



October 23, 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

RIN: 0991-AB56
Breach Notification for Unsecured Protected Health Information
Interim final rule with request for comments

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, attorneys and the North Carolina Consumer Advisory Council on Health Information.

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 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 Interim Final Rule – Selected Provisions

As defined by ARRA, *breach* means the acquisition, access, use, or disclosure of PHI which compromises the security or privacy [emphasis added] of the PHI. The Rule (at § 164.502) further elaborates on the meaning of “compromises” security or privacy, noting that “For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm [emphasis added] to the individual.” NCHICA supports this definition, which operationalizes the statutory direction that a breach must “compromise” security or privacy in some meaningful way. By requiring CEs (Covered Entities) and BAs (Business Associates) to exercise judgment in assessing the risk posed by a breach, the Rule aligns federal breach reporting requirements with those of most state laws and will serve to protect individual privacy by encouraging responsible information security practices rather than reliance on pro forma notifications of

North Carolina Healthcare Information and Communications Alliance, Inc.

PO Box 13048, Research Triangle Park, NC 27709-3048

(919) 558-9258 www.nchica.org

Page 1 of 5



breaches to individuals who, if a significant risk of harm has not occurred, have no practical steps to take toward remedying a non-existent harm.

Even as the Interim Final Rule incorporates a risk of harm threshold for breach reporting, it substantially increases the obligations of HIPAA covered entities and business associates. Health care entities must establish programs to monitor for and detect breaches, establish processes to evaluate whether a breach poses a significant financial, reputational, or other harm to individuals, document risk assessment processes and results, and determine when providing notice to individuals, the Department and the media is required. Such actions will strengthen consumer trust in health care organizations and provide meaningful, actionable information to individuals. By contrast, notification of individuals when there is not significant risk of harm would engender unnecessary concern at best, and ‘notice fatigue’ at worst.

Some may suggest that providing a measure of discretion to CEs and BAs for determining whether a harm standard has been met will lead to HIPAA covered entities failing to provide notifications to individuals when a meaningful breach has occurred – we strongly disagree that this will be the result. In fact, absent clearer guidance for determining what constitutes a “significant risk of financial, reputational, or other harm to the individual,” we believe it far more likely that risk-averse covered entities and business associates will over-report possible breaches. (The negative impact of the current HIPAA Privacy Rule on research supports the idea that CEs are unlikely to exercise the level of discretion afforded to them. NCHICA commends to the Department the IOM Report “Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research” for a fuller discussion of the need for a balance between privacy and necessary research.) Related to the question of making a determination as to whether a breach “compromises the security or privacy of protected health information,” NCHICA suggests that the Department continue and extend the very useful discussion begun in the Interim Final Rule of factors to be considered in assessing “risk of financial, reputational, or other harm” with additional Guidance or other communications, such as an FAQ on the topic.

In discussing the definition of *breach* the Interim Final Rule clarifies that an “unauthorized” acquisition, access, use, or disclosure of PHI is one that is not permitted by the Privacy Rule. We support this clarification, as well as the corollary statement that not all violations of the Privacy or Security Rules will constitute breaches or trigger notification obligations. This provides a clear roadmap that when a CE or BA discovers a use or disclosure in violation of the Privacy Rule, it should then determine whether such use or disclosure “compromises the security or privacy” of the PHI. However, this section also raises the possibility that a violation of the *minimum necessary* requirement of the Privacy Rule could trigger notification; again, we would have found useful a corollary statement that neither minimum necessary use violations, which typically occur within the CE, nor minimum necessary disclosure violations, if made as permitted to another CE or BA similarly covered by the Privacy and Security Rules, would be likely to trigger notification. In fact, while other Privacy Rule violations may indeed result in reportable breaches, we are hard pressed to envision a circumstance in which a minimum necessary violation could lead to a risk of significant harm to the individual. We suggest, then, that a discussion of the interaction between minimum necessary and breach reporting requirements be taken up in a separate Guidance regarding what constitutes “minimum necessary” as called for at Sec. 13405 (b)(1)(B) of ARRA.

For reasons outlined at length in our comment of May 21, 2009 to the previous draft Guidance and Request for Information, NCHICA continues to believe that the breach notification

North Carolina Healthcare Information and Communications Alliance, Inc.

PO Box 13048, Research Triangle Park, NC 27709-3048

(919) 558-9258 www.nchica.org

Page 2 of 5



requirements imposed on CEs and BAs by this Interim Final Rule should not apply to limited data sets (LDS), as the “acquisition, access, use, or disclosure” of an LDS in a manner not permitted by the Privacy Rule is, simply, highly unlikely to pose “a significant risk of financial, reputational, or other harm to the individual.” With direct identifiers removed, a data use agreement in place and, as we suggested, a requirement that decryption keys be maintained separately from the data set, we believe that the privacy and security risks involved in re-identifying the unique individuals for whom a single data element (e.g., date of hospital discharge) was included in an LDS will greatly outweigh any benefit of notification, which would provide no useful or actionable information to the individual.

While we appreciate that the Department has decided (at § 164.402 (1)(ii)) that an LDS that does not include date of birth and zip code does not compromise the security or privacy of PHI and thus is excluded from the definition of breach, NCHICA is concerned that this ‘redefinition’ of limited data sets will actually result in less availability of data sets for important research. Extending our request for additional guidance, perhaps in the form of an FAQ, we would suggest that the Department clarify that when performing a risk assessment relating to a potential ‘breach’ of a limited data set, a CE should presume that such a non-permitted use or disclosure will not involve a significant risk of harm absent specific and compelling evidence to the contrary.

NCHICA supports the exclusions to the definition of breach outlined in § 164.402 (2). We would suggest that § 164.402 (2)(ii) should be amended to read: “any inadvertent disclosure by a person... to another person authorized to access protected health information at the same **or another** covered entity or business associate... and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted...” Simply, we believe that inadvertent disclosures to other entities that are covered by the Privacy and Security Rules will not result in a significant risk of harm to individuals and therefore should be excluded from the definition of breach. In fact, the discussion suggests that a reporting obligation would not attach to such an inadvertent disclosure “unless the information is [then] breached while at the third party [if the third party is itself a covered entity] and it is then the third party that “will be responsible for complying with the provisions of this interim final rule.” (On a related note, we appreciate the clarification that “a covered entity or business associate is not responsible for a breach by a third party to whom it permissibly disclosed protected health information, including limited data sets, unless the third party received the information in its role as an agent of the covered entity or business associate.”).

With regard to the breach reporting obligations of multiple CEs that may ‘provide’ PHI to a comprehensive record ‘through’ a RHIO or HIE, we find the discussion of § 164.410 unhelpful on this point: “Thus, following the discovery of a breach of unsecured protected health information, a business associate is required to notify the covered entity of the breach so that the covered entity can notify affected individuals [emphasis added]... In cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potential affected covered entities” – whom, we note, will then be required to send multiple breach notices to the same individual. Unfortunately, we find very unhelpful the Department’s assertion that, “we believe it appropriate to leave it up to covered entities and business associates to determine how the required reporting should be implemented.” Again, NCHICA suggests the need for further guidance relating to the reporting obligations of covered entities in such situations.

North Carolina Healthcare Information and Communications Alliance, Inc.

PO Box 13048, Research Triangle Park, NC 27709-3048

(919) 558-9258 www.nchica.org

Page 3 of 5



Concluding Comments

Especially in light of the significant administrative requirements – including but not limited to additional workforce training and sanctions, the establishment of new complaint procedures, and the development of new risk assessment procedures and documentation – (at § 164.530) faced by CEs and BAs in order to comply with this Rule, NCHICA appreciates the Department’s decision “to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication of this rule”. While covered entities and business associates will, of course, make every effort to comply with the Rule, the opportunity to access advice and technical assistance between now and February 23, 2010 will better support the transition to widespread compliance than would the application of sanctions.

Finally, having noted the burden of new administrative requirements, NCHICA must point out that very significant costs will be incurred to comply with these breach notification requirements. From developing programs to monitor and detect potential breaches and establishing risk assessment procedures (e.g., constituting risk assessment teams,) to training staff, retaining additional legal personnel and developing a range of new communication channels for consumers, the costs to covered entities and business associates will not be trivial. We urge the Department to maintain and as possible extend the common sense balance between privacy protection and return on investment in an already overstressed and extraordinarily expensive health care system that we see in certain provisions of the Interim Final Rule, exemplified best by the inclusion of a harm standard in making a determination regarding a potential breach.

IN SUMMARY

NCHICA appreciates that the Department issued this Guidance relating to technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. 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.

Here is a summary of our suggestions:

- The Department continue and extend the very useful discussion begun in the Interim Final Rule of factors to be considered in assessing “risk of financial, reputational, or other harm” with additional Guidance or other communications, such as an FAQ on the topic.
- A discussion of the interaction between minimum necessary and breach reporting requirements be taken up in a separate Guidance regarding what constitutes “minimum necessary” as called for at Sec. 13405 (b)(1)(B) of ARRA.
- Extending our request for additional guidance, perhaps in the form of an FAQ, we would suggest that the Department clarify that when performing a risk assessment relating to a potential ‘breach’ of a limited data set, a CE should presume that such a non-permitted

North Carolina Healthcare Information and Communications Alliance, Inc.

PO Box 13048, Research Triangle Park, NC 27709-3048

(919) 558-9258 www.nchica.org

Page 4 of 5



use or disclosure will not involve a significant risk of harm absent specific and compelling evidence to the contrary.

- The Department should maintain and, if possible, extend the inclusion of a harm standard in making a determination regarding a potential breach.
- 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.
- Unfortunately, we find very unhelpful the Department's assertion that, "we believe it appropriate to leave it up to covered entities and business associates to determine how the required reporting should be implemented." Again, NCHICA suggests the need for further guidance relating to the reporting obligations of covered entities in such situations.

NCHICA thanks the Department for issuing this Interim Final Rule and appreciates the opportunity to submit comments. Please feel free to contact me at any time for further discussion of the issues raised here.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'W. Holt Anderson'.

W. Holt Anderson
Executive Director