Privacy and Security Implications of Meaningful Use for Health Care Providers

Prepared by:

Phyllis A. Patrick, MBA, FACHE, CHC
Wayne S. Martin, MS, CISA, CISM, CISSP

and the

NCHICA Meaningful Use Work Group

October 2010

Privacy and Security Implications of Meaningful Use for Health Care Providers

The Health Information Technology for Economic and Clinical Care Act (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA), authorizes incentive payments through Medicare and Medicaid to hospitals and clinicians who meet "Meaningful Use" criteria by using certified electronic health records (EHRs) to achieve improvements in health care delivery. EHRs must provide for data transmission and exchange in a private and secure manner. Organizations are to meet criteria for Meaningful Use by the beginning of the government's Fiscal Year 2011 (October 1, 2010).

The purpose of this white paper and supporting documentation is to provide the health care provider community with guidance regarding the implications of implementing the Meaningful Use criteria while meeting privacy and security requirements. It is hoped that this information will assist senior leaders, privacy and security leaders, and others in making informed decisions as they adopt and exploit the use of certified EHRs in meeting their strategic goals.

The white paper will explore the issues associated with the Meaningful Use criteria as they relate to health care provider organizations. Academic Medical Centers (AMCs) have expanded spheres of influence in the context of the AMC missions related to patient care, research, and education. Included is a review of critical privacy and security issues that must be considered as provider organizations and AMCs seek to achieve Meaningful Use as set forth in the CMS criteria. The white paper includes a discussion of the implications for Meaningful Use in meeting the criteria, and provides recommendations for senior leaders and other interested parties.

Appendix A includes a matrix, detailing the Privacy and Security Implications of Meaningful Use Readiness across a spectrum of capabilities and maturities, along with a listing of the roles and responsibilities of key stakeholders and participants in the process.

The AMC Privacy and Security Conference Workshop

"Meaningful Privacy and Security" was the theme of the Sixth Academic Medical Center Security & Privacy (AMCSP) Conference, coordinated by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) on June 7-9, 2010. The Conference brought together representatives of AMCs from throughout the United States. A pre-conference workshop on "Privacy and Security Implications of Meaningful Use" included deliberations and discussions of representatives from these AMCs and other organizations interested and involved in the development of electronic health records (EHRs) and the Meaningful Use criteria. A listing of workshop participants is included in **Appendix B** to this paper.

Discussion at the AMC workshop focused on developing recommendations related to achieving Meaningful Use across the following dimensions for distribution to senior managers at all health care provider organizations:

- Governance approaches to meeting privacy and security requirements in the context of implementing EHRs and achieving Meaningful Use
- Developing, implementing, and monitoring privacy and security policies and procedures resulting from Meaningful Use initiatives
- Defining privacy and security responsibility and accountability for AMC management, business, and technology leaders.

The workshop participants considered Meaningful Use in the context of three processes and priorities for provider organizations:

- Governance/Risk Assessment/Compliance processes
- Strategic information system planning process
- Privacy and Security Programs (HIPAA Privacy and Security Rules as the "foundation" for Meaningful Use).

Background and Overview of the Meaningful Use Rule

The Centers for Medicare and Medicaid (CMS), through the Department of Health and Human Services (HHS), released the Final Rule for Meaningful Use in July, 2010. Concurrently, HHS, through the Office of the National Coordinator for Health Information Technology (ONC), released the Final Rule establishing an initial set of standards, implementation specifications, and certification requirements for EHR technology for vendor products.

In the Rule, CMS defines Meaningful Use for the first two years (2011 and 2012) of a phased, long-term plan under HITECH. As of this writing, HHS has not released the expected publication dates for further Meaningful Use rules.

The broad goals established by CMS for Meaningful Use include the following:

- Improve quality, safety, and efficiency of health care and reduce health disparities
- Engage patients and families
- Improve care coordination
- Improve population and public health, and
- Ensure adequate privacy and security protections for personal health information.

Achieving Meaningful Use is based on health care providers establishing the capability to improve the health of the American population by supporting patient care processes and outcome measurements, leading to improvements in quality of care, patient safety, and reductions in overall cost to the health care system.

Given the incentive funding and priorities of ARRA/HITECH, there is a renewed movement toward widespread adoption of EHRs. Along with this trend and the Meaningful Use criteria, there is also a requirement and growing need to ensure adequate privacy and security protections for personal health information. AMCs and other health care providers must:

- Provide and monitor privacy and security protection of confidential protected health information through operating policies, procedures, and technologies
- Comply with all applicable federal and state laws and regulations and
- Provide transparency of data sharing to patients.

Health information technology (HIT) and electronic health record (EHR) systems are viewed as essential mechanisms for improving patient care and achieving quality and efficient health care. In announcing the incentive payment program, CMS indicated that Certified EHR technology used in a meaningful way is one component of a broader HIT infrastructure required to reform the health care system and improve health care quality, efficiency, and patient safety.

The government has mandated that, in order for hospitals and eligible providers to qualify for the maximum funding, they must begin to demonstrate Meaningful Use as early as 2010 and no later than 2015. Providers participating in Medicare programs will receive lower fees, adjusted downward beginning in 2015, if they do not meet the Meaningful Use requirements.[1]

Achieving Meaningful Use: The Three Stages

Congress established a broad framework for Meaningful Use:

- The use of certified EHR technology in a meaningful manner
- Certified EHR technology connected in a manner that provides for the electronic exchange of health information to improve the quality of care and
- Use of certified EHR technology to submit information on clinical quality measures.

"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. HHS believes this ultimate vision of reforming the health care system and improving health care quality, efficiency and patient safety should drive the definition of meaningful use consistent with the applicable provisions of Medicare and Medicaid law… Ultimately, consistent with other provisions of law, meaningful use of certified EHR technology should result in health care that is patient centered, evidence-based, prevention-oriented, efficient, and equitable."[2]

In defining Meaningful Use through the creation of criteria, CMS balanced competing considerations to propose a definition that best supports reform of health care and

improved health care quality. The definition recognizes the short time frame available under HITECH for providers to begin using certified EHR technology.
CMS notes that, given the ongoing advancement in EHR technology and standards, as well as changes in quality measurement and other health care-related reporting, the Meaningful Use definition should mature over time. Accordingly, CMS proposed three stages of criteria to be met by eligible professionals and providers over the initial years of the program, 2010 through 2015.

Stage 1 Meaningful Use criteria focus on the following functionalities and activities:

- Electronically capturing information in a structured format
- Using that information to track key clinical conditions
- Communicating that information for care coordination
- Implementing clinical decision support tools to facilitate disease and medication management
- Using EHRs to engage patients and families, and
- Reporting clinical quality measures and public health information.

Stage 2 expands upon Stage 1 criteria by encouraging the use of HIT for continuous quality improvement at the point of care and the exchange of information in "the most structured format possible." Examples include computerized provider order entry (CPOE), electronic transmission of diagnostic test results (lab, radiology, imaging, nuclear medicine, and others). As CMS notes in the Rule, Stage 2 Meaningful Use requirements will include "rigorous expectations for health information exchange, including more demanding requirements for e-prescribing and incorporating structured laboratory results and the expectation that providers will electronically transmit patient care summaries to support transitions in care across unaffiliated providers, settings, and EHR systems."

Stage 3 goals focus on the following:

- Promoting improvements in quality, safety and efficiency leading to improved health outcomes
- Focusing on decision support for national high priority conditions
- Patient access to self management tools, and
- Access to comprehensive patient data through robust, patient-centered information exchange and improving population health.

"Increasingly robust expectations for health information exchange in stage two and stage three will support and make real the goal that information follows the patient."

According to CMS, having these functionalities in certified EHR technology at the beginning of the program and requiring eligible hospitals and providers to become familiar with them will create a strong foundation on which to build in later stages.

The Meaningful Use objectives, as defined in the Final Rule, include a set of core objectives that constitute an essential starting point for Meaningful Use of EHRs and a separate list of additional important activities from which providers can select several to implement in the first two years.

Core objectives include basic patient data, including functions that support improved health care (patient demographics, vital signs, active medications, allergies, problem lists of current and active diagnoses, and smoking status). Other core objectives include using software applications that incorporate the potential of EHRs to improve quality, safety, and efficiency of care (clinical decision support tools, CPOE, etc.). In addition to the core elements, the Rule includes a menu of ten additional tasks from which providers can choose five to implement in 2011 – 2012. The menu includes capabilities to perform drug formulary checks, incorporate laboratory results into EHRs, provide reminders to patients for needed care, identify and provide patient-specific health education resources, and employ EHRs to support the patient's transitions between care settings and care givers.

Achieving Stage 1 Meaningful Use also means demonstrating progress in health outcome priorities. Reporting on blood pressure measures, smoking status, and adult weight screening will be required in 2011 and 2012.

As part of the process, HHS is establishing a nationwide network of Regional Extension Centers (RECs) to assist providers in adopting qualified EHRs and achieving meaningful use of them.

Implications for Health Care Providers

Health care providers must demonstrate Meaningful Use of HIT through reporting on clinical quality metrics, and several administrative measures related to EHR functionality.

The stages of Meaningful Use have implications for the following business and clinical processes of the AMC:

- Governance Model
- Security program components/regulatory requirements (HIPAA Privacy and Security, Breach Notification Laws, HITECH, Red Flags Rule, State laws)
- Risk Assessment and Mitigation Processes
- Security Program Evaluation
- Risk Assessment and Risk Management
- Privacy and Security Awareness and Training
- Incident Reporting and Response
- Accounting of Disclosures

Significant time and resource commitments will be required to demonstrate Meaningful Use measures. Providers will need to upgrade existing clinical systems to certified

EHRs. Providers will need to make business process and workflow changes to ensure that all data necessary for reporting are being captured accurately and completely. Organizations may need to invest in process re-design and improving efficiencies in work flow.

Key Themes from the Workshop Discussions

A number of key themes related to successful implementation of EHRs and Meaningful Use at AMCs emerged from the workshop discussions. The key themes include the following:

- Achieving Privacy and Security Compliance in Meaningful Use Criteria
- The Role of the Privacy and Security Officers in Development of EHR and Meaningful Use Strategy, Processes, and Implementation
- Data Exchange and Coordinated Care in the Context of Privacy and Security
- The Role of the Health Care Provider in Health Information Exchanges
- Engaging and Enabling the Patient in EHRs and Meaningful Use

Each of these key themes is discussed below, followed by recommendations for consideration by senior leaders at health care provider organizations including AMCs.

Achieving Privacy and Security Compliance in Meaningful Use Criteria

The Meaningful Use rules, while referencing privacy and security as a goal, do not include specific requirements or criteria regarding what is expected in achieving Meaningful Use, other than to note that by 2011 an eligible provider should "conduct or review a security risk analysis and implement security updates as necessary," per 45 CRF 164.308(a)(i). This refers to the HIPAA Security Rule requirement to conduct regular risk analyses, one of the administrative safeguards and implementation specifications included in the Security Rule. The intent may be broadly interpreted that eligible professionals and eligible hospitals should assess their privacy and security practices in general and make improvements where necessary and appropriate.

While having privacy and security programs in place that meet the requirements of the HIPAA Privacy and Security Rules may be assumed under the Meaningful Use criteria, it is not clear that most health care providers have fully implemented robust programs that can meet the existing rules, in addition to new requirements imposed by HITECH (e.g., breach notification, accounting of disclosures, etc.). Other than the Rules and increasing enforcement activities, there is minimal experience from which providers can draw to determine where their privacy and security programs may fall on the compliance spectrum. The results of the CMS efforts to audit security programs in 2008 were not widely circulated; thus, lessons learned in that endeavor may have been overlooked. The audit/review process has been transferred to the Office of Civil Rights (OCR); however, OCR is not expected to begin audits of existing programs until 2011.

Most of the literature regarding Meaningful Use and guidance to providers in achieving Meaningful Use has been focused on the following:

- Financial incentive programs
- Implementing clinical systems
- Developing strategies for achieving EHR certification, and
- General tactical advice in moving the EHR along a spectrum of health information exchange and interoperability.

Little has been documented about the privacy and security program requirements already in place. What happens if an eligible provider or eligible hospital appears to meet the Meaningful Use criteria, including EHR certification, and suffers a major security breach or privacy incident? Providers are also required to follow a myriad of state laws regarding use of social security numbers, protection of personal information, breach notification and remediation, and others.

Privacy and security compliance relative to HIPAA is required for all stages of Meaningful Use. Eligible providers and eligible hospitals should be aware of the implications for not meeting the regulations and should be conducting regular reviews of their capabilities in this area. The effective dates for compliance, according to the HIPAA Privacy and Security Rules, were April, 2003 for Privacy and April, 2005 for Security.

Establishing effective privacy and security programs requires a leadership view that the programs are integral to the organization's overall strategic plan. Effective privacy and security goes beyond responding to regulations or designating privacy and security officers to coordinate the programs. The lowest common threshold is compliance with the laws and regulations. Consequences of failing to ensure that management is meeting its responsibilities regarding privacy and security include: reputational damage; contractual noncompliance (contracts increasingly contain stipulations for the protection of information); inaccurate or incomplete data (e.g., research studies and multi-organization clinical trials, etc.); and competitive advantage (compromise of key corporate information).

Privacy and security are central to the AMC missions related to patient care, research, and education. Privacy and security should receive the same attention from senior leaders and the Board as other strategic resources and programs, e.g., quality and safety.

Senior leaders and Boards of provider organizations are concerned with risk and improving risk management, but they may not fully understand the privacy and security risks associated with existing laws, requirements, and mandates. Management and Boards need to exercise governance over the privacy and security of their information resources.

The IT Compliance Institute, a U.S.-based authority on the role of technology in regulatory compliance, defines an effective security governance program as having the following attributes:

- Involves appropriate organizational personnel
- Defines a governance framework or methodology
- Enables uniform risk measurement across the organization
- Produces quantifiable, meaningful deliverables
- Reflects business practices, organizational risk appetites, and changing levels of risk.

Effective privacy and security requires both governance and management actions. The board and management need privacy and security program officers to help mitigate risk to the organization and report on confidentiality, integrity, and availability risks to the organization's goals.

Privacy and Security Governance consists of leadership, organizational structures and processes that support the privacy and security practices while supporting and sustaining the organization's mission and strategies.

There are a number of best practices with respect to governance of privacy and security programs. Common themes associated with good governance include: promoting good and effective privacy and security practices with clear direction and understanding at all levels of the organization; controlling risks associated with the mission and work of the organization; and creating a risk management process for privacy and security that reflects the organization's needs and risk appetite level.

An example of good governance is represented by the **Information Privacy and Security Executive Committee at Vanderbilt University Medical Center**. The purpose of the Committee is "to foster an environment in which work processes, policies and structures, and professional practices demonstrate the balance of patient care, teaching, and research needs with the constraints necessary to safeguard business and health information integrity, confidentiality, and availability."

The Committee is chaired by the Chief Strategy and Information Officer, who also serves as Associate Vice Chancellor for Health Affairs, and is made up of senior executives from across the enterprise. The Committee assumes various roles, including promoting a "culture where professional integrity and respect for patient privacy permeate all operational work processes, patient care encounters, academic experiences, and research efforts." The Committee also works to "assure deliberate planned progress towards the Privacy and Information Security Strategic Visioning Statement for the EMR." (For further details, visit www.vanderbilthealth.com.)

Recommendations for Health Care Providers: Achieving Privacy and Security Compliance in Meaningful Use Criteria

1. Review existing governance of privacy and security programs.

2. Implement effective security governance processes.

3. Include privacy and security as primary components of the organization's strategic planning process.

4. Enhance internal controls for compliance with privacy and security requirements (HIPAA and other federal and state regulations).

5. Conduct regular evaluations and audits of compliance with HIPAA and new requirements included in HITECH (e.g., breach notification, accounting of disclosures, sale of PHI for marketing and fundraising). Understand the gaps and prioritize improvement efforts.

6. Develop an ongoing and documented process for evaluating the privacy and security programs. This is not a one-time process, but rather a regular recurring assessment to consider changes in the environment and regulatory requirements.

7. Include privacy and security risk assessment in the enterprise-wide risk assessment and management (EWRA) processes.

8. Develop new and enhanced training programs in privacy and security for management, board, staff, and all those considered to be part of the organization's workforce (e.g., medical students, residents, fellows, volunteers, contractors, etc.).

The Role of Privacy and Security Officers in the Development of EHR and Meaningful Use Strategy, Processes, and Implementation

The views and experiences of Privacy and Security Officers are often overlooked in designing EHRs and developing information technology strategic plans. Often the contributions that these individuals bring to the strategic planning, risk management and other high-level organizational processes may not be well understood.

The roles were generally created in the last few years, in response to the requirements in the HIPAA Privacy and Security Rules that there be a designated Privacy Officer and a designated Security Officer for the covered entity. Sometimes responsibilities were combined with existing roles, e.g., HIM Director, Chief Information Officer, IT Director, etc.

There are different approaches to IT security reporting. Thus, there is a preponderance of titles for individuals with responsibility for privacy and security (e.g., IT Security Director, Chief Security Officer, Chief Information Security Officer, Chief Privacy Officer, Chief HIPAA Officer, Chief Risk Officer, etc.). The positions are sometimes viewed as necessary to meet compliance with regulations and to respond to possible instances of wrong-doing or threats. As such, the roles may be more reactionary and less strategic.

Privacy and Security Officers need clearly defined roles and responsibilities. They should be viewed as key participants in the provider's governance processes, with regular, ongoing reporting of privacy and security program progress and issues to senior leaders and the Board.

The roles and responsibilities of Privacy and Security Officers should be clearly delineated and serve as a check/balance to protect the organization against possible privacy and security issues that can increase risk and jeopardize the AMC missions related to patient care, research, and education.

Privacy and security responsibilities should result in collaborative working relationships, but the functions should also be separate to assure that compliance requirements, privacy controls, and technical security controls are handled independently, providing for segregation of duties and in concert with preventing single points of failure in threat situations.

The roles of Privacy and Security Officers need to become more strategic and focused on meeting privacy and security challenges in the era of health care reform, including working with AMCs to meet the Meaningful Use criteria and representing the interests of AMCs in the development of Health Information Exchanges (HIEs).

Health care providers generally have a Board level Audit Committee, on which the full Board relies to manage risk areas, including IT and Security risk, and provide oversight of internal and external auditing. Generally, audit responsibilities are not separated from risk responsibilities; thus, there is not adequate segregation of duties with the same committee essentially overseeing the development of security programs and the controls and effectiveness of these programs. The focus may be more on the responsibilities of IT for security and not cover all aspects of privacy and security risks and regulatory requirements at both federal and state levels. Risk assessment processes for privacy and security may not be integrated into the enterprise-wide risk assessment process.

Recommendations for Health Care Providers: The Role of Privacy and Security Officers

1. Providers should re-evaluate the roles and responsibilities of their Privacy and Security Officers and elevate the positions to key senior leaders, with enhanced responsibilities for strategic planning. The Officers should actively participate in

2. Privacy and Security Officers should regularly report on the status of the programs to senior leaders and to the Board, including Board committees responsible for compliance, risk, and audit oversight.

3. Providers should establish formal, mandatory annual training in privacy and security risks for senior leaders and Board members.

4. Providers should consider establishing a Board-level Risk Committee charged with enterprise-wide risk management (EWRM), including privacy and security risks. This Committee should be separate from the Board Audit Committee.

5. Providers should conduct annual evaluations of the privacy and security programs and ongoing privacy and security compliance assessments.

Data Exchange and Coordinated Care in the Context of Privacy and Security

Establishing criteria and models for the exchange of data will be integral to meeting ARRA and HITECH goals, as outlined by the government. Data Exchange and Coordinated Care, as exemplified in the Medical Home and Accountable Care Organization concepts, may help to further the goals of HITECH and enhance the goal of information exchange between health care professionals, thereby improving quality, safety, and efficiency; improving care coordination; and reducing health disparities.

Improving the safety and efficiency of health care delivery in a community starts with having access to comprehensive patient health records and current clinical information. Partners in the health care community, including clinicians, hospitals, community resources, and payers face unique challenges in producing accurate and timely health records. Care is coordinated through the use of IT, registries, and HIE.

Effective privacy and security, including assuring the confidentiality, integrity, and availability of data is the foundation for efficient, timely, and accurate data exchange. It will be necessary to re-engineer workflows across organizations, replacing point-to-point connections/interfaces with robust HIE processes.

Data exchange will provide the foundation for care coordination across all elements of the health care system and the patient's community. Meeting clinician and patient expectations and achieving clinician and patient buy-in will be critical to achieving Meaningful Use in this context. Additionally, secondary uses of data, including the purchase of protected health information for research, marketing, and other purposes will need to incorporate privacy and security safeguards from the outset of these arrangements.

The Medical Home and Accountable Care Organization (ACO) represent models for alternative delivery systems included in recent health care reform legislative proposals. Both models focus on quality and management of care, but they also face implementation challenges, including how to achieve close, timely communication involving possibly a large array of providers and support systems, including EHRs. The expense and coordination issues involved in implementing effective, efficient, common EHRs may be exacerbated if they cannot meet the intended goal of producing significant reductions in health care spending.

Recommendations: Data Exchange and Coordinated Care in the Context of Privacy and Security

1. Health care providers should develop policies or revise existing policies for responding to requests for secondary uses of data, consistent with new requirements of ARRA and HITECH.

2. AMCs should work with health care providers in their regions and states to assess the Medical Home and ACO models for possible inclusion in their strategic goals related to EHR development and attainment of Meaningful Use.

The Role of the Health Care Provider in Health Information Exchanges

The Health Information Exchange (HIE), as defined by the Healthcare Information and Management Systems Society (HIMSS), represents the activity of secure health data exchange between two authorized and consenting trading partners (a data supplier and a data receiver). Third parties may be involved in HIEs as facilitators operating between the data supplier and the data receiver. The third party's role may also include storing data from and on behalf of the data supplier, transmitting data on behalf of the data supplier, and/or receiving data on behalf of a data receiver. HIE activity can enhance virtually any clinical function by providing clinicians and others with a broader set of data upon which to base clinical decisions.

The Meaningful Use Notice Final Rule includes the acknowledgement of the benefits ofHIEs; thus, it is clear that HIE represents a national strategy.

"Health information exchanges have the potential to transform the health care system by facilitating timely, accurate, and portable health information on each patient at the point of service…. use of health information exchange models can reduce the need for costly point-to-point interfaces between different EHR tools, as used in laboratories and pharmacies, thus providing a more scalable model of interoperable health information exchange. HIEs promote adoption of certified EHR technology by providing the infrastructure for provider EHRs to reach outside of their clinical practice sites and connect with other points of care… Without health information exchange, electronic health records are simply digitized filing cabinets and will not achieve their quality of care or cost containment potential… The inclusion in HITECH of HIE grants to be awarded to States or State-designated entities by ONC are an additional indication of the symbiotic relationship between health information exchanges and optimal use of EHRs." (75 Fed. Reg. at 1932, 1033, 1034).

The goal of an HIE is to ensure that health information is available when and where it is needed at hospitals, in local communities, in physicians' offices, across the state/region, in neighboring states and throughout the nation.

HIEs, in various forms, including community and state-level HIEs, are growing and maturing across the United States. HIEs are not currently available in all demographic areas and it is not likely that there will be adequate expansion over the next few years. At this time, CMS has not addressed HIE dependency for most of the Meaningful Use objectives.

The development and evolution of HIEs pose significant opportunities for AMCs to achieve organizational objectives related to HIT, EHRs, and Meaningful Use. By working with other providers, communities, and data exchanges to discuss cross-organizational issues and put agreements in place, the AMC can also achieve goals related to research, patient care, and education. Privacy and Security Officers at AMCs can facilitate the AMC/HIE/community partnerships, and make sure that the exchange of data incorporates key principles and requirements for Privacy and Security programs.

While a number of HIEs exist in various regions of the country, not all are closely associated with AMCs and organizational models vary. The more successful HIEs have been developed out of mutual needs and cooperation by stakeholders. Maintaining a state/regional perspective, based on the unique needs of the community and the unique resources of AMCs and other regional providers, may be the best approach to successful implementation across the country. This approach may provide for more effective, efficient, and patient-centered exchanges without the imposition of a nation-wide HIE.

HealthBridge is demonstrating that an HIE can deliver improved quality and efficiency. Founded in 1997, HealthBridge is one of the nation's largest, most comprehensive and successful HIEs. The organization provides secure, electronic exchange for Southwestern Ohio, parts of Southern Indiana, and Northern Kentucky. HealthBridge includes hundreds of different hospitals and health systems, laboratories, diagnostic and imaging facilities, physician offices and clinics, community health centers, local health departments and nursing homes.

Services include physician access to hospital information systems, results reporting, order entry system, e-prescribing, quality and registry reporting capabilities, and support services for other health information exchanges.

HealthBridge's electronic network and communications infrastructure reduces health care costs by an estimated $20 million per year in the Greater Cincinnati tri-state area.

As a leader in health information exchange, HealthBridge assists other communities and states with their HIE efforts. (For further information, visit www.healthbridge.org.)

Recommendations for Health Care Providers: The Role of the Health Care Provider in HIEs

1. AMCs should take a leadership role in developing, implementing, and maintaining HIEs in their states/regions that meet community needs, while also enhancing the AMC goals related to research and education.

2. Senior leaders of AMCs, Privacy and Security Officers, and other personnel should take an active role in HIE strategic planning and implementation activities.

3. HIE workshops should be formed to develop strategies, specific requirements, capacity, and implementation plans for meeting HIE requirements under HITECH.

Engaging and Enabling the Patient in EHR/Meaningful Use

The Meaningful Use criteria include the provision for engaging patients and families in their health care. Many providers have set up communication portals to provide patients with information regarding their health care and to assist with registration and scheduling appointments, follow-up care, and online billing for services provided. Hospitals are generally lagging in their ability to implement portals that provide access to EHRs for patients, or providing the functionality to import records from commercial services (e.g., Google and Microsoft HealthVault).

In most areas, patients have not been given much information about their electronic health records. Health literacy levels vary, with some patients requiring substantial assistance with becoming involved and conversant with their health issues and concerns. Some patients take an active role in managing their health information. Others may require assistance, not only with the technology associated with accessing their electronic records, but with engaging in two-way communication with clinicians and other care-givers.

Patients don't have enough information about electronic patient records in general. Also, when HIEs are involved, it may be difficult for the patient to opt-out of record sharing, if they so desire.

Achieving patient "trust" is key to working with patients and families/delegates directly in achieving patient and family engagement in the care process. Clinicians, who may not recognize their role in the information sharing/discussion that needs to occur between patient and caregiver should understand and relate to the patient's needs for information. Patient expectations also need to be defined and managed.

As health care providers continue to develop their EHRs and move toward achieving Meaningful Use, clinicians and other caregivers will need to actively partner with patients. Trust among all parties involved is critical to the success of meeting

expectations of patients and clinicians. Achieving this may require new or diverted resources to actively manage processes for both patients and clinicians.

Providers will need to focus on patient and family/delegate requirements in this area. It is clear that establishing effective and efficient EHRs and HIEs extends beyond establishing patient portals, i.e., the portal is one method of communication, but it will not meet all requirements and needs.

A suggestion from the workshop participants is that providers may want to consider a patient advocate or liaison role, a designated resource to work directly with patients and clinicians in order to bridge the gaps that exist and provide the patient with the ability to engage and participate fully in his/her health care, including decision making. The traditional role assumes that patient advocates navigate the health care system; then inform, counsel, and help their patients and their families understand the results. Patient advocates complete paperwork, such as insurance claims. Advocates must keep abreast of current medical laws, rules and policies such as Medicare requirements, etc. Having the patient advocate become involved in the patient's EHR navigation process may be a natural adjunct to the existing concept of patient advocate. This should be explored more fully.

Giving Duke Medicine patients a "window on their health information", **HealthView** is a web site created by **Duke University Health System.** The site allows patients to view lab results and appointment and account information. The portal was initially launched in 2007 and now has more than 28,000 users. The portal has become a central hub for communications with patients and caregivers.

With HealthView, patients can schedule or request an appointment online any time; see lab results when they are available; pay bills online; update personal and insurance information; and complete advance registration forms.

Future features planned by Duke include providing physicians with access to clinical information, med lists, and e-prescribing functions, book operating suites and consult with other Duke specialists.

(For further details, visit www.healthview.dukehealth.org.)

Recommendations: Engaging and Enabling the Patient in EHR/Meaningful Use

1. Providers should develop methods to more actively engage patients in their care.

2. AMCs should revise training programs for health care practitioners, residents, fellows, and other personnel to include the role of the patient/family in managing their care using EHRs, and enabling the patient to be an active participant in decision making.

3. Providers should continue the development of patient portals in the context of their overall strategic planning for EHR and HIE adoption across the continuum of care.

4. Providers should re-assess the role of the patient advocate and, where appropriate, incorporate aspects of EHR adoption, PHR services, Meaningful Use criteria, and HIE growth in the job performance expectations.

APPENDIX A

The matrix includes the Privacy and Security Implications of Meaningful Use Readiness across a spectrum of capabilities and maturities, along with a listing of the roles and responsibilities of key stakeholders and participants in the process. The authors used criteria from the Malcolm Baldrige National Quality Program to portray the various stages of development and maturity of EHR technology and Meaningful Use across an organization.

Quality outcome and process measures are familiar concepts to senior leaders and Board members of AMCs and health care providers. The use of process measures enables the organization to assess specific components of a process to determine the degree of adherence to regulatory standards or best practices.

The matrix provides a model for:

- Assessing an organization's capability/maturity related to achieving EHR implementation and Meaningful Use
- Determining the various roles and responsibilities of key players (senior leaders, business leaders, technology leaders, privacy leaders, security leaders, and compliance leaders), and
- Evaluating the measures of success across the three stages of Meaningful Use, as currently defined by CMS.

Definitions for the process measures include:

"Systematic Approach": methods are appropriate to the requirements of regulations and organizational goals, and are practiced in a systematic way across the organization.

"Learning" indicates that new knowledge or skills have been acquired within the organization through evaluation, analysis, experience, and innovation.

"Alignment" indicates that there is consistency of plans, processes, resource decisions, actions, results, and analyses across the organization and that the approach to privacy and security supports key organization-wide goals.

"Integration" refers to the harmonization of plans, processes, information, resource decisions, actions, results, and analyses to support organization-wide goals. Effective integration goes beyond Alignment and is achieved when the individual components achieve interoperability.

MEASURING MEANINGFUL USE READINESS and ORGANIZATION APPROACHES

CAPABILITY / MATURITY	1	2	3	4
	SYSTEMATIC APPROACH	**LEARNING**	**ALIGNMENT**	**INTEGRATION**
Meaningful Use Requirements and Expectations	HIPAA-compliant privacy and security policies developed and implemented. Information Technology risk assessment performed on regular basis; process and results documented	HIPAA security program evaluation performed on regular basis. Risk Assessment findings used to drive program improvements and changes. Privacy and security implications of meaningful use identified.	Security Risk Assessment processes and findings integrated within enterprise risk management program. Non-technical HIPAA security program evaluation incorporated within audit and technical assessment cycles.	Privacy and security programs clearly communicated and understood by all levels of the organization. Ongoing, continuous review, assessment, awareness, monitoring, and education programs for Privacy and Security.
Awareness and Understanding	Basic awareness and understanding of privacy and security compliance requirements within organization.	Formal and routine communication and awareness training regarding privacy and security programs.	Comprehensive awareness training on requirements, expectations, management, and monitoring of privacy and security programs.	Comprehensive and consistent monitoring and compliance with privacy and security programs. Effective change management processes throughout organization to ensure privacy and security compliance. Effective Issue identification and resolution process.
Perceptions of Employees, Staff, Partners, Business Associates, etc	Privacy and security programs are separate from business operations.	Privacy and security programs are integral components of business operations and processes.	Privacy and security programs are included in organizational strategic planning and implementation of new initiatives.	Privacy and security programs are integrated within continuous improvement processes built in.
Documentation	Limited, sporadic, and Inconsistent	Formalized and consistent	Comprehensive and consistent	Comprehensive, consistent, and current
Management and Monitoring	Ad hoc, unlinked, intuitive	Formal, standardized, and/or no monitoring	Formal, standardized, periodic monitoring initiated.	Formal, standardized, real-time monitoring.

ROLE / RESPONSIBILITY	SYSTEMATIC APPROACH	LEARNING	ALIGNMENT	INTEGRATION
Senior Leaders	Establish effective privacy and security programs as central elements of the organization's strategic plan. Review existing governance of privacy and security programs. Implement effective security governance processes.	Senior management and Board provide active oversight of information resources and privacy and security protections. Privacy and security risk assessment included in the enterprise-wide risk assessment and management (EWRA) processes.	Roles/responsibilities of Privacy and Security Officers re-evaluated. Officer positions are elevated to key senior management executives, with enhanced responsibilities for strategic planning. Officers actively participate in AMC strategic planning, risk assessment and management processes, EHR development and MU processes.	Board level Risk Committee charged with enterprise–wide risk management (EWRM), including privacy and security risks. (This Committee should be separate from the Board Audit Committee.) Privacy & Security Officers assume leadership roles in developing, implementing, and maintaining HIEs in their states/regions that meet community needs, while also enhancing the AMC goals related to research and education.
Business Leaders	Ensure privacy and security protection for confidential information through operating policies and procedures.	Enhance internal process controls for compliance with HIPAA and HITECH privacy and security requirements.	Conduct regular evaluations of the privacy and security programs, annual risk assessments, and ongoing privacy and security compliance audits within all business operations and processes.	Develop methods to more actively engage patients in their care. Develop policies or refine existing policies for responding to requests for secondary uses of data, consistent with new requirements. Work with clinicians, hospitals, and other providers in their regions/states to assess the Medical Home and ACO models for possible inclusion in strategic goals. Form HIE Work Groups to develop strategies, specific requirements, capacity, and implementation plans for meeting health information exchange requirements.

ROLE / RESPONSIBILITY	SYSTEMATIC APPROACH	LEARNING	ALIGNMENT	INTEGRATION
Technology Leaders	Ensure privacy and security protection for confidential information through leveraging technology.	Enhance internal technical controls for compliance with HIPAA and HITECH privacy and security requirements.	Conduct regular evaluations of the privacy and security programs, annual risk assessments, and ongoing privacy and security compliance audits within all business operations and processes.	Develop methods to more actively engage patients in their care. Develop policies or refine existing policies for responding to requests for secondary uses of data, consistent with new requirements. Work with clinicians, hospitals, and other providers in their regions/states to assess Medical Home and ACO models for possible inclusion in strategic goals. Form Work Groups to develop strategies, specific requirements, capacity, and implementation plans for meeting HIE requirements.
Privacy Leaders	Provide transparency of data sharing to patients. Develop new and enhanced training programs in privacy and security for management, Board, and all members of the workforce. Include training requirements for all contractors.	Mitigate and report on information confidentiality, integrity, availability, and other risks to organizational goals and objectives.	Conduct regular evaluations of the privacy and security programs, annual risk assessments, and ongoing privacy and security compliance audits within all business operations and processes.	Privacy and Security Officers should regularly report on the status of programs to senior management and to the Board, including Board committees charged with compliance, risk, and audit oversight.
Security Leaders	Ensure privacy and security protection for confidential information through standards-based policies and procedures. Develop new and enhanced training programs in security for management, board, and all staff. Include training requirements for all contractors.	Mitigate and report on information confidentiality, integrity, availability, and other risks to organizational goals and objectives.	Conduct regular evaluations of the privacy and security programs, annual risk assessments, and ongoing privacy and security compliance audits within all business operations and processes.	Privacy and Security Officers should regularly report on the status of programs to senior management and to the Board, including Board committees charged with compliance, risk, and audit oversight.
Compliance Leaders	Ensure compliance with applicable laws and regulations. Work with Privacy and Security Officers to develop an ongoing and documented process for evaluating the AMC's privacy and security programs.	Conduct or lead regular evaluations of both technical and non-technical compliance with HIPAA and HITECH.	Establish mandatory annual training in privacy and security risks for senior management and Board members.	AMCs should establish mandatory annual training in privacy and security risks for senior management and Board members.

MEASURES OF SUCCESS	SYSTEMATIC APPROACH	LEARNING	ALIGNMENT	INTEGRATION
MU Stage 1	Full Compliance with HIPAA Privacy and Security Rules	Conduct a security risk assessment and implement security updates as necessary.		
MU Stage 2	Full Compliance with HIPAA Privacy and Security Rules	Conduct a security risk assessment and implement security updates as necessary.	Provide summarized or de-indentified data when reporting data for health purposes (e.g., public health quality reporting, and research), where appropriate, so that important information is available with minimal privacy risk.	
MU Stage 3	Full Compliance with HIPAA Privacy and Security Rules	Conduct a security risk assessment and implement security updates as necessary.	Provide summarized or de-indentified data when reporting data for health purposes (e.g., public health quality reporting, and research), where appropriate, so that important information is available with minimal privacy risk.	Provide patients, on request, with a timely accounting of disclosures for treatment, payment, and health care operations, in compliance with applicable law. Incorporate and utilize technology to segment sensitive data.

APPENDIX B - ACKNOWLEDGEMENTS

This white paper is the result of a workshop on “Privacy and Security Implications of Meaningful Use” held on June 6, 2010. The workshop participants are commended for sharing their knowledge and information and assisting in summarizing the key themes and adaptive practices contained herein. Their enthusiasm in preparing this paper and their active participation made this endeavor possible.

The writers would like to acknowledge the contributions of the following workshop participants:

Martha B. Adams, MA, MD
Duke University

Claudia G. Allen, Esq.
Greater Cincinnati HealthBridge, Inc.

Holt Anderson
NCHICA

Camilla Hull Brown
Strategies for Tomorrow, Inc.

Cheryl L. Brown, Ph.D.
University of North Carolina at Charlotte

Angel Hoffman, RN, MSN
AP Health Care Compliance Group, LLC

David Kirby
Kirby Information Management Consulting

M. Gaye Smith
Vanderbilt University Medical Center

Aaron Van Artsen. B.A., MLRHR
University Physicians, Inc., University of Colorado

Wayne Wilson
Erlanger Health System

We would also like to thank members of the NCHICA Privacy and Security Officials Workgroup and the NCHICA Board of Directors for their review and comments.

Co-authors:

Phyllis A. Patrick, MBA, FACHE, CHC
AP Health Care Compliance Group, LLC

Wayne S. Martin, MS, CISA, CISM, CISSP
Blue Ridge Community College

FOOTNOTES

[1] Section 1848 (a)(7) of the HITECH Act provides that beginning in Calendar Year 2015, eligible professionals who do not demonstrate that they are meaningful users of certified EHR technology will receive an adjustment to their fee schedule for their professional services of 99 percent for 2015, 98 percent for 2016, and 97 percent for 2017 and subsequent years.

[2] Sections 1848(a)(2)(A) and 1886 (n)(3)(A) of the HITECH Act includes Congress' identification of the broad goal of expanding the use of EHRs through the term meaningful use.