TechTarget | SearchHealthIT

E-guide

PRO+ Content

# Guide to Healthcare Compliance Resources and Agencies

## In this e-guide

## In this e-guide:

**A collection of agencies regulate and govern the technological side of healthcare in the United States:**

- **The Department of Health and Human Services Office for Civil Rights (OCR)**
- **The Centers for Medicare and Medicaid Services (CMS)**
- **The Office of the National Coordinator for Health IT (ONC)**
- **The Food and Drug Administration (FDA) evaluates medical devices and classifies them by the level of risk they could present to users**

**This guide provides an overview of these regulatory bodies that govern the use of health IT through the law and by functioning as healthcare compliance resources.**

# Section 1: Terms to Know

There are 9 key regulations and agencies that you need to know:

- Centers for Medicare & Medicaid Services (CMS)
- Centers for Disease Control and Prevention (CDC)
- HIPAA (Health Insurance Portability and Accountability Act)
- Meaningful use
- ONC – Office of the National Coordinator for Health Information Technology
- Health Information Exchange (HIE)
- US Department of Health and Human Services (HHS)
- ICD-10
- Office for Civil Rights (OCR)

Continue reading

# Centers for Medicare & Medicaid Services (CMS)

The Centers for Medicare & Medicaid Services (CMS) is part of the U.S. Department of Health and Human Services. CMS oversees many federal healthcare programs, including those that involve health information technology such as the meaningful use incentive program for electronic health records (EHR).

## Reimbursement and regulatory functions

In addition to Medicare (the federal health insurance program for the elderly) and Medicaid (the federal needs-based program that helps with medical costs), CMS administers the Children's Health Insurance Program (CHIP), the Health Insurance Portability and Accountability Act (HIPAA) and key portions of the 2015 Medicare Access and CHIP Reauthorization Act (MACRA) law.

MACRA includes programs such as Merit-Based Incentive Payment System (MIPS) in which physicians and healthcare organizations are reimbursed based on their scores on healthcare quality and patient satisfaction measures. The approach is also known as value-based reimbursement. CMS also administers alternative payment models (APMs) for healthcare providers such as bundled payments for groups of healthcare organizations, and accountable care organizations, which are reimbursed based on positive medical outcomes.

Since passage of the Health Information Technology for Economic and Clinical Health Act in 2009, CMS has been charged with running the meaningful use program, which is in its final phase with nearly $30 billion of incentive funds having been paid out to healthcare providers.

Under meaningful use, and now the MIPS part of MACRA, CMS determines whether healthcare providers have successfully used health IT systems, and sets Medicare and Medicaid reimbursement rates for healthcare providers that use federally certified health IT systems.

## ONC-affiliated agency

The Office of the National Coordinator for Health Information Technology (ONC), another Health and Human Services agency that works closely with CMS, is responsible for approving certified health IT systems and updating health information privacy and security regulations under HIPAA.

Meaningful use has been credited for driving the widespread adoption of EHRs among hospitals and physicians. As of 2015, ONC reported that 96% of nonfederal acute care hospitals were using certified EHR systems. At the end of 2015, 56% of office-based physicians were using certified EHRs.

## History of CMS

After Medicare and Medicaid were established in 1965, the Social Security Administration -- through the then Department of Health, Education and Welfare -- administered federal health programs.

In 1977, the former Health Care Financing Administration (HCFA) took over administration of Medicare and Medicaid. In 2001, HCFA became CMS.

Next article

# Centers for Disease Control and Prevention (CDC)

The Centers for Disease Control and Prevention (CDC) is a federal agency that conducts and supports health promotion, prevention and preparedness activities in the United States with the goal of improving overall public health. Established in 1946 and based in Atlanta, the CDC is managed by the Department of Health and Human Services (HHS).

The CDC works with partners at the local, state and national level to monitor and prevent disease outbreaks (including bioterrorism), implement disease prevention strategies, and maintain national health statistics. The agency also leads public health efforts to prevent and control infectious and chronic diseases, injuries, workplace hazards, disabilities and environmental health threats. The CDC focuses on the following five strategic areas -- increasing support to local and state health departments, improving global health, decreasing leading causes of death, strengthening surveillance and epidemiology, and reforming health policies.

The CDC's disease prevention efforts include educating the public on how to recognize and avoid contracting common infectious diseases, such as the flu and strep throat. The CDC also monitors outbreaks of chronic diseases, including Ebola, which are often met with updates from the CDC on how to recognize and combat possible symptoms.

For people who believe they might have contracted an infectious disease, the CDC website shares guidance on how to test for the disease and avoid spreading it to others before they can receive treatment. More in-depth directions for treatment, including possible quarantine, are available for patients and healthcare workers that may have been exposed to more potent viruses, such as Ebola.

The CDC recognizes the importance of health IT and invests in information systems for a wide range of public health functions. These include the Public Health Information Network, a project tasked with developing standards for sharing public health information, and BioSense, a bioinformatics surveillance system. The Office of the Chief Information Officer (OCIO) provides governance and oversight of CDC's IT investments.

The CDC, along with the U.S. Senate, is examining the safety of EHRs and common causes of errors in electronic healthcare systems. Interoperability between EHRs and other internal hospital resources, such as lab systems, has been targeted as an area that could use improvement. The Public Health-EHR Vendors Collaboration Initiative was created in August 2013 by the CDC and the Office of the National Coordinator for Health IT with a primary focus on helping providers meet public reporting requirements set by the first two stages of the meaningful use program. The initiative has taken on other missions, including how to use EHRs to track patients for signs of Ebola.

Next article

# HIPAA (Health Insurance Portability and Accountability Act)

HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information. The act, which was signed into law by President Bill Clinton in August 1996, contains five sections, or titles:

- HIPAA Title I protects health insurance coverage for individuals who lose or change jobs. It also prohibits group health plans from denying coverage to individuals with specific diseases and pre-existing conditions, and from setting lifetime coverage limits.
- HIPAA Title II directs the U.S. Department of Health and Human Services to establish national standards for processing electronic healthcare transactions. It also requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS.
- HIPAA Title III includes tax-related provisions and guidelines for medical care.
- HIPAA Title IV further defines health insurance reform, including provisions for individuals with pre-existing conditions and those seeking continued coverage.
- HIPAA Title V includes provisions on company-owned life insurance and treatment of those who lose their U.S. citizenship for income tax purposes.

In IT circles, adhering to HIPAA Title II is what most people mean when they refer to *HIPAA compliance*. Also known as the Administrative Simplification provisions, Title II includes the following HIPAA compliance requirements:

- **National Provider Identifier Standard.** Each healthcare entity, including individuals, employers, health plans and healthcare providers, must have a unique 10-digit national provider identifier number, or NPI.
- **Transactions and Code Sets Standards.** Healthcare organizations must follow a standardized mechanism for electronic data interchange (EDI) in order to submit and process insurance claims.
- **HIPAA Privacy Rule.** Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule establishes national standards to protect patient health information.
- **HIPAA Security Rule.** The Security Standards for the Protection of Electronic Protected Health Information sets standards for patient data security.
- **HIPAA Enforcement Rule.** This rule establishes guidelines for investigations into HIPAA compliance violations.

In 2013, the HIPAA Omnibus Rule was put in place by HHS to implement modifications to HIPAA in accordance with guidelines set in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act concerning the responsibilities of business associates of covered entities. The omnibus rule also increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident.

HIPAA violations can prove quite costly for healthcare organizations. First, the HIPAA Breach Notification Rule within the omnibus set of regulations requires covered entities and any affected business associates to notify patients following a data breach. In addition to the notification costs, healthcare organizations can encounter fines after HIPAA audits mandated by the HITECH Act and conducted by the Office for Civil Rights (OCR). Providers could also face criminal penalties stemming from violations of the HIPAA privacy and security rules.

Organizations can lower their risk of regulatory action through HIPAA compliance training programs. The OCR has six educational programs on complying with the privacy and security rules; a number of consultancies and training groups offer programs as well. Healthcare providers may also choose to create their own training programs, which often encompass each organization's current HIPAA privacy and security policies, the HITECH Act, mobile device management processes and other applicable guidelines.

While there is no official HIPAA compliance certification program, training companies offer certification credentials to indicate an understanding of the guidelines and regulations specified by the act.

↘ Next article

# Meaningful use

Meaningful use (MU), in a health information technology (HIT) context, defines minimum U.S. government standards for using electronic health records (EHR) and for exchanging patient clinical data between healthcare providers, between healthcare providers and insurers, and between healthcare providers and patients.

Its rules, known as meaningful use measures or meaningful use criteria, determine whether or not a healthcare provider may receive federal funds from the Medicare EHR Incentive Program, the Medicaid EHR Incentive Program or both, in cases of "dually eligible" practitioners (EP) and eligible hospitals (EH).

## Meaningful use stage 1, stage 2, stage 3

Meaningful use is divided into three stages. Stage 1, which began in 2010, focused on promoting adoption of EHRs. Stage 2, finalized in late 2012, increases thresholds of criteria compliance and introduces more clinical decision support, care-coordination requirements and rudimentary patient engagement rules. Stage 3, which the Centers for Medicare & Medicaid Services (CMS) rulemakers are writing from late 2014 through early-to-mid 2016, will focus on robust health information exchange as well as other more fully formed meaningful use guidelines introduced in earlier stages.

According to the provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, organizations that are eligible for the Medicare EHR Incentive Program and achieve meaningful use by 2014 will be eligible for incentive payments; those who have failed to achieve that standard by 2015 will be penalized, unless Congress overrides that portion of the 2009 HITECH Act that codified CMS's rulemaking timeline into law.

While meaningful use is voluntary, it is often referred to as a carrot-and-stick program whose penalties provide a strong economic compulsion to participate.  Penalties against Medicare and Medicaid reimbursements for skipping meaningful use will increase in each successive year, expressed as a "payment adjustment" or reduction of a provider's reimbursement for care provided to Medicare or Medicaid patients. If fewer than 75% of EPs have become meaningful users of EHRs by 2018, the adjustment will change by 1% point each year to a maximum of 5%.

But because the meaningful use program is technically voluntary, meaningful use criteria are considered to be guidelines, as opposed to meaningful use regulations.

## ONC Meaningful Use Certified EHR Technology (CEHRT)

Healthcare providers can only prove compliance with meaningful use while using government-certified EHR technology, commonly referred to as

CEHRT. Meaningful use criteria for healthcare providers are written by CMS, with input from the Office of the National Coordinator for Health IT (ONC). EHR vendors, however, get their systems certified under rules written by the ONC, which currently are updated yearly. Some years CEHRT rules are voluntary, in other years they're mandatory.

CMS has indicated that all CEHRT rules, in the future, may be tied to one or more of its provider reimbursement programs beyond meaningful use, such as the Physician Quality Reporting System (PQRS), a voluntary program that rewards providers who can prove they meet specific care-quality measures.

The net effect of requiring meaningful use CEHRT for other programs will be de facto forcing vendors to certify their EHRs in years when CEHRT rules are voluntary, if they want to hold on to customers in the programs for which CMS requires CEHRT such as, potentially, PQRS.

## Meaningful use attestation, meaningful use penalties, meaningful use audits

To have received the maximum reimbursement, physicians and hospitals must have attested (essentially, swearing to a CMS website that one has met all of the criteria for a particular stage) stage 1 of meaningful use of EHR for at least a 90-day period within the 2011 or 2012 federal fiscal year and for the entire year thereafter.

While there is little validation required to attest to meaningful use, providers who have attested are subject to random audits, sometimes before CMS cuts their next incentive check, sometimes after the fact. Keeping detailed documentation proving meaningful use is essential to passing the audits and keeping EHR incentive program funds. Many providers who have failed audits as of late 2014 have done so because of inadequate or nonexistent HIPAA risk assessments, which are required under meaningful use.

Those eligible for the Medicaid program must demonstrate meaningful use by 2016 in order to receive incentive payments. Many healthcare providers attested to stage 1 in its early years in order to receive the maximum incentives from Medicare, Medicaid or both; in 2015 and 2016, many of these providers are expected to drop out as stage 2 attestation becomes due, because of the difficulty in attesting. Those who have attested cite the "view, download and transmit" criteria as well as care-coordination criteria to be the most difficult with which to comply.

## Recent changes to meaningful use stage 2 and stage 3 timelines

To help potential program dropouts stay in the program, CMS adjusted timelines for meaningful use. In a 2014 final rule, CMS extend Stage 2 through 2016 and delayed the start of Stage 3 until 2017. These proposed changes, CMS said, "would address concerns raised by stakeholders and will encourage the continued adoption of Certified EHR Technology."

Further changes may be legislated by Congress if bills up for consideration become law. For example, beginning in 2015, all eligible hospitals and professionals on the Medicare EHR Incentive Program side must use CEHRT based on 2014 standards. And, to attest to stage 2 and avoid future penalties, they must attest for the full calendar 2015. The Flex-IT bill before Congress, advocated by many healthcare providers, proposes reducing that to 90 days, pegged to any calendar quarter.

Next article

## ONC - Office of the National Coordinator for Health Information Technology

The Office of the National Coordinator for Health Information Technology, abbreviated ONC, is a position within the US Department of Health & Human Services (HHS). The position was created by Executive Order in 2004 and written into legislation by the HITECH Act. The ONC's purpose is to promote a national health Information Technology infrastructure and oversee its development.

The ONC's mission involves many aspects of health information technology (HIT ), including policy coordination, strategic planning for the adoption of health IT and health information exchanges (HIE), establishing governance for the  Nationwide Health Information Network and, above all, promoting a national health IT infrastructure. This last mission, according to the ONC, aims, among other things, to improve the quality of health care while reducing costs; improve the coordination of care and information among hospitals, labs, physicians and other health care organizations; ensure that personal health records (PHR) remain secure, and promote the early detection, prevention and management of chronic illness.

For the ONC to do its work, significant upgrades to health IT systems across the country will be necessary. To that end, and in response to provisions of the HITECH Act, the ONC drafted an interim final rule for an initial set of standards, implementation specifications and certification criteria for electronic health record (EHR) systems. This rule was released on Dec. 30, 2009, which was the same day the Centers for Medicare & Medicaid Services, or CMS, released a notice of proposed rulemaking for meaningful use. Health care providers must demonstrate meaningful use of a certified EHR system in order to qualify for financial incentives under the HITECH Act. Both sets of rules are open to public comment and will be finalized later in 2010, with the first awards to hospitals and eligible health care providers coming in 2011.

Also in response to the HITECH Act, the ONC is reviewing proposals for the formation of up to 70 Regional Extension Centers (RECs) which will receive federal funding to help hospitals and community clinics in their area make the transition from paper-based to EHR systems.

Next article

# Health information exchange (HIE)

Health information exchange (HIE) is the transmission of healthcare-related data among facilities, health information organizations (HIO) and government agencies according to national standards. HIE is an integral component of the health information technology (HIT) infrastructure under development in the United States and the associated National Health Information Network (NHIN).

To meet requirements, HIE technology must enable reliable and secure transfer of data among diverse systems and also facilitate access and retrieval data. The purpose of HIE development is to improve healthcare delivery and information gathering.

Next article

# US Department of Health and Human Services (HHS)

The U.S. Department of Health and Human Services (HHS) is part of the federal government. Its mission is to enhance and protect the well-being of all Americans by providing effective health and human services and fostering advances in medicine, public health and social services. HHS is responsible for administrating programs that deal with health, welfare and health IT. The Department works with almost one-fourth of all federal government expenditures and administers more grant dollars than all other federal agencies combined. HHS' programs are administered by 11 operating divisions:

- Administration for Children and Families (ACF)
- Administration for Community Living (ACL)
- Agency for Health Research and Quality (AHRQ)
- Agency for Toxic Substances and Disease Registry (ATSDR)
- Centers for Disease Control and Prevention (CDC)
- Centers for Medicare & Medicaid Services (CMS)
- Food and Drug Administration (FDA)
- Health Resources and Services Administration (HRSA)
- Indian Health Service (IHS)
- National Institutes of Health (NIH)
- Substance Abuse and Mental Health Services Administration (SAMHSA)

HHS also includes the U.S. Public Health Service Commissioned Corps (USPHS), which is overseen by the surgeon general.
However, another important aspect of HHS' job is overseeing the implementation of certain types of health IT. The agency has been active in this area in several ways, including:

- Providing guidance for healthcare application development;
- Providing guidance to protect against ransomware attacks;
- Working toward fully understanding new cutting-edge technology such as blockchain; and
- Actively administering a health IT infrastructure.

Furthermore, the Secretary of HHS Sylvia Burwell has become a leader in the health IT space, including publicly speaking out about the adoption of electronic health records (EHR) and data blocking.

## Centers for Medicare & Medicaid Services (CMS)

CMS administers the Medicare and Medicaid programs as well as oversees the Children's Health Insurance Program (CHIP), the Health Insurance Portability and Accountability Act (HIPAA), the Clinical Laboratory Improvement Amendments (CLIA) and more.

In 2009, CMS was charged with several key tasks for advancing health IT via the Health Information Technology for Economic and Clinical Health (HITECH) Act, including the implementation of EHR incentive programs, defining the meaningful use of certified EHR technology, drafting standards for the certification of EHR technology, and updating the health information privacy and security regulations under HIPAA.

Many of these efforts are being done in conjunction with the Office of the National Coordinator for Health Information Technology (ONC), which also comes under HHS.

## Office of the National Coordinator for Health Information Technology

Former President George W. Bush created the ONC in 2004 and the office was written into legislation by the HITECH Act. The ONC's purpose is to promote a national health IT infrastructure and oversee its development. This includes policy coordination, strategic planning for the adoption of health IT and health information exchanges (HIE), establishing the Nationwide Health Information Network and promoting a national health IT infrastructure.

The ONC aims to achieve its ultimate goal, promoting a national health IT infrastructure, by improving the quality of healthcare while reducing costs; improving the coordination of care and information among hospitals, labs, physicians and other healthcare organizations; ensuring that personal health records (PHR) remain secure; and promoting the early detection, prevention and management of chronic illnesses.

In this e-guide

## ICD-10

The International Classification of Diseases, Tenth Edition (ICD-10) is a clinical cataloging system that went into effect for the U.S. healthcare industry on Oct. 1, 2015, after a series of lengthy delays. Accounting for modern advances in clinical treatment and medical devices, ICD-10 codes offer many more classification options compared to those found in predecessor ICD-9.

Within the healthcare industry, providers, coders, IT professionals, insurance carriers, government agencies and others use ICD codes to properly note diseases on health records, track epidemiological trends, and assist in medical reimbursement decisions.

The World Health Organization (WHO) owns, develops and publishes ICD codes, and national governments and other regulating bodies adopt the system.

In the U.S., ICD-10 is split into two systems: ICD-10-CM (Clinical Modification) for diagnostic coding and ICD-10-PCS (Procedure Coding System) for inpatient hospital procedure coding. These U.S.-specific adaptions conform to WHO's ICD-10 layout while allowing for additional details found in U.S. healthcare. The U.S. took a similar approach with ICD-9-CM and ICD-9-PCS.

The ICD-10 code list greatly expands classification options.

For example, ICD-10-CM has 68,000 codes, compared to 13,000 in ICD-9-CM, according to the Centers for Medicare & Medicaid Services (CMS).

The ICD-10 conversion in the U.S. was delayed by lobbying, politics and general opposition to the increased amount of codes in the newer set. Here is a brief history of those delays:

- Jan. 16, 2009 -- The U.S. Department of Health and Human Services (HHS) published a final rule establishing ICD-10 as the new national coding standard, with an adoption date of Oct. 1, 2013.
- Aug. 24, 2012 -- HHS announced a delay in ICD-10 adoption from Oct. 1, 2013, until Oct. 1, 2014, to allow healthcare systems more time to prepare for the transition.
- March 2013 -- At the 2013 HIMSS (Healthcare Information and Management Systems Society) meeting, a CMS administrator said ICD-10 would not be delayed past Oct. 1, 2014.
- April 1, 2014 -- President Obama signed a Medicare reimbursement bill from Congress that included a delay in ICD-10 implementation from Oct. 1, 2014, until Oct. 1, 2015.

The U.S. used ICD-9 from 1979 to 2015. In those 35-plus years, supporters of ICD-10 said its predecessor has become obsolete, didn't account for modern healthcare practices, and lacked ICD-10's specificity for clinical diagnoses and medical device coding.

For example, if a patient broke a wrist, ICD-9 did not specify whether it was the left or right wrist, while ICD-10 offers either option. ICD-10 also presents additional details on when a patient is seen by a caregiver and how an injury or disease is progressing or healing. ICD-9's codes are based on three to five letters and numbers, while ICD-10's are based on three to seven letters and numbers.

Ironically, ICD-10 itself is 25 years old, having first been adopted by WHO in 1990. Some countries began using ICD-10 codes in 1994.

Meanwhile, the upcoming ICD-11 is under development now, and WHO will release the update in 2017.

↘ Next article

# Office for Civil Rights (OCR)

The Office for Civil Rights (OCR) is an organization within the U.S. Department of Health & Human Services (HHS). OCR works closely with both doctors and patients to ensure that every patient knows their rights and privacies concerning personal health information and medical treatment options.

With the Health Information Technology for Economic and Clinical Health Act, or HITECH Act, calling for the widespread adoption of electronic health record (EHR) technology, many patients and their families are concerned that electronic information is more susceptible to a data breach than traditional paper-based files. The OCR helps organizations teach health and social service workers about the civil rights, health information privacy and patient confidentiality laws that they, as medical professionals, must follow.

As a government agency, the OCR also investigates health information privacy and patient safety confidentiality complaints to decide if a discriminatory act or a violation of law has occurred and takes action to correct those problems. Under the HITECH Act's updates to the Health Insurance Portability and Accountability Act (HIPAA), the OCR can levy significant fines to health care providers and their business associates if personal health information is lost or stolen.

Next article

In this e-guide

# Section 2: OCR and HIPAA Compliance

The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) is responsible for enforcing HIPAA Privacy and Security Rules. To this end, the OCR investigates privacy violations and enforces penalties for noncompliance.

Prior to the HITECH Act, the OCR only audited a HIPAA covered entity when a patient filed a complaint with the agency. However, the HITECH Act now requires the OCR to conduct periodic audits of providers and HIPAA business associates to ensure they are HIPAA compliant.

In addition to holding covered entities accountable, the OCR publishes HIPAA Privacy Rule guidance materials, which are intended to help organizations meet requirements for compliance. The OCR also provides a variety of healthcare compliance resources in the form of training materials and guidance materials for covered entities.

Continue reading

# Expert warns OCR HIPAA audits ahead

**Shaun Sutner,** News and Features Writer

Download this podcast

HIPAA audits of healthcare providers and their business associates are coming soon, warns David Holtzman, a lawyer and vice president for compliance for health data privacy and security consulting firm CynergisTek, Inc.

Holtzman knows of what he speaks when it comes to HIPAA audits, because he served from 2005 to 2013 as the U.S. Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) senior adviser for health information privacy.

Now, after months of delays, Holtzman says he expects OCR to launch at least "desk" audits conducted mainly remotely by interview sometime this year, with more comprehensive on-site audits in 2016 and beyond.

Meanwhile, Holtzman warns in this podcast -- the first of a two-part series -- that healthcare providers large and small should fortify their HIPAA programs rather than risk fines, and even worse, health data breaches that damage customers and harm companies' reputations.

At a minimum, it is imperative that providers maintain risk management plans and organizational policies governing which employees get access to protected health information. Also critical, Holtzman says, are policies and processes for evaluating the potential for breaches and notifying OCR when they occur.

Healthcare systems, hospitals and physicians that have participated in HHS' meaningful use program will be better prepared, he notes.

That is because many of the measures to which providers have to attest are built into HIPAA compliance, and are, indeed, based on the HIPAA privacy and security rules.

One such feature actually has to do with patients' ability to get their hands on their own health data -- a HIPAA requirement -- via secure electronic portals.

Holtzman says he finds it troubling that there has been a nearly 25% meaningful use audit failure rate, a trend that does not portend well for HIPAA audits.

Next article

# HIPAA audits to affect healthcare business associates

**Shaun Sutner,** News and Features Writer

Download this podcast

It's not only healthcare providers that should get ready for the upcoming round of HIPAA audits by the U.S. Department of Health and Human Services Office for Civil Rights (OCR).

David Holtzman, a lawyer and vice president for compliance for health data privacy and security consulting firm CynergisTek, Inc., warns that healthcare business associates, such as insurers and claims processing firms, should also be on guard.

"The prospects are very great that business associates will find themselves subject to enforcement of HIPAA privacy and security rules," Holtzman says in this podcast, the second of a two-part series. "This has been on OCR's radar for a long time, and I expect they are going to be rather aggressive in making sure business associates are in compliance and are safeguarding health information."

It is still unclear, however, whether healthcare business associates will be subject to fines.

Meanwhile, Holtzman, a former senior OCR official, says providing patients with timely access to their own health information helps them make more informed decisions about their healthcare.

Also, such health data transparency can allow third parties to better evaluate the business processes of provider organizations, Holtzman says.

Therefore, such access, which is required by the HIPAA omnibus rule, will also be fodder for audits expected in 2015 and 2016, he says.

*See transcript below:*

**How significant is the prospect of business associates being audited and possibly fined by OCR?**

David Holtzman: I think the prospects are very great that business associates are going to find themselves subject to enforcement activities for compliance with the HIPAA privacy and security rules. In addition, OCR has indicated that they will include business associates in a separate review that will take place as, sort of, a second step in their process for doing desk audits. My understanding from OCR is that they are actively engaged in investigations of business associates who have been responsible for breaches that have been reported, as well as complaints from consumers alleging that the business associate has not complied with the requirements for the HIPAA security rules or the use and disclosure provisions of the privacy rule.

I know that OCR was anticipating that when the rules came into effect, or the compliance date in 2013 took effect, that there [would] be opportunities to look at the practices of some business associates. And, in fact, between the time the HITECH Act was passed into law and the compliance date of the Omnibus Rules expanding the jurisdiction of the HIPAA rules to business associates, a number of cases came up involving breaches and other allegations of inappropriate use and disclosure of protected health information by business associates. Information regarding those cases was shared with other federal agencies who had enforcement power over the use of information like health information.

So this has been on OCR's radar for a long time, and I expect that they are going to be rather aggressive in making sure that business associates are in compliance and are safeguarding health information as they are required to do through the HIPAA security rule and the provisions of the privacy and breach notification rules.

**Are patients' rights to protected health information (PHI) as important as the privacy of that data? How do we weigh the relative importance of those two issues?**

Hotlzman: I don't think that the privacy of health information is distinctly different from an individual's rights regarding the use and disclosure of or access to their protected health information. I think they're part of the same, and they really support each other. So the HIPAA privacy rules essentially put controls on health care providers, business associates and health plans [to restrict] how they use and disclose protected health information, so as to not interfere with the provision of treatment -- but to allow individuals some ability to understand how their information is used and disclosed for payment purposes, as well as for health care operations and other activities like fundraising and marketing.

[The goal is] to make it more transparent and to allow individuals choices in how their information is used outside of the usual, [like in the] everyday business of health care, in which they are receiving treatment. Their health insurers are paying for that treatment. Health care, as a business, carries on its activities and planning and engaging in forecasting how it can provide services to patients better.

Next article

# Section 3: Meaningful Use Attestation

The Centers for Medicare and Medicaid Services (CMS), also a division of HHS, is responsible for the administration of Medicare, Medicaid and the Children's Health Insurance Program.

The HITECH Act also adds several key tasks to CMS' list of responsibilities that are intended to advance health IT. To this end, CMS is charged with the following:

-- Implementing the federal government's EHR Incentive Programs

-- Defining criteria for meaningful use of certified EHR technology

-- Drafting standards for the certification of EHR technology

-- Updating HIPAA health information privacy and security regulations

CMS also oversees the ICD-10 program.

Continue reading

In this e-guide

# CHIME, athenahealth lukewarm to meaningful use stage 3

**Shaun Sutner,** News and Features Writer

Beyond the expected focus on increased patient access to health data, medical outcomes, and clinical quality and safety, proposed rules for meaningful use stage 3 and vendor certification also contain new features, such as APIs for electronic health records (EHR) systems and patient-generated health data from wellness devices.

And the 300 pages of modifications to the HITECH Act of 2009, which originally created meaningful use, contain few mentions of financial incentives now that most of the $30 billion for providers to digitize health records has been spent -- but it does include extensive language about reduced Medicare and Medicaid reimbursement.

"We've gone from the carrot to the stick," said Charles Christian, chairman of the board of the College of Healthcare Information Management Executives (CHIME), and vice president and CIO at St. Francis Hospital in Columbus, Ga. "Now it's about avoiding penalties."

## Patient engagement, API challenges

The new "view, download and transmit" measure -- which has given many physicians and hospital officials trouble when it required only 5% of patients to electronically obtain their health data -- will be hard to achieve at the 25% required in the proposed rule, Christian said.

"We've struggled as organizations with that," Christian said.

On the vendor side, provider CIOs will closely watch the new stage 3 EHR certification rules for the proposed 2015 Edition released by the U.S. Office of the National Coordinator (ONC) for Health IT for how vendors incorporate data-sharing APIs into new EHR platforms, Christian said.

APIs are seen by interoperability advocates as the means by which health data will be exchanged more easily than it is now, both between EHRs from competing vendors and between providers and other providers.

API advocates claim API-based interoperability -- of which the fast-developing Fast Health Interoperability Resources standard is one current example backed by ONC -- will be less expensive and cumbersome than Direct messaging and many HIEs.

Many providers that have struggled to attest to meaningful use stage 2 have cited technical problems with HIEs and Direct in exchanging health data with other providers.

One vendor, athenahealth Inc. of Watertown, Mass., gave a similarly ambivalent review to the new stage 3 vision.

"We are pleased ... that the stage 3 proposed rules move beyond check-boxes and provider micromanagement to focus more deliberately on the need to foster actual interoperation in healthcare," Dan Haley, athenahealth's vice president of government and regulatory affairs, said in an email.

However, Haley said that while athenahealth -- which prides itself on the openness of its cloud-based systems -- pledges to enable its clients for stage 3 requirements, the company is disappointed that the proposed rules do not go farther. A bill filed by U.S. Rep. Michael Burgess, M.D., (R-Texas) to legally mandate EHR interoperability would do more for "information sharing and openness," Haley said.

"As written, we believe the proposed rules make incremental improvements to the struggling MU program, but will do little to achieve the potential of information technology to vastly improve care delivery and efficiency in healthcare," Haley added.

## HHS wants guidance on wearables data

One unusual aspect of the unveiling of the new rules for providers is the extensive amount of input that CMS solicited not only in the introduction, but also in the statutory text of the document, Christian said.

"One of the biggest surprises was how much CMS is asking for more comment ," Christian said. "I think they truly are asking for more feedback."

Among the areas in which federal health IT officials are soliciting guidance is how to use patient-generated data from wearable wellness devices and tracking systems.

Christian expressed skepticism about that effort, saying it is difficult for hospitals to oversee how primary care physicians get and use wellness information, including data about physical activity, blood pressure, heart rate and body weight.

"It seems like Apple and others got their wish to get their information into our records," Christian said, referring to Apple Corp.'s Health Kit app, which appears to be emerging as a standard of sorts for wellness devices from various manufacturers. Microsoft. Corp. and other companies also have health apps.

## Stage 3 will be hot at HIMSS

Following HHS' release on Friday of the proposed meaningful use provider rule and a related vendor certification rule, there is a public comment period until May 29 for both draft regulations. Under the proposal, providers will start attesting to meaningful use stage 3 -- the final stage of the program -- in 2017, and new Medicare payment adjustments would take effect in 2018.

With the short comment period, providers, vendors and others in health IT will likely make stage 3 a top discussion item at the HIMSS 2015 annual conference in Chicago next month, Christian said. Karen DeSalvo, M.D., national health IT coordinator, is slated to make the final keynote at the event.

Christian said that while healthcare CIOs will take many of the proposed new requirements in stride, they are bound to be unhappy with a mandated 365-day reporting period for stage 3 for most providers and a dramatic increase in the number of patients required to use electronic health portals.

## Federal officials say stage 3 is progress

It's clear healthcare regulators think the stage 3 and vendor certification drafts offer a step in the right direction. "ONC's proposed rule will be an integral component in the shared nationwide effort to achieve an interoperable health system," DeSalvo said in an HHS release.

"The certification criteria we have proposed in the 2015 Edition will help achieve that vision through provisions that consider the range of health IT users and uses across the care continuum, including those focused on interoperable standards, data portability, improved transparency, privacy and security capabilities, and increased oversight," DeSalvo said.

CMS' top meaningful use official, Patrick Conway, M.D., the agency's acting deputy administrator and chief medical officer, said in the HHS release that the proposed stage 3 rules simplify meaningful use, advance health IT by improving healthcare quality and align meaningful use with HHS' value-based reimbursement program.

The proposed measures for providers are grouped in 18 main categories, with 15 new core measures, fewer than in stage 1 and stage 2.

"That doesn't make it any less difficult," Christian said.

Next article

In this e-guide

# Meaningful use stage 3 proposed rule tweaks EHR program

**Reda Chouffani,** Co-founder – Biz Technology Solutions

Healthcare providers working to qualify for EHR incentive payments and avoid payment adjustments have a new set of criteria to prepare for. The Centers for Medicare and Medicaid Services released a proposal for the third -- and what is expected to be the final -- stage of the meaningful use program, in which it details the final requirements to be met by participating eligible professionals and hospitals.

The meaningful use stage 3 proposed rule represents the culmination of the EHR incentive project that began as part of the HITECH Act. The broad goal of the meaningful use program is to encourage eligible professionals (EPs) and eligible hospitals (EHs) to use more health IT tools. More specifically, the program is set up to promote collaborative and less costly patient care through health information exchange and data interoperability.

The meaningful use stage 3 proposed rule lists several significant changes that will affect incentive program participants. Stage 3's preliminary emphasis is on reducing the complexity of the program established during stages 1 and 2.

## Meaningful use in 2017 and beyond

If the proposal stands, EPs and EHs will face a year-long attestation period. The only exception to that rule will be Medicaid EPs and EHs that attempt to demonstrate meaningful use for the first time. They will have to attest only for the duration of the current 90-day period. The reporting period for stage 3 will begin in 2017, when it will be optional for participants. In 2018, it becomes required for all EPs and EHs.

## Requirements, objectives and measures

To simplify the set of requirements in this stage, HHS has proposed a limited set of eight objectives to help achieve the goals of the final stage.

**Objective 1: Protect patient health information** -- Providers will have to guard patients' electronic protected health information by maintaining physical and technical security measures.

**Objective 2: Electronic prescribing** -- Under the proposed objective, EPs would have to electronically create and transmit prescriptions to patients.

**Objective 3: Clinical decision support** -- Stage 3 would have clinical decision support efforts target improvement in treating high-priority conditions.

**Objective 4: Computerized provider order entry (CPOE)** -- Credentialed medical staff will be able to use CPOE for laboratory, diagnostic imaging and medication orders under the stage 3 proposal.

**Objective 5: Patient electronic access to health information** -- Patients will be offered access to their health information through an API within 24 hours of its availability.

**Objective 6: Coordination of care through patient engagement** -- This objective would have providers interact with patients about their care through certified EHR technology (CEHRT).

**Objective 7: Health information exchange** -- EPs, EHs or critical access hospitals will receive and transmit a patient's summary of care record as that patient moves between different care facilities.

**Objective 8: Public health and clinical data registry reporting** -- This proposed objective would have meaningful use participants communicate with and share health data with public health agencies or clinical data registries.

## Payment adjustments and hardship exceptions

The meaningful use stage 3 proposed rule would permit the following four exceptions that would excuse providers from incentive payment adjustments:

- "The lack of availability of Internet access or barriers to obtain IT infrastructure.
- A time-limited exception for newly practicing EPs or new hospitals that would not otherwise be able to avoid payment adjustments.
- Unforeseen circumstances such as natural disasters that would be handled on a case-by-case basis.
- (EP only) exceptions due to a combination of clinical features limiting a provider's interaction with patients or, if the EP practices at multiple locations, lack of control over the availability of CEHRT at practice locations constituting 50 percent or more of their encounters."

## Summary of costs and benefits

The federal costs of the Medicare and Medicaid EHR Incentive Programs between 2017 and 2020 is projected to be approximately $3.7 billion. The stage 3 proposal does not contain a sum cost estimate for healthcare providers as a group, but suggests that segment of the healthcare industry can derive significant value from the meaningful use program by improving population health, reducing patient and operational costs, and increasing patient safety and outcomes.

Providers may welcome the flexibility offered to them in the stage 3 proposal. If they have additional changes or other feedback to offer CMS, it must be received by the May 29, 2015 deadline.

# Stage 2 woes may temper the effect of stage 3 meaningful use

**Scott Wallask,** Editorial Director

The soapboxes of healthcare IT littered the streets of Washington, D.C., during a recent, particularly lively week -- and in the aftermath, it's possible that stage 3 meaningful use reporting faces some changes.

To be clear, stage 3 isn't on the chopping block. But enough evidence is lying around from debates, press releases and political ballyhoos to suspect that the final stage 3 attestation rules may get a makeover before things settle down.

For example, the College of Healthcare Information Management Executives (CHIME) is hopeful that past tugs-of-war over meaningful use will lead to a final version of stage 3 that favors a patient-outcome-based reporting model over the initial proposal's metric-based approach, said Russell Branzell, FCHIME, CHCIO, president of the organization.

Generally, stage 3 further pushes physicians and hospitals to delve into the digital word with medical records and data interoperability. For example, the proposed rule recommends that clinicians should record notes in EHRs for more than 30% of patient office visits within four calendar days.

The health IT buzz in our nation's capital hit a flurry Feb. 10-11, as evidenced by the following declarations:

- "Eligible professionals hit with $200M in EHR penalties" -- iHealthBeat.org headline
- "Meaningful use is still broken" -- American Medical Association (AMA) press release

## Not quite kicked to the curb, but ...

Wait a minute: What does ICD-10's scheduled implementation on Oct. 1 have to do with meaningful use?

Although ICD-10 is not direct competition to reporting attestation, the disease classification system is a long-delayed behemoth of a mandate that could distract attention from stage 3 meaningful use discussions. Another factor to add in: Officials at the U.S. Office of the National Coordinator for Health IT want to talk more about health data interoperability these days, and not as much about meaningful use.

Branzell doesn't buy that ICD-10 has the aura to sweep stage 3 completely aside. The current administration will push forth some version of stage 3 because it would be difficult to uncouple it from EHR laws without incurring a political battle, he said.

## Eligible professionals backed into a corner

Notwithstanding stage 3's chances in the limelight, eligible professionals already aren't enamored with meaningful use, having struggled with stage 2 reporting. As a result, the AMA has long pressed for more meaningful use flexibility for physician practices on the grounds that it takes plenty of time and money to comply -- efforts that are better spent elsewhere, AMA President Stephen J. Stack, M.D., said in a release on Feb. 11.

"In order to successfully attest, physicians must spend tens of thousands of dollars for tech support, software upgrades, interfaces and data exchange, often on a recurring basis," Stack said.

His comments came after a CMS official estimated that 256,000 eligible providers (out of 384,000 nationwide) will need to repay some of their incentive payments because they were not able to fully attest to meaningful use in 2014. Elisabeth Myers, policy and outreach leader for CMS' Center for Clinical Standards and Quality, presented these figures to the joint federal Health IT Policy and Standards committees. CMS provided *Pulse* with a copy of her slides.

Hospitals fared better: 4,090 out of 5,700 U.S. hospitals attested to meaningful use in 2014, according to Myers.

The difficulties faced by some physicians and organizations to meet stage 2 reporting prompted the AMA, CHIME and other industry groups to pressure CMS to reduce stage 2 reporting requirements. The agency responded in their favor in January by proposing to update its Medicare and Medicaid EHR Incentive Programs in the following ways:

- Adjust hospital EHR reporting periods to the calendar year to allow eligible hospitals more time to install and implement 2014 edition software.
- Modify other aspects of the program to match long-term goals, reduce complexity, and lessen provider reporting burdens.
- Shorten the meaningful use reporting period in 2015 from 365 days to 90 days to accommodate these changes.

The feds intend to release stage 3 requirements in parallel with the proposed changes to stage 2. If government plans go as scheduled, the final stage 3 rule will be out near the time you read this article. It won't be clear until then what the healthcare industry's influence has been on the final requirements (see Reda Chouffani's article for more about this aspect). But Branzell said wording in the CMS announcement about the 90-day reporting implies that the agency will offer more flexibility during the transition to stage 3.
A CMS spokesperson said because the rule is still in development, the agency would not comment about stage 3 details or whether officials expected any resistance from the industry.

Next article

# Stage 2 stats tell tale of meeting meaningful use measures

**Reda Chouffani,** Co-founder – Biz Technology Solutions

With the potential that stage 2 meaningful use measures may undergo revisions in response to industry pressure, it's interesting to look back at the latest round of statistics to see what percentages of hospitals and eligible professionals were ready for stage 2.

The data curated by the ONC and CMS pinpointed that, as of November 2014, 56% of all hospitals eligible for the meaningful use program were qualified for meaningful use stage 2, compared to only 42% of eligible professionals (EPs) at the same point in time.

There was also proof that most of the hospitals eligible for stage 2 were prepared before December. Through last November, more than three-quarters (77%) of stage 2-eligible hospitals had attested for the 2014 reporting. These numbers could be taken as a sign that the monthlong extension provided by CMS was needed and taken advantage of by some providers.

Turning to EPs, nearly 60% of those that attested to meaningful use in 2014 did so to stage 2 of the program -- ahead of the Feb. 28 deadline for the 2014 reporting period. The figures from CMS and ONC also showed that historically, a portion of EPs and eligible hospitals didn't submit their attestation documentation until after the close of the fiscal or calendar year.

As for any physicians and hospitals that have not attested and don't plan on participating in either of the two meaningful use stages, CMS will continue to impose a 1% reduction in their Medicare reimbursement payments. EPs and hospitals can avoid that penalty if they apply for and receive a meaningful use hardship exception.

CMS announced in January that it intends to relax its meaningful use reporting period to 90 days for stage 2 in 2015, a move that industry groups such as the College of Healthcare Information Management Executives and the American Medical Association pushed hard for.

Specifically, CMS proposed to update its Medicare and Medicaid EHR Incentive Programs to accomplish the following goals:

- Adjust hospital EHR reporting periods to the calendar year to allow eligible hospitals more time to install and implement 2014 edition software.
- Modify other aspects of the program to match long-term goals, reduce complexity and lessen provider reporting burdens.
- Shorten the EHR reporting period in 2015 to 90 days to accommodate these changes.

Once published, the proposal will go through a public comment period. Representatives from CMS and ONC presented the meaningful use stage 2 statistics at a gathering of the Health IT Policy Committee in January.

In this e-guide

# Proposed CMS rule guides Shared Savings Program

**Reda Chouffani,** Co-founder – Biz Technology Solutions

In an effort to shift healthcare from a fee-for-service payment model toward a care quality-based model, CMS continues to offer support and incentives to physicians that form or join an accountable care organization. With that in mind, CMS has released a proposed rule that aims to improve care coordination within ACOs as part of the agency's Shared Savings Program. The industry can submit comments about the proposal through February 6, 2015.

More than 330 accountable care organizations (ACOs) are members of the Shared Savings Program, and there are 4.9 million beneficiaries in the participating organizations. Fifty-eight organizations that participated in the first year of the Shared Savings Program reported earning a combined $315 million in shared savings payments.

The 110-page proposed rule aims to clarify the following aspects, among others, of accountable care.

- Requirements for ACO participant agreements, the application and application review process. This provision was added because past Shared Savings applications contained incorrect information which caused them to experience processing delays. CMS recommends

ACOs view its ACO Participant Agreement Guidance to confirm their application will be accepted.

- The identification and reporting of ACO participants. This step specifies that an ACO must include a list of all its ACO participants during the application process and submit an updated list annually.
- Eligibility requirements based on the ACO's number of beneficiaries, structure and governing body. A section of the ACO agreement clarifies participating ACOs must "include primary care ACO professionals that are sufficient for the number of Medicare fee-for-service beneficiaries" and that the amount of beneficiaries must be 5,000 at a minimum.
- The two-sided performance-based risk tracks for ACOs. Track 1 is a shared savings only option, while track 2 applies to ACOs that take on performance-based risk. Upon reviewing these two choices, CMS has proposed the creation of a third track in which providers would accept even more performance-based risk. Track 3 ACOs would have greater incentive to improve their care quality because doing so could maximize their cut of any shared savings.
- ACO public reporting and transparency. This can be accomplished by each ACO maintaining a website that lists the organization's name, identifies ACO participants and discloses data on their shared savings and losses owed to CMS.

The new proposed ruling is a clear indication of how important health IT is to the success of an ACO. As detailed in the document, the rule would require an ACO to outline in its application what technologies would be used to promote more coordinated care for their beneficiaries. Examples of things that could be listed in an application include the use of EHRs to track

patient's data, telehealth services to remotely monitor patients and the electronic exchange of patients' health information.
CMS is working to document the success of ACOs and share insights and accomplishments with the healthcare industry to spur the creation of more accountable care groups. The proposed rule offers a template for participating ACOs to make to make certain information -- such as the identification of ACO participants, governing body members and the amount of any shared savings or shared losses incurred -- available to the public on a website that meets CMS requirements.

The need for an outcome-based payment model and a reduction in healthcare costs are the leading forces behind the creation of ACOs. Some of the first ACOs faced significant challenges during the early adoption stages due to a lack of supporting technologies and health information exchange platforms. Due to the public disclosure of ACO success stories, along with a helpful push from meaningful use criteria, physician-led groups and hospitals have a growing interest in signing up for ACOs.

Next article

# CMS to levy Medicare penalties against physicians

**Shaun Sutner,** News and Features Writer

If the views of Richard Porwancher, M.D., also represent even some of the quarter of a million physicians who face Medicare penalties from CMS in 2015, there are a lot of unhappy providers to whom EHRs feel more like a burden than a medical advancement.

CMS is set to begin levying 1% and 2% Medicare penalties against some 257,000 physicians who did not attest to meaningful use of EHRs in 2013 and 2014.

The reimbursement reductions will hit doctors starting Jan. 1, 2015, and are built into the provisions of the 2009 HITECH Act, which provided up to $30 billion in financial incentives for doctors and hospitals to adopt EHRs.

## Doctors angry at the federal move

But while the penalties -- which can cumulatively total as much as 5% over several years -- were expected, CMS officials' pre-Christmas announcement triggered outrage from the American Medical Association (AMA) and consternation among many doctors who say meaningful use rules are often arbitrary and the penalties unfair. AMA officials said the numbers of doctors to be targeted by penalties were much higher than expected.

Porwancher said his five-doctor infectious disease practice had been unable to attest to meaningful use stage 2 in 2014 after successfully attesting to the less stringent stage 1 in 2013. Porwancher called the meaningful use program "coercive" and unfair, saying his practice has been unable to convince enough of its roughly 2,000 patients to meet the stage 2 measure requiring 10% of a practice's patients to use an electronic portal to communicate with doctors.

"It's neither realistic nor fair to expect 100% compliance with the patient portal. We're begging our patients to help, but we don't have control over our patients," Porwancher said.

Meanwhile, speaking to reporters on a not-for-attribution basis, a CMS official noted in a conference call that about 43,000 doctors who received hardship exceptions will not be subject to reimbursement reductions, but must reapply in 2015 to be exempt from meaningful use in 2016 and avoid future penalties.

## Appeals possible

Also, doctors who receive letters in early 2015 notifying them about penalties have until the end of February to request a review of their situations by CMS, the official said.

The official said that the penalties should not be a surprise and that most physicians ought to be able to attest to meaningful use, receive incentives and avoid penalties.

Steven Stack, president-elect of the AMA, said in a statement that that AMA "is appalled by news from the Centers for Medicare and Medicaid Services ... that more than 50% of eligible professionals will face penalties under the meaningful use program in 2015, a number that is even worse than we anticipated."

In the statement, Stack lumped in the meaningful use sanctions with other cutbacks and potential reductions in Medicare payments to doctors, including those in the Physician Quality Reporting System and the sustainable growth rate reimbursement formula.

"The penalties physicians are facing under the meaningful use program are part of a regulatory tsunami," Stack said.

## Doc says his practice is trying, patients avoid portal

While his practice's EHR includes a portal as required under the meaningful use program, the specific nature of Porwancher's infectious disease practice -- which serves many patients with AIDS and other sexually transmitted diseases, as well as elderly patients -- is such that most patients shy from the portal, he said.

While the portal is secure, Porwancher said patients are still afraid to use it.

In this e-guide

"We take care of patients who are rightfully concerned with confidentiality," he said. "We have people who are afraid about us even sending letters to their home."

Next article

In this e-guide

# Section 4: Health Data Interoperability

The Office of the National Coordinator for Health Information Technology (ONC) is the principal entity responsible for coordinating nationwide efforts to implement and use advanced health information technology and health information exchange. To this end, the ONC is spearheading the effort to move America's healthcare system from paper to electronic health records. This includes programs to encourage EHR adoption, as well as the use of other technologies, by holding competitions and offering prizes.

ONC's mission also includes coordinating health IT policy, providing leadership in the development, recognition and implementation of standards, and the certification of health IT products. In addressing these myriad tasks, the ONC uses the HealthIT.gov site to share healthcare compliance resources and other helpful information.

Continue reading

# Industry shifts focus to health IT interoperability

**Reda Chouffani,** Co-founder – Biz Technology Solutions

The recent rise in EHR adoption and participation in the Medicare and Medicaid EHR Incentive Programs has spurred an increase in the exchange of health information. Several health systems across the nation have supported private and/or state-based HIEs to exchange patient continuity of care records.

Motivated by an underwhelming level of HIE activity, ONC released its Shared Nationwide Interoperability Roadmap in January. The document outlines the ONC's strategy to boost interoperability over the next 10 years, including new regulations and policy updates to secure a greater chance of success. The document is a framework in which true nationwide health IT interoperability can be achieved. It also addresses some of the following predicted barriers the healthcare industry will be faced with on its journey:

**Standardization of electronic health records:** To achieve true interoperability, healthcare entities such as hospitals, HIEs and other care facilities must be able to adopt and use a common data standard, regardless of what EHR or other health IT systems they deploy. As a result of meaningful use criteria, all certified EHR applications could support the Consolidated-Clinical Document Architecture, or C-CDA.

The ONC has indicated that it is looking to encourage wider adoption of a newer standard. CDA Release 2.0 contains far more meaningful health information content and will further enhance the value of the data being transmitted. However, switching to a new standard would be time-consuming because it would force software vendors to upgrade and test all current systems against the new standard.

**Overall costs of integrations and system readiness:** Many organizations see that the expenses of participating in an information exchange go beyond the cost of systems integration. Many EHR products will require the purchase of upgrades to function with a new interoperability standard. Additional systems training and changes to the workflows of the IT department and other employees may also prove costly. The ONC has signaled that it will likely offer future incentive programs to help providers offset the costs of meeting interoperability standards.

**Limited federal and state policies:** Eligible hospitals and professionals that are meaningful users of EHRs have avoided reimbursement reductions from Medicare and Medicaid. In doing so, they have also met some of the baseline requirements for interoperability. However, there are still policy gaps. There needs to be much clearer set of requirements to make a more serious push for nationwide interoperability.

**Lack of trust in public HIE plans:** While it is accepted that long-term HIE adoption hinges on the sharing of meaningful health data, the best way to approach this is unknown. The majority of independent physicians don't have faith in public HIEs, with 94% of them waiting on healthcare payers to play a major role in funding HIE development. That was among the findings of a recent survey on health information exchange done by Black Book Market Research.

## Interoperability would cause more security concerns

As more physicians link to HIEs, it will create another area of vulnerability for patients' health information. Policymakers will have to make note of data breach and cyberattack patterns and adjust regulations to keep HIE participants protected from such threats.

The ONC has put its spotlight on interoperability. The release of the Shared Nationwide Interoperability Roadmap and a new round of HIE funding announced by HHS and the ONC signal that 2015 and beyond will be focused on improving the secure sharing of healthcare information.

➘ Next article

# SMS doesn't translate to secure messaging in healthcare

**Trevor Strome,** Informatics and Process Improvement Lead – Winnipeg Regional Health Authority Emergency Program

An estimate from 2010 put the number of Short Message Service messages sent that year in the range of 6.1 trillion, which contributed $114.6 billion to the global economy. Recently, these numbers have been challenged by competing systems such as Apple's iMessage and BlackBerry Messenger. Despite their popularity, the limitations of SMS and other consumer-grade messaging services make them a bad fit for secure messaging in healthcare.

Although Short Message Service (SMS) can be a quick and effective way to communicate, there are definite drawbacks to the use of SMS and similar messaging services when used for purposes beyond quick greetings. In addition to being limited to 160 characters in a single SMS message, delivery of an SMS message is not guaranteed. Many SMS subscribers have no way to reliably confirm delivery. That leaves users vulnerable to sending messages that contain health information that can be intercepted, read by and forwarded to anyone. Such messages may also remain unencrypted on the servers of telecommunication providers, and persist indefinitely on senders' and receivers' phones. Many of today's physicians are eager to accommodate their patients through electronic communication, but are aware of the privacy considerations that must be addressed first.

According to an article from the American Society of Orthopaedic Surgeons, hospital accreditor The Joint Commission has "effectively banned physicians from using traditional SMS for any communication that contains ePHI [electronic protected health information] data or includes an order for a patient to a hospital or other healthcare setting." According to the article, a single violation involving unsecured communication can result in a fine of $50,000, and "repeated violations can lead to $1.5 million in fines in a single year, not to mention the reputational damage done to an organization and its ability to attract patients." Clearly, alternatives to SMS for medical purposes should be examined.

Apple's iMessage is one of a number of other messaging systems that are growing in popularity. Apple's iMessage works on a similar premise as SMS, but differs in that it "relies on Apple's messaging system to intercept a text message sent to another iOS device and re-routes it through its servers rather than sending it via the wireless carriers as a standard SMS or MMS message" according to an explanation from mobile tech site Re/code. Even iMessage's system has experienced delivery and reliability issues as of late, with iMessage users experiencing message routing glitches after switching to phones with a different operating system.

## Introduction to secure messaging

A safer alternative that can be used in healthcare is secure messaging. The goal of secure messaging in healthcare is to enable patients and their providers to electronically communicate both privately and securely.

Similar to other messaging services, secure messaging utilizes a server-based approach which enables "secure and protected transmission of information between patients and their providers, including clinicians and their support staff," according to an article on the Health and Resources and Services Administration (HRSA) website.

The website provides further details of the secure messaging framework, stating that it is "built around existing communication tools such as the patient portal, secure email and the [personal health record] PHR." The article also clarifies that correspondence can be initiated by the patient or the provider, is sent live, and can consist of structured, unstructured or mixed-format content.

## Securing a messaging service

Because privacy and security are essential when engaging in healthcare-related messaging, providers must take extra precautions to keep the information safe. Secure messages employ bidirectional encryption of point-to-point delivery of messages, are stored on a secured network server, and ensure delivery to a single known receiving entity.

According to Australia's National E-Health Transition Authority (NEHTA), three basic tenets of secure messaging are that it:

- Prevents unauthorized interception of the message content;
- Provides verification that the message has not been altered since it was sent; and

- Provides system notification of successful delivery.

According to an AAOS report, to assist in the development of compliant messaging systems, The Joint Commission has established Administrative Simplification Provisions that outline four major areas that are critical to compliance:

- Secure data centers -- Patient information is usually stored in data centers that are on-site or cloud-based, and HIPAA requires that the data centers have high-level physical security and policies for regularly conducting risk assessments and reviewing controls.
- Encryption -- Electronic personal health information must be encrypted in transit (bidirectionally) and while in storage.
- Recipient authentication -- All communications of electronic personal health information must reach (and only reach) its intended recipient, and should inform the sender when a message has been delivered *and* received.
- Audit controls -- Any compliant messaging system must also have the ability to create and record an audit trail of all activity that contains ePHI [electronic protected health information]. For a text messaging system, this includes the ability to archive messages and information about them, to retrieve that information quickly, and to monitor the system.

## Secure messaging in healthcare

Secure messaging is experiencing increased use in healthcare. Possible healthcare applications range from making (and confirming) medical appointments and asking medical questions to discussing treatment options and sending medical device readings (such as blood pressure) to a care provider. Secure messaging applications expedite processes that formally were handled over the phone and avoid the compliance issues presented by default SMS programs.

A benefit of secure messaging, according to HIMSS, is that it "allows patients and healthcare teams to communicate non-urgent, health related information in a private and safe computer environment." Several specific examples cited by HIMSS regarding how secure messaging can be used include within the healthcare setting include:

- Patient-clinician communication management;
- Healthcare team management;
- Message management; and
- Patient services/clinical operations management.

It is important to recognize that secure messaging is not simply an email application, but a fully encrypted, secure system of communication. This enables secure messaging to be used in conjunction with other electronic or mobile health services.
According to NEHTA, some of the documented benefits of secure message delivery include:

- It allows for the secure, encrypted exchange of sensitive clinical information and documents (including eReferrals and discharge summaries) and prevents the unauthorized interception of the private content contained within the message.
- It reduces the use of paper-based correspondence resulting in less time wasted searching for clinical information and investigations, resending or chasing referrals, and performing other miscellaneous activities (such as scanning, printing, filing and posting).
- Confidential patient correspondence is seen only by the treating clinicians (no scanning of documentation is necessary).
- Notification of the successful delivery of messages, allowing the sending party to know that a message has been successfully received (and decrypted) by the proper receiving party.
- It has the potential to improve the quality of clinical care through improved timeliness of the providers' receipt of clinical information.

As society becomes increasingly digitized, consumers expect the convenience of digital communications to extend to healthcare. Given the popularity and convenience of consumer-grade messaging services on mobile devices, there are obvious opportunities to transform both provider-to-provider and patient-provider communications in healthcare. Healthcare organizations need to be observant of regulatory requirements and technical considerations in order to protect individuals' electronic health information, to ensure the efficient electronic provider-provider and patient-provider communications do not succumb to faulty practices and overwhelming security concerns.

# Digital signature technology can bolster health care data security

**Don Fluckinger,** News Director

The movement to build a health IT infrastructure whose goal is to improve patient care is opening up new opportunities for the use of digital signatures. This technology can improve health care data security and can be wired into an electronic workflow, as well as into systems for physician order entry and e-prescribing; and patient admission, discharge and transfer.

Hospital accreditors, such as the Joint Commission and the American Osteopathic Association, recognize e-signatures as equivalent to signatures on paper. Considering the reports (those for safety and quality practices alone use copious amounts of paper) that come with accreditation -- not to mention the policies, training documents and disaster planning materials -- digital signatures can reduce significantly the amount of paper hospitals have to store when they integrate the technology into accreditation standards compliance programs.

E-signatures solve more than just the problems of storing paper. "We know that our electronic health records [EHR] systems provide the ability for us to sign entries electronically," said Jan Hecht, an assistant professor at Eastern Kentucky University in Richmond, Ky., who teaches courses in the field of health services administration. "We're hoping that by using electronic signatures, we can really tackle some of the issues with legibility and the timeliness of authentication."

Hecht and Kerry Costa, a management consultant for Dell Inc.'s Healthcare Services, spoke in a May 11 webinar on behalf of the American Health Information Management Association, and offered tips for evaluating and implementing digital signature technology in a health care setting.

## How different levels of e-signatures affect health care data security

There are three levels of e-signatures, Hecht explained:

- Level 1 is literally a digitized signature. This electronic representation of a person's handwritten signature provides the lowest level of security and is similar to the credit card signatures that many retail stores collect via signature pads.
- Level 2 is a biometric scan, PIN or token. These "signatures" provide midlevel security.
- Level 3 is a digital certificate that provides a tamperproof seal that breaks when a message is altered.

It's important that, before it implements digital signature technology, the company understand how e-signatures work in each of its facility's systems -- most importantly, the EHR and e-prescribing systems. Companies need to develop policies and procedures around these systems to address health care data security, as well as regulatory compliance, Hecht said.

That might not be as simple as it seems, however. Health care environments include physician assistants and nurse practitioners, who deliver prescriptions to patients as proxies for the physician; and emergency rooms and intensive care units often involve numerous staff members in a patient's care, especially during high-pressure situations. As a result,  Dell's Costa said, facilities probably will have to develop e-signature policies for these scenarios:

- Multiple and dual signatures, and countersignatures.
- Entries made on behalf of others.
- Signatures by proxy.
- Batch signings.

Finally, e-signature systems will have to accommodate physician scribes, who act for physicians who just can't get the hang of a new EHR system but still have to use it anyway, Costa said.

Writing these policies before implementing digital signature technology can help sort out the other complicated situations that can show up in a patient health record. Consider the care a patient receives while a doctor is on sabbatical or leave -- one scenario where planning digital signature policies helps accommodate health care-specific needs. A physician typically signs the record and attests that it is true, but when a substitute physician administers care, the system needs to let the regular physician sign on behalf of the substitute within the patient record, Costa noted.

Along those same lines, it pays to avoid auto-attestation, the process by which a physician attests all his entries upon sign-in, Costa said. Both the Uniform Electronic Transactions Act (UETA), which is law in 47 U.S. states, and Medicare Conditions of Participation, which controls reimbursement, require a signer to take a specific action to attest and verify each entry. For good reason, too: Auto-attestation gives a physician the opportunity to approve orders that did not get transcribed properly, do not display or were not reviewed previously.

## Regulations for digital signature technology in health care

Health IT leaders should note that the proposed Drug Enforcement Administration's latest e-prescribing proposed regulation mandates Level 2 authentication in the form of a biometric or retinal scan. That brings up an additional step that should be taken before any purchasing decision is made: Check state regulations regarding e-prescribing, as well as digital signatures in general, Hecht said. The states of Illinois, New York and Washington, which have not signed on to UETA, vary in what they require.

If a facility mandates compliance with the ISO 14888, ASTM EI 762-94 and Certification Commission for Healthcare Information Technology digital signature standards, doctors should check into them, Costa said. In addition, any facility reviewing its own enterprise protocols for digital signatures or embarking on a new implementation might want to read those standards, too, for guidance and best practices information.

Lastly, before doctors sign on the dotted line for the purchase of new digital signature technology, they should check with payers and with Medicare's signature guidelines, to make sure those organizations accept e-signatures on claims generated by the system, Costa said.

↘ Next article

In this e-guide

## About SearchHealthIT

SearchHealthIT provides free unbiased news, analysis, resources and strategies for healthcare IT professionals that manage healthcare operations for hospitals, medical centers, health systems, and other organizations.

We know that patient care at your organization is your number one concern. That's why we are dedicated to providing you with the tools, guides and techniques to improve efficiencies, cut costs, and meet regulatory requirements.

## For further reading, visit us at http://SearchHealthIT.com/

Images; Fotalia