NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.

May 21, 2009

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
Room 509 F
200 Independence Avenue, SW
Washington, DC 20201

45 CFR PARTS 160 and 164

Response to "***Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII [Health Information Technology for Economic and Clinical Health (HITECH) Act] of the American Recovery and Reinvestment Act of 2009; Request for Information***"; hereinafter "Guidance"

Submitted via Federal eRulemaking Portal

Dear Secretary Sebelius:

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nationally-recognized nonprofit consortium that serves as an open, effective, and neutral forum for health information technology (HIT) initiatives that improve health and care. NCHICA is comprised of nearly 200 member organizations, representing the many sectors of the healthcare industry including providers, payers, government agencies, clearinghouses, business associates, research organizations, health care vendors, and attorneys.

NCHICA's role in advancing healthcare technology through the protection of patients' privacy and security of patient data has been well established. NCHICA was actively involved in analyzing and providing support to its members regarding compliance with the provisions of the HIPAA privacy regulation, which became effective in 2003. NCHICA's comments on this Guidance is the result of a collaborative effort from NCHICA's various and diverse member organizations, which, through its activities, have developed considerable expertise in the various aspects of the HIPAA Privacy and Security regulations.

NCHICA's Comments to the Guidance

NCHICA believes that HHS should be commended for the intent behind the Guidance as required by the HITECH Act. It is NCHICA's view that the proposed clarifications to the Guidance provide the protection of the confidentiality of identifiable health information, without compromising the strong protections afforded protected health information (PHI) by HIPAA. Our suggestions for clarification to the Guidance follow:

In particular, NCHICA is providing comment and request for clarification with respect to HHS request for comments:

(1) The security standards for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals for purposes of breach notification,
(2) whether PHI in a limited data set (LDS) should be treated as unusable, unreadable, or indecipherable to unauthorized persons for purposes of breach notification,
(3) request for clarification of breach notification requirements following a breach by a Health Information Exchange (HIE), and
(4) request for clarification in the apparent two inconsistent definitions of 'breach' in Sections 13400 and 13407.

SECURITY STANDARDS:

1) Apparent Conflicting Language Between HIPAA Security Rule And The Guidance

NCHICA is concerned that in declaring encryption and destruction as the only acceptable methods for rendering PHI as "not unsecured", the Guidance conflicts with the HIPAA Security rule. This rule provides significant flexibility, which would encourage the development of newer and improved methodologies to enhance security of PHI. Indeed, 45 CFR 164.306(b)(1) specifically provides that covered entities "*may use **any** security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications of the subpart.*" (Emphasis provided) Accordingly, NCHICA requests the Department not to specify such an absolute standard of only encryption and destruction for rendering data secure.

2) Request For Clarification of Encryption Safe Harbor Requirements Under the "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals"

The Guidance currently states that the "*successful use of encryption depends upon two main features: the strength of the encryption algorithm and the security of the decryption key or process*." Some NCHICA members have asked if there should be a discussion in

the Guidance that Covered Entities (CEs) and Business Associates (BAs) can use to prove that both encryption and strong keys are present on devices after they have already been lost, misplaced, or stolen.

DEFINING LIMITED DATA SET AS ONE OF THE "SAFE HARBOR" PROTECTIONS OF PHI:

In NCHICA's view, there are several convincing arguments for including the LDS as a methodology for securing PHI and as a "safe harbor" in relation to breach notification requirements. These are summarized below.

1) LDS is "Not Fully Identifiable"

For instance, NCHICA notes that when a LDS is disclosed for purposes of treatment, payment, or health care operations, or as permitted or required under 164.502 or under 164.514 (e) for research, public health, or health care operations activities, the fact of the disclosure itself need not be included in the accounting of disclosures of PHI provided to an individual on request under 164.528. The Department established the LDS as a means to be utilized without an authorization from the individual for legitimate research, public health, and health care operations activities. As such, the Department created a subset of "not fully-identifiable PHI," which not only removes direct identifiers but includes an additional mechanism (a data use agreement) that further reduces the risk that a breach of the subset would "compromise[s] the security and privacy of such information" [Section 13400 (1)(A)]. Given that the HIPAA Privacy Rule treats the LDS as "not fully-identifiable PHI" in the context of accounting for disclosures, it is arbitrary and contradictory for the Department now to say that the LDS is, for all intents and purposes, "fully-identifiable" PHI for breach reporting requirements.

2) Notification Barriers Following a Breach of LDS without a "Key"

Section 13402 (a) requires a covered entity to notify each individual "whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, or disclosed during such breach." Similarly, Section 13402 (b) sets out the requirement for business associates to notify covered entities of breaches. As the LDS does not include the "key" for re-identification of individuals, we contend that the covered entity would not have a "reasonable" belief that a breach of the LDS (which contains "not fully-identifiable" PHI) would have necessarily "compromise[d] the security and privacy" of any given individual's protected health information. Furthermore, despite how unlikely it would be for the person who had unauthorized access to the LDS with data elements limited only to date of birth and ZIP code, for example, to re-identify the individuals, all would have to be notified that there was a "breach" of their PHI. This would create unwarranted concerns for them, making them worry without reasonable justification that their most sensitive health information, not just their date of birth and ZIP code, could be posted on the Internet for all to see. Indeed, under the European Union data protection law, this would abuse the proportionality principle, which entails a two-step assessment: (i) "whether the means

employed by the measure to be evaluated are suitable and reasonably likely to achieve its objectives;" and (ii) "the adverse consequences that the measure has on an interest worthy of legal protection and a determination of whether those consequences are justified in view of the importance of the objective pursued." [T. Tridimas, The General Principles of EU Law (Oxford University Press 2007) 139; see also Christopher Kuner, "Proportionality in European Data Protection Law and Its Importance for Data Processing by Companies," Privacy & Security Law Report, Vol. 07, No. 44, 11/10/2008, pp. 1615.]

Examples

NCHICA is providing below some examples of administrative and legal difficulties that may be faced by covered entities that would be required to notify individuals of a breach of an LDS when a breach becomes known to the entity.

Section 13402 (b) requires a BA to notify a CE of a breach and to identify for the CE the individual whose "unsecured PHI" has been, or is reasonably believed to have been breached, i.e., "unauthorized acquisition, access, use, or disclosure." But without the key, it would be impracticable for the recipient of the LDS to re-identify "each individual" as required by this section. Thus, it is likely that a covered entity would have to "re-identify" all of the individuals whose data elements may be contained in the LDS and notify some individuals whose data may not have been included in the purported breach. Again, this creates an over-reaction to the *de minimis* risk identified. As mentioned above, this would raise concerns regarding the proportionality principle.

Similarly, Section 13402(f) requires covered entities to include in a breach notification a "description of the types of unsecured protected health information that were involved in the breach" and "the steps individuals should take to protect themselves from potential harm." NCHICA can see no reasonable means that a covered entity could adequately comply with these requirements in providing a notice of breach in relation to a limited data set. We are equally doubtful about the utility to any specific individual of a breach notice saying, for example, that "a data set containing the date of birth and ZIP code was created for public health or research purposes as permitted by law and was disclosed by us (the CE) to a business associate (or researcher) under a data use agreement that required the recipient to have in place appropriate safeguards to prevent unauthorized use or disclosure – we (the CE) have been notified that the data set, and your date of birth and ZIP code, may have been acquired, accessed, used, or disclosed by an unauthorized person; we suggest that you should take the following steps to protect yourself from harm…"

In order to protect the security and privacy of PHI, the limited data set relies on the deletion of direct identifiers, execution of a data use agreement, and adherence to the minimum necessary standard found at 164.514(d). With these three robust protections in place, NCHICA strongly recommends that the LDS should be included in the revised Guidance as a method for rendering PHI "unusable, unreadable, or indecipherable" to

unauthorized individuals and should provide a safe harbor for CEs, BAs and recipients of LDS, in regard to breach notification to individuals.

3) Disincentive for Use of Limited Data Sets for Research and FDA Drug Safety Sentinel Network

Often, health research requires large data sources, including electronic health records, patient registries, claims databases, and public health data sets. These multiple data sources are utilized for outcome and population research, drug and patient safety analyses, and comparative effectiveness research. Usually and ideally, this research is conducted with limited data sets rather than directly identifiable health information.

The federal government has been strongly supportive of research using health care databases. Two particularly prominent activities would be the clinical effectiveness research funded under ARRA and the FDA Sentinel Initiative, established under the Food and Drug Administration Amendments Act (FDAAA) of 2007.

NCHICA shares support for this position with the federal government. However, we view the exclusion of limited data sets from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals as chilling to both comparative effectiveness research and the active safety surveillance programs established by FDAAA. Therefore, we urge the Department to revise the Guidance to provide that LDS is not subject to the breach notification. This supports health policy goals while still maintaining protection for the security of health information.

If the Department chooses not to exclude LDS from the breach notification requirements, then why would any covered entity allow for the creation, disclosure, and use of limited data sets for public health, research or health care operations purposes? To do so would expose them to the new liabilities (and untold costs) of breach reporting without attendant benefit. Under the proposed Guidance, the costs and liabilities of breach reporting fall upon covered entities. The NCHICA members are concerned that covered entities will seek to reduce exposure by either requiring individual authorization for data use or, alternatively, disclose “minimum necessary” with disclosure accounting. Both of these risk mitigation actions by covered entities would increase health care costs and disincentivize their participation in important external health care and research activities.

REQUEST FOR INFORMATION REGARDING BREACH NOTIFICATION PROVISIONS OF ARRA

The federal government is encouraging sharing of electronic health records (EHRs) among covered entities as a foundation for reducing health care costs while improving health care. As a result, multiple CEs will be sharing data through an HIE. These entities are treated as BAs of the multiple CEs. If there were an instance in which an HIE (a BA) suffered a breach of PHI, that HIE would, presumably, need to notify all of

the CEs that 'provided' PHI relating to a given individual – or perhaps even all the CEs with which it has contracts – and each of those CEs would in turn need to send a notice to the individual that his/her unsecured PHI was acquired, accessed, used, or disclosed in a way that compromised the security or privacy of the individual's information.

NCHICA is concerned that multiple breach notices sent to the same individual from multiple covered entities will confuse the individual and add unnecessary costs. While we understand that an HIE is unlikely to have any direct treatment relationship to an individual and thus is probably not appropriate for the sending of breach notices, we recommend that the Guidance permit that a single shared breach notification can be sent from all or some of the affected CEs.

REQUEST FOR CLARIFICATION REGARDING THE APPARENT INCONSISTENT DEFINITIONS FOR "BREACH" IN HITECH

NCHICA notices that the two definitions of "breach" in Sections 13400 and 13407, respectively, are inconsistent. As we believe that these differing definitions of "breach" most likely reflect a legislative drafting error, NCHICA suggests clarification. Specifically, it appears the term "*breach*" is defined in Section 13400 and used the last sentence of Section 13402(a) is different than the definition and use of "*breach of security*" in Section 13407.

The NCHICA membership recommends the adoption of the definition in Section 13400 throughout HITECH as it appears to be more complete.

EXCEPTIONS FROM BREACH NOTIFICATION (QUESTION 4 IN THE GUIDANCE)

NCHICA members submitted two specific examples that meet the exceptions from breach notification stipulated at 13400(1)(B)(i) and (ii). Those include:

1) An employee accidentally accesses information from a wrong patient in the an EMR system that is not needed for his work but immediately exits the screen and notifies his or her supervisor upon discovery. The employee does not further use or disclose the access.
2) An employee of a covered entity accidentally sends a data file with PHI to another individual within the covered entity who is authorized to view PHI within the minimum necessary boundaries, but not the specific data in the file. The receiving employee deletes the file upon discovery and notifies the sender of the error. The original employee resends the file to the correct individual.

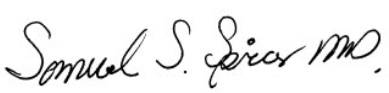
SUMMARY

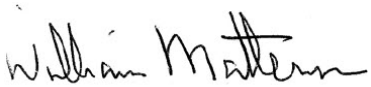
NCHICA appreciates that the Department issued this Guidance relating to technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. While we agree that encryption and destruction are adequate methods to secure PHI, we urge that the Guidance be revised not to preclude or

discourage other new and improved methodologies. Moreover, we urge that the Guidance be clarified so that the use of Limited Data Sets are encouraged rather than rendered impracticable as would result from the current language in the Guidance. Otherwise, NCHICA is concerned that there would be a significant negative effect on public health and research activities.

The member organizations of NCHICA include CEs and BAs as well as other entities that support them every day. We are concerned that the new breach reporting requirements of Sections 13402 will have a chilling effect on the health sector, including health research. We urge the Department to revise the Guidance issued for public comment before issuing the final Guidance document.

Respectfully submitted,





W. Holt Anderson	Samuel S. Spicer, MD	William D. Mattern, MD
Executive Director	President	Chairman of the Board