In short, we restrict the use and disclosure of data and information first, to what is permitted by law, and second, to what is permitted in our contract with you.

The law says that Covered Entities (your practice) and their Business Associates can use PHI for treatment, payment and health plan operations if they enter into a "Business Associate Agreement" that identifies how PHI will and will not be used. (Note that not everyone to whom you provide PHI needs a Business Associate Agreement. For example, you may provide PHI to a health plan or its vendor for payment purposes.

(See http://1.usa.gov/l6uYee, a guide created by the Department of Health and Human Services, for more information.)

Before sharing paper or electronic PHI with Business Associates, both parties should execute an agreement that includes:

- A confidentiality clause that holds the Business Associate accountable for protecting PHI in the course of the work they do on behalf of your practice.
- Statements that the Business Associate:
  - Cannot use or further disclose the information in a manner that violates the HIPAA privacy rule.
  - Must safeguard the information from any use or disclosure other than provided in the agreement.
  - Must report any use or disclosure of information not provided for by the agreement.
  - Must ensure that any agents, including subcontractors, that receive PHI comply with similar restrictions and conditions that apply to the Business Associate.

## it's personal

### Creating a culture of respect for privacy

No safeguards in the world can protect sensitive information if the workplace culture doesn't exist to reinforce those measures and act as a first-line of defense. Beyond encryption systems and locking files, it is essential that day-to-day operations are managed with a sense of respect for data security and patient privacy.

It begins with training your staff to use and disclose only the "minimum necessary" amount of PHI in order to do their jobs. This includes disclosing only the information necessary for treatment to other health care providers.

Here are some other practical steps for protecting patient privacy:

- Always close doors when talking on the phone about patients and be careful what is said aloud.
- Close examination room doors when discussing treatments and administering procedures.

- Avoid discussions of patients and their conditions in public areas.
- Ensure that you and your staff never leave voice mail messages detailing patient conditions or test results, unless you receive express permission from the patient in advance to do so.
- Do not use identifiable information that could reveal health issues when summoning patients in open settings, such as your waiting room.

Privacy training for new employees and refresher courses for existing employees are vital to ensuring that everyone who interacts with patients and patient information complies with HIPAA requirements. As an example, in 2009, OptumInsight implemented *"it's personal,"* a comprehensive training program that emphasizes data privacy and security. Every new employee completes *it's personal* training as part of their orientation, and ALL employees must re-certify annually. This ensures everyone receives continuous reinforcement and updates as privacy and security laws and challenges evolve.

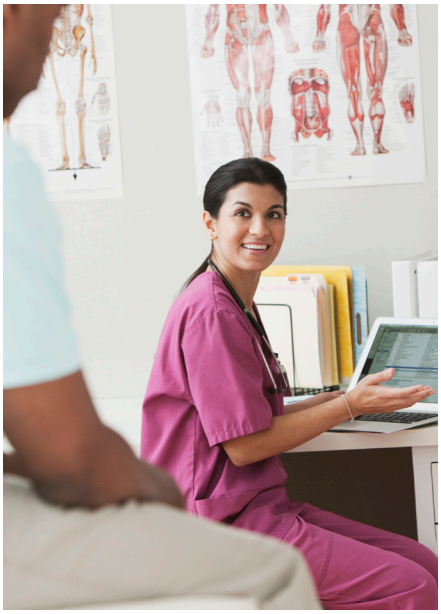
## Making security and privacy a priority

Moving to EHR systems and other forms of electronic communications can help the entire health community provide better patient care and enable physicians to improve the efficiency of their practices. The ability to share data electronically among providers and health plans can improve continuity and quality of care. In addition, financial incentives to adopt electronic medical records are available to help you take advantage of this new technology. With these benefits comes the added responsibility of protecting electronic PHI and meeting HIPAA standards for its use. The consequences for failure to do so, which include fines and penalties, are significant, and impact your personal and professional reputation.

## Protecting your own privacy

Beyond adhering to HIPAA regulations, there are simple steps that you as a physician can take to protect yourself and your practice from inadvertently compromising your privacy. For example, some physicians, especially those in smaller practices, still use their social security number as their provider identifier. Since other physicians, health plans and external entities refer to and transmit your provider identifier daily, using your social security number as a provider identifier puts you at considerable risk for identity theft and other fraud. To be more secure, obtain a separate tax identification number from the IRS (visit www.irs.gov for details). Additionally, CMS issues a national provider identifier (NPI) that is different from your social security number and is the industry standard for physician identification. If you do not have an NPI, one can be obtained, at no cost from: www.cms.gov/nationalprovidentstand/

Adopting and enforcing rigorous policies and procedures such as those outlined in this guide will help you manage risks while reaping the benefits that the use of electronic health information provides for your patients and your practice.



OptumInsight's clinical data philosophy is simple and clear. We believe that we have a responsibility to manage and protect your data and that of your patients.

OPTUM™ www.optum.com

12125 Technology Drive, Eden Prairie, MN 55344