HIMSS Electronic Health Record Association

230 E. Ohio Street
Suite 500
Chicago, IL 60611

Phone: 734-477-0852
Fax: 734-973-6996
E-mail: himssEHRA@himss.org

Privacy Position Statement

The Electronic Health Record (EHR) Association supports public policy initiatives which protect the confidentiality, security and integrity of protected health information (PHI) while promoting the access to PHI and other data necessary to ensure safe, timely, appropriate, quality healthcare and protect public health and safety.

The EHR Association respectfully requests that the consideration of new laws or policies concerning the privacy and security of PHI in treatment, payment and healthcare operations (TPO) should be developed in collaboration with all affected parties, based on research and data provided by experts in the field, utilizing standards developed by recognized standards organizations. Such a collaborative approach would promote effective health care delivery, research, and public health and safety while building confidence in the structure of our privacy and security structures.

Background: Concerns over the privacy and security of electronic health information primarily fall into three general categories:

1. Preventing the inappropriate use of information within a provider organization, resulting in the unauthorized dissemination of information in violation of law and organizational policy.

2. Preventing non-authorized users from gaining access to an organization's information system with malicious intent.

3. Providing security for the exchange of information through healthcare systems that relate to patient care activities while prohibiting use of individually identifiable health information beyond that necessary for TPO without the authorization of the individual.

Some “privacy advocates” have been advocating for laws, regulations and policies that mandate further restrictions on the use and exchange of information beyond those already provided by federal law. The EHR Association asserts that, in most cases, current law is sufficient and further restrictions could adversely impact the provision of high-quality health care to individuals and the functioning of the health care system without the expected improvements in privacy. In place today is extensive state

and federal laws governing PHI. Careful consideration needs to be given to ensure any changes to current laws or the addition of laws would achieve the intended benefits and would not impose unfunded and unnecessary administrative and technical requirements that will impede the day-to-day processes of our information-centric healthcare system, thereby negatively impacting quality of and access to care and rendering disease management, quality assurance and reporting, licensing, credentialing, training, audits for fraud and abuse, unworkable.

The EHR Association proposes a better way.

The EHR Association policy position on leading privacy issues are as follows:

Access to PHI and Accounting for Disclosures:
The EHR Association fully supports the use of audit trails and user authentication tools to limit access to PHI on a need-to-know basis and to track access to PHI. Such tools are already in wide use among healthcare organizations. The EHR Association supports the sharing of selected and pertinent audit trail information generated during TPO with patients and providing individuals with their health records.

Background: In the HIPAA Privacy Rule, patients are given the right to see and obtain copies of their medical records and request amendments to the record if they identify errors and mistakes. Under HIPAA, health plans, doctors, hospitals, clinics, nursing homes and other Covered Entities (CEs) must provide access to health records within 30 days. CEs can charge patients for the cost of copying and sending their records. There is proposed legislation attempting to ensure that CEs that maintain health information through an EMR provide for an individual's PHI to be readily available and that such Entities maintain PHI for a period of time.

Second, under current law, TPO (Treatment, Payment and Healthcare Operations) are exempt from HIPAA requirements for Covered Entities to produce an accounting of disclosures of PHI upon request extending back six years from the date of request. Proposed legislation would remove this exemption for non-oral TPO disclosures and establish the right for an individual to obtain an "accounting of disclosures" of PHI made by a Covered Entity for TPO over a certain period of time (proposed legislative time periods range from three or six years prior to the request). In addition to addressing the maintenance of PHI through an EMR, legislation would require that CEs make available electronic copies of PHI in electronic format without charge.

Finally, proposed legislation would revise the definition of "marketing" that has been established under HIPAA. For example, legislative provisions would limit the conditions under which marketing is considered a healthcare operation and precludes fundraising and direct payment to CEs for the use of PHI to make certain communications without valid authorization.

EHR Association Position: The EHR Association supports a requirement that Covered Entities provide patients, upon request, with selected and pertinent data elements from existing HIPAA-required audit trails, which would provide information on the external entities and individuals within the covered entity to which PHI is disclosed for TPO activities. In addition, if the Congress determines that accounting for disclosures for TPO is necessary, we urge that the legislative provisions for TPO accounting reflect the special characteristics of such data that resulted in the original HIPAA exemptions, limiting what is considered a disclosure (for

example, exempting non-employee medical staff) and the level of detail needed for the disclosures (for example, the persons role or indicating whether the reason for the disclosure was treatment, payment, or operations).

In regards to legislation attempting to clarify the definition of marketing under HIPAA, the EHR Association believes that measures should be implemented to restrict certain communications, such as "pure" marketing, without prior authorization. At the same time, the Association believes that legislative provisions should not impede such essential activities as disease management programs and clinical and prescription refill reminders.

The EHR Association is very concerned that the unintended consequences of changes in disclosure rules could prevent interoperability and data sharing, thus preventing care providers from accessing critically needed information at the point of care. Another unintended consequence could be serious workflow obstacles for patient care providers.

The EHR Association warns that accounting for all disclosures of PHI contained in a health IT product would be a very cumbersome and costly task with substantial implications for clinical and administrative workflows, product functionality and data storage. While PHI is often made available to clinicians and other authorized users through such tools as EMRs and EHRs, it is often stored across multiple departments and information systems, many of which have their own direct access. Also, definitions of disclosure are not always clear-cut. Would disclosure be considered to occur when an automated process produces a back-up tape or when a billing clerk communicates about a bill with a payer? In addition, it is important to recognize that the proposed changes in HIPAA provisions for accounting for TPO disclosures go well beyond audit trails and require a description of the reason for the disclosure.

For example, the data needed for disclosure under proposed HIPAA TPO provisions includes a brief description of the PHI disclosed and a brief statement of the purpose of the disclosure. While seemingly benign, this data can be very burdensome to collect for routine patient care that occurs within a single institution, Caregiver productivity could be severely impacted. This information is not now generally included in audit trail functionality but must be derived based on the individual, system, time of day and other events happening at the same time. It would require new data collection tools and user interfaces. In addition, some interpretations of the provision suggest that it would become required to account for disclosures to physicians and other healthcare providers who are not actual employees of the Covered Entity, such as voluntary members of the hospital medical staff.

Fundamentally, such a requirement would be a major impediment to clinical workflow, would require substantial revision to a huge number of health IT systems, would require data storage for far longer than is now the case, and would impose new requirements for electronic and other data flows between hundreds or even thousands of PHI-containing systems in large healthcare institutions. Concerns have also been raised around employee privacy if the accounting of disclosures would expose that an employee has been given a specific task.

Business Associates and Covered Entities:
The EHR Association believes that, with regard to penalties for Business Associates for the inappropriate use and disclosure of PHI, the current HIPAA provisions are sound with the addition of some further clarification by the Secretary of HHS on how to appropriately account for violations. The Association believes that federal government penalties should not be inflicted on Business Associates but rather that the Covered Entities should remain responsible for ensuring that their Business Associates fully comply with their contracted privacy and security obligations. Finally, the EHR Association believes that providers of personal health records (PHR) solutions, that are primarily offered by those providers to "patients", and who are not always operating as Business Associates of Covered Entities, should be brought within the HIPAA privacy and security framework. Many providers of PHR solutions to "healthcare providers" are already Business Associates of Covered Entities and therefore covered by the current HIPAA privacy and security framework.

Background: According to HIPAA, CEs include healthcare providers, health plans (including employer-sponsored plans), and healthcare clearinghouses (e.g. billing agents). HIPAA only allows for PHI to be freely communicated and transferred for TPO among CEs. According to HIPAA, a Business Associate is an individual or corporate "person" that performs on behalf of a Covered Entity any function or activity involving the use or disclosure of PHI and is not a member of the Covered Entity's workforce. A Covered Entity may disclose PHI to a Business Associate and may allow for a Business Associate to create or receive PHI on its behalf only if the Covered Entity executes a contract or other binding written agreement that details permitted activities. Under such contracts and agreements, Business Associates are required by the Covered Entities to adhere to HIPAA standards and to use appropriate safeguards to prevent the unauthorized use or disclosure of PHI and report all unauthorized uses and/or disclosures of PHI. Although CEs are not held liable for privacy violations of Business Associates, CEs must report problems to the Department of Health and Human Services (HHS) and terminate contracts and agreements when appropriate. HIPAA allows for problems to be cured, and also realizes that terminating some contracts is not always practical and could lead to additional problems.

Proposed legislation aimed to extend the regulatory requirements and penalties applicable to CEs under HIPAA to Business Associates. Current legislation also required such organizations as HIEs, RHIOs, electronic prescribing gateways and providers of PHRs who have entered into contracts with CEs to also have Business Associate agreements. Therefore, these organizations would also be held to the same standards as CEs.

EHR Association Position: Fundamentally, the Covered Entity has sole control over the data and dictates what the Business Associate can and cannot do with the data. Today, under HIPAA, the Covered Entity is the liable party because they are the controllers of the data. The obligations/responsibilities of the Covered Entity are significantly different than the obligations of the Business Associate and this distinction should not be intermingled. Regulatory, civil and criminal treatment of Business Associates as Covered Entities would cause considerable confusion and we urge that legislation maintain a clear distinction with regard to Business Associates' responsibilities and how they are applied without seeking to equate them to Covered Entities.

In addition, because of the sensitivity of patient data held in PHRs, the EHR Association believes that providers of PHR that are primarily offered by those providers to "patients", and who are not always operating as Business Associates of Covered Entities, should be brought within the HIPAA privacy and security framework. Many providers of PHR solutions to "healthcare providers" are already Business Associates of Covered Entities and are adequately covered by the current HIPAA privacy and security framework and therefore should not be further burdened with additional regulation.

Finally, it is important to recognize that there are many types of Business Associates, each of which has differential needs for access to PHI and de-identified data and each of which has a different view of or indirect relationship with the individual patient. A focus on contractual agreements between Covered Entities and Business Associates will be the best way to ensure that Business Associates operate under agreements that reflect the specific risks and associated mitigation strategies

Consent:
The EHR Association believes that the current HIPAA TPO consent provisions are sufficient to protect patient privacy. The proposed changes giving individuals the ability to select what medical information to disclose for TPO (and to whom) will have the unintended impact of creating patient safety risks, slowing or preventing interoperability, impeding day-to- day healthcare operations (and increasing their cost and complexity) and preventing many types of quality management programs (for example those sponsored by a health plan).

Background: HIPAA allows for PHI, in the minimum necessary form, to be electronically exchanged among Covered Entities (CEs) for TPO. CEs can apply their discretion in obtaining consent from patients for the use and disclosure of PHI for TPO. When disclosures of PHI are made beyond what is permitted under HIPAA, such as for fundraising, authorization is required from affected individuals. Beyond what is required under HIPAA, states can impose consent requirements for PHI that provide stronger protections for patient privacy, such as in the case of psychotherapeutic services.

Proposed health IT legislation included provisions that would enable individuals to restrict what PHI can be disclosed to a Covered Entity for the purposes of payment or healthcare operations if the individual pays out of pocket for a healthcare service and the information is to be disclosed to a health plan (except for treatment) unless otherwise required by law. Other proposed legislation would require a healthcare provider to receive a patient's consent to use or disclose PHI for healthcare operations if that provider maintains that patient's information in an electronic medical record (EMR).

EHR Association Position: Healthcare operations are an essential element of delivering healthcare services to patients, including, for example, quality management programs. In addition, healthcare operations include business management and general administration and support services used to deliver care to patients. Enabling patients to limit the disclosure of particular PHI could cause much confusion to the healthcare provider as they must use the IT systems to treat and manage their patients and evaluate quality of care; and in some emergency cases could impede obtaining consent for critical healthcare services. Healthcare operations and payment are now an essential and integral element of an increasingly complex and coordinated

healthcare system. It would be cumbersome, if not impossible, to require consent for some patients and not others with respect to such integral and interrelated components of the health care system, many of which access PHI but not on a patient-by-patient basis.

Minimum Necessary and Limited Data Set:
The EHR Association believes that the "minimum necessary" standard, required by HIPAA, already provides for a strong, safe and flexible approach to protecting privacy. The limited data set does not provide enough information for carrying out everyday TPO and essential activities.

Background: According to HIPAA, a Covered Entity must make reasonable efforts to limit itself to "the minimum necessary" data to accomplish the intended purpose for the use, disclosure or request. Under the law, CEs must develop policies and procedures that limit information uses, disclosures and requests to those that are only necessary to carry out the work. The minimum necessary standard does not apply to PHI disclosures by and among healthcare providers for treatment purposes, the individual who is subject to the information, compliance reviews and to comply with requirements of other laws. HIPAA also includes an exception to the Privacy Rule that does not require the authorization from the individual for research use of PHI. A limited data set can include such information as dates of birth, zip code, state and dates of services.

Proposed health IT legislation aimed to further restrict the use and disclosure of PHI through legislation that would limit CEs, to the extent practicable, to a limited data set.

EHR Association Position: The EHR Association believes that the "minimum necessary" standard, required by HIPAA, already provides for a strong, safe and flexible approach to protecting privacy. The limited data set does not provide enough information for treating patients or for the effective functioning of the health care system.

Breach of PHI and Enforcement of HIPAA:

Breach
The EHR Association supports notification to individuals concerning the breach of PHI by the Covered Entity or Entities with the relationship with the individuals or with a business associate that has assumed responsibility for such notification

Background: A breach of PHI involves the unauthorized acquisition, access or disclosure of PHI that compromises the security, privacy and integrity of PHI maintained by or on behalf of a person. Under the HIPAA Privacy Rule, patient health information is protected if it is maintained or transmitted by a healthcare provider, health plan, healthcare clearinghouse or any of their Business Associates, whether the information is electronic, on paper or spoken. Under the current law and regulations, penalties for the unauthorized disclosure of PHI are severe. For privacy: a person who knowingly violates the privacy rules and uses or discloses PHI may be fined not more than $50,000, and imprisoned not more than one year, or both; if the offense is committed under false pretenses, they may be fined not more than $100,000, and imprisoned not more than five 5 years, or both; and if the offense is committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, they may be fined not more

than $250,000, imprisoned not more than 10 years, or both. Enforcement authority resides with the Department of Justice (DoJ) HHS' Office of Civil Rights (OCR).

Proposed legislation aimed to create additional requirements for addressing the breach of PHI. For example, legislation that addressed the breach of unencrypted PHI would require that CEs under HIPAA notify individuals whose information has been, or is reasonably believed to have been, breached. In the case of Business Associates, a Business Associate would be required to notify the Covered Entity of a possible breach. This legislation included timelines for notification, such as no later than 60 days after discovery.

Proposed legislation aimed to strengthen enforcement of HIPAA by authorizing state attorneys general to enforce all federal privacy and security laws.

EHR Association Position: With regard to triggers that result in the determination of a breach and notification to an individual, the EHR Association believes that the Secretary of HHS should establish risk-based standards and time limits for notification. As states adopt "breach laws" that set requirements for a duty to report breaches of privacy, inconsistencies can emerge as to what must be reported, when and by whom. For example, under Michigan law, the entity that physically holds the data bears the duty to report a breach, and not the entity that collects the data. If a hospital is managing its own electronic health record system as a local installation, the hospital would bear the duty, but if it were an ASP-hosted system, it would be the ASP host. This creates a complex, confusing and non-coordinated web of breach policy and specifically creates a burden to report breaches that happen from end use not related to any activities, in this case, that the ASP host would be in a position to know. ASP hosts should be expected to be accountable for audit of their own employees, but cannot be accountable for policing their clients' end user access. Nationally developed standards would identify which pieces of PHI must be included in a breach to warrant a notification to an individual, what circumstances define a breach and provide guidance to CEs as to policy requirements for reporting breaches of privacy related to PHI. Such an approach would ensure that individuals are notified only when there is a real likelihood of harm related to the unauthorized acquisition, access or disclosure of PHI. We urge that this approach becomes a national standard that supersedes state laws.

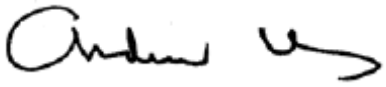
Enforcement

The EHR Association supports the initiation and prosecution of those who willfully violate HIPAA privacy and security provisions. Those functions should remain the purview of the Department of Health and Human Services and the Justice Department.

In reference to the authority of state attorneys general, the Association believes that responsibility for HIPAA enforcement should remain within the DoJ and HHS' OCR. The Association believes that granting additional enforcement authority to state attorneys general would not result in nor guarantee greater compliance to HIPAA, and could create a much less uniform approach to enforcement of federal laws and regulations. It was precisely the need for greater national uniformity of healthcare privacy and security that originally led to these provisions.

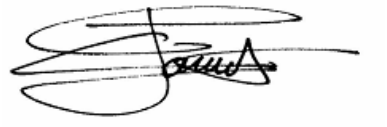
HIMSS EHR Association Executive Committee

Justin Barnes
Chairman, EHR Association
Greenway Medical Technologies



Andrew Ury, MD
Vice Chairperson, EHR Association
McKesson Corporation

HealthPort
Lynn Hudson



GE Healthcare Integrated IT Solutions
Charles Parisot

NextGen Healthcare Information Systems
Charles Jarvis

CPSI
Rick W. Reeves

Siemens
Michele McGlynn

Allscripts Healthcare Solutions
Steven Tolle

About HIMSS EHR Association

HIMSS EHR Association is a trade association of Electronic Health Record (EHR) companies that join together to lead the health information technology industry in the accelerated adoption of EHRs in hospital and ambulatory care settings in the US. Representing a substantial portion of the installed EHR systems in the US, the association provides a forum for the EHR community to speak with a unified voice relative to standards development, the EHR certification process, interoperability, performance and quality measures, and other EHR issues as they become subject to increasing government, insurance and provider driven initiatives and requests. Membership is open to HIMSS corporate members with legally formed companies designing, developing and marketing their own commercially available EHRs with installations in the US. The association, comprised of more than 40 member companies, is a partner of the Healthcare Information and Management Systems Society (HIMSS) and operates as an organizational unit within HIMSS. For more information, visit http://www.himssehra.org.