

WHITE PAPER

Health Care Solutions Group



LORICCA
RELIABLE TECHNOLOGY SOLUTIONS

HITECH Act, Electronic Health Records and Meaningful Use



Loricca is a **Service-Disabled Veteran Owned Small Business.**

HITECH Act, Electronic Health Records and Meaningful Use

The Health Information Technology for Economic and Clinical Health (HITECH) Act added a number of funding opportunities to advance the secure use of health information technology. Health information technology (HIT) makes it possible for health care providers to better manage patient care through the secure use and secure sharing of health information. HIT includes the use of electronic health records (EHRs) instead of paper medical records to maintain an individual's health information.

HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to various aspects of health care information technology, such as the creation of a more robust and integrated health care infrastructure on a national basis. It also contains specific incentives designed to accelerate the adoption of EHR systems among healthcare providers.

Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), HITECH broadens the reach and scope of privacy and security protections mandated by HIPAA and also increases the potential legal liability for non-compliance. There is also specific wording that provides for more enforcement.

What is of interest to many healthcare providers is that the Medicare and Medicaid EHR incentive programs will provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals as they adopt, implement, upgrade or demonstrate the '*meaningful use*' of certified EHR technology.

Some of the key dates to keep in mind going forward include:

- *April 2011 – Attestation for the Medicare EHR Incentive Program begins.*
- *May 2011 – EHR Incentive Payments expected to begin.*
- *July 3, 2011 – Last day for eligible hospitals to begin their 90-day reporting period to demonstrate meaningful use for the Medicare EHR Incentive Program.*
- *September 30, 2011 – Last day of the federal fiscal year. Reporting year ends for eligible hospitals and critical access hospitals.*
- *October 1, 2011 – Last day for eligible professionals to begin their 90-day reporting period for calendar year 2011 for the Medicare EHR Incentive Program.*
- *November 30, 2011 – Last day for eligible hospitals and critical access hospitals to register and attest to receive an incentive payment for Federal fiscal year 2011.*
- *December 31, 2011 – Reporting year ends for eligible professionals.*
- *February 29, 2012 – Last day for eligible professionals to register and attest to receive an incentive payment for calendar year 2011.*

Meaningful Use Security Risk Analysis

One of the goals in the 2009 federal economic stimulus package was to provide billions of dollars in funding to help offset part of the cost for hospitals and physicians to adopt comprehensive electronic health records. Subsequently, federal regulators issued a proposed rule to define how hospitals and physicians must demonstrate their "meaningful use" of EHRs so they can qualify for the Medicare and Medicaid incentive payments.

The rule addresses data security by saying that the "meaningful use" requirements are designed to ensure that organizations implementing EHRs use the data protection functions within the software as well as *"processes and possibly tools outside the scope of the certified EHR technology."*

Some data security experts acknowledge that this requirement is far from crystal-clear, but they interpret it to mean that organizations that want to receive incentive payments should evaluate their use of the security functions within their EHR software as part of their broader risk assessments and vulnerability analysis. The rule implies that organizations implementing EHRs should do a risk assessment of that technology against their broader privacy security risk assessments that they should have already been doing under HIPAA.

The rule states that to qualify for Stage 1 of the incentive payments, healthcare providers must ***"conduct or review a security risk analysis of certified EHR technology and implement updates as necessary."***

The security rule under HIPAA required healthcare organizations to conduct periodic risk assessments, especially when implementing new software systems, hardware and processes. When an organization implements new technology it is crucial that the organization looks at how it fits into the broader risk assessment of the entire enterprise. Some implementations have caused 'holes' in the network, rogue access points, and threats/vulnerabilities that were not there before.

An organization should conduct a security risk analysis of their implemented EHR or contract with a third party to complete a thorough security risk analysis that provides a Findings & Recommendations document as a key deliverable. The results of the assessment can then be reviewed and decisions can be made based upon the recommendations received to determine what changes or additions might be needed to update various security controls to address any risks that were uncovered during the assessment. The identified risks should be prioritized by severity level and a meaningful remediation plan should be developed and documented so that updates can be made showing what was remediated; by whom; and when.

The general flavor and message of HITECH is that implementing new technology alone is not enough, because if an organization only focuses on the technical controls, they will not have a very secure environment. For that reason, it is imperative that organizations roll out a comprehensive data security program that's built, in part, on a thorough risk assessment of their EHR software and all other application systems and IT components.

Healthcare provider organizations also will need to carefully review whether they are using all of an EHR's built-in security capabilities, such as data encryption, access control, frequent changing of 'strong' passwords, etc. To earn incentives, hospitals and physicians must implement certified software. The software certification standards require that the software include encryption capability, access controls and other provisions.

Enforcement Issues

Many healthcare covered entities have been questioning for years whether there are really any HIPAA police out there that they should be aware of. It has been widely speculated within the healthcare industry that HIPAA has not been as actively enforced in the past as what was expected and anticipated. With the coming of the HITECH Act and especially with the wording that 'beefs up' security and penalties, there is a general increased awareness among healthcare entities that has caused them to give more attention to the specific compliance requirements and related remediation within their own organizations and service footprint.

Under HITECH, mandatory penalties will be imposed for *"willful neglect."* Willful neglect, and what that means to each entity will be determined on a case-by-case basis. However, as the Office of Civil Rights (OCR) has been saying for years, *"If it isn't documented, it didn't occur."* So, documentation of previous and current compliance activities and initiatives must be kept up to date, showing what has taken place thus far and what is 'in process' or planned, as the enterprise proactively moves toward compliance. Those who do not have a well-documented compliance program are likely to be at significant risk.

Civil penalties for willful neglect are increased under the HITECH Act. These penalties can extend up to \$250,000, with repeat (or uncorrected) violations extending up to \$1.5 million. Additionally, HIPAA's civil and criminal penalties may now be enforceable against business associates of healthcare covered entities. Like HIPAA, HITECH does not allow an individual to take direct action against a provider, although it does allow a state attorney general to bring an action on behalf of their residents. One key point to keep in mind is that HHS is now required to conduct periodic audits of covered entities and business associates.

The message is becoming clear. The legislative authorities are intent on providing for more noticeable enforcement of these regulations.

Notification of Breach

The HITECH Act now imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." These notification requirements are very similar to many data breach laws within the states related to personally identifiable financial information, such as banking and credit card data. HITECH considers unencrypted PHI data to be unsecured PHI, so data encryption is another key topic of interest at this time.

In general, HITECH requires that patients be notified of any unsecured breach. If a breach impacts at least five hundred patients, then HHS must also be notified. If notified, HHS will post and display the breaching entity's name on its website. Under certain conditions local media will also need to be notified of breaches. Another thing to keep in mind is that the notification requirement is triggered whether the unsecured breach occurred externally or internally. This is another example of how the HITECH Act is putting more emphasis on the privacy and security of PHI.

Electronic Health Record Access

In the case where a provider has implemented an EHR system, HITECH provides individuals with a right to obtain their PHI in an electronic format. An individual can also designate that a third party be the recipient of the ePHI. All that should need to be done on a healthcare provider's part is to click on a few screens and transmit the requested records, if they already have an EHR system in place and/or have the capability to meet this request. With everything going digital, it should be expected that electronic health records will be requested much more often than hardcopy records.

Any provider expecting to receive incentives as part of the HITECH Act provisions should be prepared to successfully handle and deliver on these requests, or sadly, they may find out later that the way they manage and use patient data in the form of electronic health records does not qualify as meaningful use. Lack of meaningful use may end up blocking incentive payments.

Business Associates

The HITECH Act has now applied certain HIPAA provisions directly to business associates. In the past, privacy and security requirements were imposed on business associates via their own contractual agreements with covered entities. From what we have seen, many small providers do not have the requisite contracts in place; and, in some cases contracts exist but they do not meet all of the requirements of the rules.

Business associates are now directly required to comply with the safeguards contained within the HIPAA Security Rule. Most software vendors providing EHR systems will clearly qualify as business associates. Requiring vendors to comply directly ensures that more provider/vendor dialog will occur regarding the necessary contracts, and regarding other compliance issues of mutual interest.

Additionally, business associates are required to report security breaches to covered entities consistent with the notification requirements of HITECH. They are now subject to civil and criminal penalties under HIPAA if certain conditions exist. There are additional business associate requirements that may be imposed depending on how the relationship with the provider is defined. The bottom line is that business associates and providers will share more joint responsibilities than they have previously.

The HITECH points discussed here are only a small subset of the content and provisions that may be relevant to healthcare providers. The HITECH Act now makes HIPAA more directly relevant to providers, especially when you consider the financial ramifications.

Under HITECH there are significant taxpayer dollars appropriated in the form of incentive funding that directly target a provider's adoption and implementation of an EHR system. Federal and state regulators, patients and other stakeholders can be expected to demand more transparency and accountability. If a healthcare provider wants to receive the benefit of incentives, or at a minimum wants to avoid any subsequent penalties, then they appear to have little choice, other than to increase their awareness and adherence to the HIPAA Privacy and Security provisions that have been highlighted with HITECH. Small providers may benefit enormously if they can find creative ways to pool resources to respond to these challenges.

Whereas the HIPAA Privacy Rule deals with PHI in general, the HIPAA Security Rule deals with electronic protected health information (ePHI), which essentially causes somewhat of an overlap with the Privacy Rule. In terms of actual regulatory text the HIPAA Security Rule only spans approximately 8 pages, which is the good news. The bad news is the HIPAA Security Rule is highly technical in nature. For all intents and purposes this rule is the codification of certain information technology standards and industry 'best practices'.

Basically, the HIPAA Security Rule requires implementation of three types of safeguards:

- 1. administrative**
- 2. physical**
- 3. technical.**

Basically, the HIPAA Security Rule requires implementation of three types of safeguards: 1) administrative, 2) physical, and 3) technical. Appropriate action will need to be taken if healthcare providers want to "reasonably and appropriately" comply with the HIPAA Security Rule. A given standard usually has implementation specifications associated with it. The advice we regularly give to clients with respect to this rule is to make sure that they implement the necessary safeguards to avoid unnecessary risk to the organization. We understand and agree that this is much easier said than done, since there may not be a good understanding within the customer management ranks of what is really necessary. The

HIPAA Security Rule has provided some flexibility here as an apparent acknowledgement of the challenges faced by healthcare providers, but unfortunately does not really reduce the burden of compliance implementation.

Being a Meaningful User of Electronic Health Records

It is widely believed and accepted that electronic health records play a critical role in getting to a higher quality, safer, more effective health care system. The release of the final rules on 'meaningful use' along with the applicable standards and required certifications has laid the groundwork for EHR in the US. Health care providers now have additional funding to support the meaningful use of electronic health records as well as guidelines that can help them implement them in a way that improves the overall care for their patients.

Benefits of Electronic Health Records

Many more are recognizing that electronic health records (EHR) and health information exchange (HIE) can help to provide higher quality and safer care for patients. By adopting electronic health records in a 'meaningful' way, healthcare providers can:

- **Know more about their patients.** Information in electronic health records can be used to coordinate and improve the quality of patient care.
- **Make better decisions.** With more comprehensive information readily and securely available, providers will have the information they need about specific treatments and specific conditions when making patient treatment decisions.
- **Save money.** Electronic health records require an initial investment of time and money, those who have implemented them have reported reductions in the amount of time spent locating paper files, transcribing and spending time on the phone with labs or pharmacies, along with more accurate coding and reduced time spent in reporting.

Medicare and Medicaid EHR Incentive Programs

Through the Medicare and Medicaid EHR incentive programs, the Centers for Medicare & Medicaid Services (CMS) is providing incentive payments to eligible health care professionals and hospitals who adopt certified EHR technology and achieve meaningful use.

Note that EHR incentives registration started on January 3, 2011.

CMS and the Office of the National Coordinator for Health Information Technology (ONC) announced the availability of registration for the Medicare and Medicaid EHR incentive programs as of January 3, 2011. CMS and ONC encouraged broad participation and outlined online and in-person resources that are in place to assist eligible professionals and eligible hospitals who wish to participate.

Registration in the Medicaid EHR Incentive Program is now available in Alaska, Iowa, Kentucky, Louisiana, Oklahoma, Michigan, Mississippi, North Carolina, South Carolina, Tennessee, and Texas. In February, registration will open in California, Missouri, and North Dakota. Other states likely will launch their Medicaid EHR Incentive Programs during the spring and summer of 2011.

CMS Administrator Donald Berwick, MD has stated that CMS has many resources available to help providers register and participate, and they look forward to working with eligible professionals and eligible hospitals to facilitate the process, now and going forward.

David Blumenthal, MD, MPP, National Coordinator for Health Information Technology, stated that it's time to get connected. ONC and CMS have worked together over many months to prepare for the startup that began in early January. ONC has a certified product list that includes more than 130 certified EHR systems or modules and is updated frequently. ONC also has hands-on assistance available across the country through 62 separate Regional Extension Centers.

Eligible professionals and eligible hospitals must register in order to participate in the Medicare and Medicaid EHR incentive programs. To prepare for registration, interested providers should first familiarize themselves with the incentive programs' requirements, incentive payments, eligibility, meaningful use and certified EHR technology.

Under the EHR incentive programs, eligible professionals can receive as much as \$44,000 over a five-year period through Medicare. For Medicaid, eligible professionals can receive as much as \$63,750 over six years. Under both Medicare and Medicaid, eligible hospitals may receive millions of dollars for implementing and meaningfully using certified EHR technology.

The changeover from paper to electronic records will be challenging for many, but CMS and ONC have taken steps to ease the transition. They have provided flexibility in meeting the meaningful use requirements, both agencies have conducted extensive outreach, and they have the resources in place to help providers meet the programs' requirements. Immediate registration is not required, but they do encourage eligible providers to sign up as soon as they have certified EHR technology and are prepared to participate.

The Security Rule has largely been ignored by small providers since most do not currently have EHR systems in place. As we discussed earlier, HHS is attempting to build a national health infrastructure and is therefore pushing for the adoption of electronic health records. It is Loricca's belief that privacy and security issues are important public policy concerns for all vertical markets, not just healthcare. Compliance with HIPAA and HITECH is certainly a goal that all healthcare providers should work diligently to meet.

However, we also believe that the majority of providers need help in reaching this goal. For this reason Loricca has developed effective and cost-conscious compliance solutions that are framed by a well-thought-out and proven process methodology.

SUMMARY: Meaningful Use – Policy Goals and Definition

Through the Medicare and Medicaid EHR incentive programs, CMS hopes to expand the meaningful use of certified EHR technology. Certified EHR technology used in a meaningful way is one piece of a broader HIT infrastructure needed to reform the health care system and improve health care quality, efficiency, and patient safety. ONC issued a final rule establishing a temporary certification program for health IT on June 24, 2010 and anticipates issuing a final rule establishing a permanent certification program later this year.

CMS' goal is for the definition of meaningful use to be consistent with applicable provisions of Medicare and Medicaid law while continually advancing the contributions certified EHR technology can make to improving

health care quality, efficiency, and patient safety. To accomplish this, CMS' final rule would phase in more robust criteria for demonstrating meaningful use in three primary stages.

Development of Stage 1 Criteria for Meaningful Use

The meaningful use criteria is the culmination of an intensive process that involved input from several Federal Advisory Committees (the National Center for Vital Health Statistics, the HIT Policy Committee, and the HIT Standards Committee) and a notice of proposed rulemaking (NPRM) published on January 13, 2010. Over 2,000 comments were received on the proposed rule for the Medicare and Medicaid EHR incentive programs. Review of these comments caused several changes to be made to the NPRM Stage 1 criteria of meaningful use. Most notably, the option for deferral of some objectives and/or measures and the evaluation of the applicability of some objectives and/or measures to EPs and eligible hospitals will now be allowed. Many other specific changes were made to the objectives and measures individually and interested stakeholders should review the final rule for these changes.

Stage 1 Criteria for Meaningful Use

The Stage 1 criteria for meaningful use focus on electronically capturing health information in a coded format, using that information to track key clinical conditions, communicating that information for care coordination purposes, and initiating the reporting of clinical quality measures and public health information. The criteria for meaningful use are based on a series of specific objectives, each of which is tied to a measure that allows EPs and hospitals to demonstrate that they are 'meaningful users' of certified EHR technology.

For Stage 1, which begins in 2011, there will be 25 objectives/measures for EPs and 24 objectives/measures for eligible hospitals. The objectives/measures have been divided into a core set and menu set. EPs and eligible hospitals must meet all objectives/measures in the core set (15 for EPs and 14 for eligible hospitals). They can choose to defer up to five remaining objectives/measures. Each objective/measure was evaluated for its potential applicability to all EPs and eligible hospitals. Where it is impossible for an EP or eligible hospital to meet a specific measure, exclusion is defined in the final rule. If an exclusion applies to an EP or eligible hospital, then such professional or hospital does not have to meet that objective/measure in order to be determined a meaningful EHR user. For example, if an EP has two exceptions (one for a core objective/measure and one for a menu objective/measure), the EP would need to meet the remaining 14 objectives/measures in the core set and four of the remaining nine objectives/measures in the menu set.

In 2011, EPs, eligible hospitals and critical access hospitals seeking to demonstrate meaningful use are required to submit aggregate clinical quality measure numerator, denominator, and exclusion data to CMS or the States by attestation. In 2012, EPs, eligible hospitals and critical access hospitals seeking to demonstrate meaningful use must electronically submit clinical quality measures selected by CMS directly to CMS (or the States) through

certified EHR technology. CMS recognizes that for clinical quality reporting to become routine, the administrative burden of reporting must be reduced. By using certified EHR technology to report information on clinical quality measures electronically to a health information network, a State, CMS, or a registry, the burden on providers that are gathering the data and transmitting them will be greatly reduced.

The burden of generating the necessary information for the provider to then use the information to improve health care quality, efficiency, and patient safety will also be reduced. CMS expects that by their second implementation year, States will have the capacity to accept direct submission of Medicaid providers' clinical quality measures from certified EHR technology.

Beyond the Stage 1 Criteria for Meaningful Use

The policy goals of meaningful use will be most fully realized by building on findings from Stage 1 and by making full use of the greater proliferation of certified EHR technology and supporting HIT/E infrastructure that will take place under Stage 1. CMS intends to propose through future rulemaking two additional stages of the criteria for meaningful use.

Stage 2 would expand upon the Stage 1 criteria in the areas of disease management, clinical decision support, medication management support for patient access to their health information, transitions in care, quality measurement and research, and bi-directional communication with public health agencies. These changes will be reflected by a larger number of core objective requirements for Stage 2. CMS may also consider applying the criteria more broadly to the outpatient hospital settings (and not just the emergency department). CMS believes that information exchange is a critical part of care coordination and it is expected that the infrastructure will support greater requirements for using health information exchanges for Stage 2.

Stage 3 would focus on achieving improvements in quality, safety and efficiency, focusing on decision support for national high priority conditions, patient access to self management tools, access to comprehensive patient data, and improving population health outcomes.

The Meaningful Use Objectives specification sheets for the Medicare and Medicaid EHR Incentive Programs bring together critical information on each objective to help eligible professionals, eligible hospitals and eligible critical access hospitals to understand what they need to do to demonstrate meaningful use successfully. For eligible professionals, there are a total of 25 meaningful use objectives.

To qualify for an incentive payment, 20 of these 25 objectives must be met, including:

- **15 required core objectives**
- **5 menu set objectives that may be chosen from a list of 10**

For eligible hospitals and critical access hospitals, there are a total of 24 meaningful use objectives. To qualify for an incentive payment, 19 of these 24 objectives must be met, including:

- *14 required core objectives*
- *5 menu set objectives that may be chosen from a list of 10*
- *Each specification sheet covers a single eligible professional core or menu set objective in detail, including information on:*
 - *Meeting the measure for each objective*
 - *How to calculate the numerator and denominator for each objective*
 - *How to qualify for an exclusion to an objective*
 - *In-depth definitions of terms that clarify objective requirements*
 - *Requirements for attesting to each measure*

Conclusion

Loricca has developed internally and in collaboration with key strategic alliance partners, other services and solutions related to the EHR Incentive Programs, to provide technical assistance and best practices in EHR adoption and demonstration of meaningful use.

Michael Whitcomb, PMP, CISM

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.

Loricca, Inc. | www.loricca.com | 813.600.3005 | mwhitcomb@loricca.com