May 29, 2009

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

16 CFR Part 318 – Proposed Rule

Health Breach Notification Rulemaking
Project No. R911002

Dear Secretary Clark:

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research organizations (CROs). Our member companies provide a wide range of specialized services across the entire spectrum of development for new drugs, biologics and medical devices, from pre-clinical, proof of concept and first-in-man studies through post-approval and pharmacovigilance research. With more than 70,000 employees engaged in research activities around the world, ACRO advances clinical outsourcing to improve the safety, quality and efficiency of biomedical research.

In general, CROs are neither covered entities (CEs) nor business associates (BAs) under HIPAA. While we may collect, transmit, analyze, use and disclose protected health information (PHI) in the course of a clinical trial, we do so with the research participant's informed consent and a HIPAA authorization. Though we are not subject directly to HIPAA, we frequently receive PHI from physicians, hospitals and other covered entities that are, and we are fully committed to protecting the security and confidentiality of individual health data. Further, beyond our work in clinical trials, the member companies of ACRO regularly use de-identified data and limited data sets in the course of late-phase work, including safety surveillance and epidemiology studies, patient registry and health outcomes analyses, comparative effectiveness research (CER), and the like.

Just as we are not CEs or BAs under HIPAA, neither are CROs vendors of personal health records (PHRs). However, certain CRO activities, such as developing a website to assist in the recruitment of research participants into a clinical trial, may qualify as what the Commission calls the "web-based entities that collect consumers' health information" that will be among the subjects taken up in a study and report by the Secretary of Health and Human Services (HHS), in

818 Connecticut Avenue, NW, Suite 1100, Washington, DC, 20006
T 202 464 2310 F 202 464 2309 E info@acrohealth.org www.acrohealth.org

ACRO
ASSOCIATION OF CLINICAL RESEARCH ORGANIZATIONS

consultation with the FTC, to be delivered to Congress not later than February 17, 2010. Called for by Section 13424(b) of the American Recovery and Reinvestment Act (ARRA), this report is to include recommendations regarding privacy, security and breach notification requirements that should apply to entities that are not CEs or BAs under HIPAA, but are "vendors of personal health records and online applications that interact [emphasis added] with such personal health records." Section 13424(b)(1)(A)(ii-iv) of ARRA describes a range of entities to be included in the Secretary's report and subject to the temporary breach notification requirements called for at Section 13407, which are the subject of this proposed rule. These include: "entities that offer products or services through the website of a vendor of personal health records; entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records; [and] entities that are not covered entities and that access information in a personal health record or send information to a personal health record." Even though no CRO web-based services "interact" with PHRs today, this very expansive language could have the effect of 'capturing' web portals that simply offer health information to consumers and or in some way interact with individuals around health information, so it is possible that certain consumer-facing activities of a CRO could be included as one of the entities of 13424(b)(1)(A)(ii-iv).

Because certain CRO activities could be implicated by this NPRM and because we are very much interested in the Secretary's report that is to follow, ACRO is pleased to submit the following comments on the proposed rule regarding health breach notification outside of HIPAA.

Section-by-Section Comments

Proposed Section 318.1: Purpose and scope

We support the FTC's interpretation that the language of Section 13407 of ARRA is not limited to the Commission's Section 5 jurisdiction and does include non-profit entities.

Responding to questions (1) and (2), we are concerned that the definition of "other entities" at ARRA 13424(b)(1)(A)(ii-iv) is so broad that it captures not only "web-based entities that collect consumers' health information" but entities that advertise goods and services without collecting or accessing individually identifiable health information, and services that simply offer health information, via messages such as "see what the CDC says about how to protect yourself from H1N1" or "want to know more about clinical trials?" Other "related entities" may never contain protected health information (PHI) covered by HIPAA, but only hold the portion of "PHR identifiable health information" that is provided directly by the individual and never allow access to such information to anyone other than the individual, i.e., the service simply holds the individual's personal health information like a paper notebook would.

Within the limits of the legislative language, we urge the FTC to be judicious in applying the temporary breach notification requirements of the proposed rule to the range of entities under its jurisdiction. Certainly, there seem to us to be qualitative differences between the potential risks

to privacy that could be posed by: 1) a third party service provider that works for or on behalf of a PHR vendor and has access to PHR identifiable health information; 2) an online application that accesses or analyzes a PHR containing PHI received from multiple CEs in order to facilitate care management of a complicated chronic illness, such as diabetes; 3) an online application that contains only information provided by the individual, such as a workout regimen that notes the individual's heart rate along with the number of sit-ups or push-ups she does each day; and 4) an entity that simply advertises products or services through the website of a hospital that happens to offer a PHR to its patients but does not interact with the hospital PHR in any way. *To the extent that they collect, maintain, use or disclose an individual's identifiable health information*, each of these entities should be subject to privacy, security and breach notification requirements, but we question whether those requirements should be the same and we hope that the Secretary and the FTC will carefully consider the issue of relative risk in crafting the report and recommendations to be delivered to Congress within one year.

Proposed Section 318.2: Definitions

Breach of security – We recognize that the differing definitions of breach contained at ARRA 13407(f) and 13400(1)(A) might be better harmonized. However, given the concern that PHR identifiable health information is very broadly defined, and that PHR vendors, third party service providers and related entities are not provided the kinds of 'exceptions' relating to breach specified at 13400(1)(B), we do not support the Commission's expansive interpretation of the legislative language, such that "unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any [emphasis added] unauthorized acquisition of such information." Not only does this exceed the plain language of 13407(f)(1) but in placing the burden of proof on the entity that unauthorized access could not have resulted in acquisition, the usual standard for breach reporting – that the entity 'knows or should have known' that a breach has compromised the security or privacy of information – has been expanded almost beyond recognition.

Personal health record – The language of ARRA says that a PHR is "managed, shared, and controlled by or primarily for the individual." We note that the term "primarily for" is not the same as "on behalf of" and seems to get us into a question of the PHR vendor's intent; for example, is the PHR 'primarily for' the individual's management of his care, or is it primarily for the revenue stream of the vendor? We would appreciate clarification of the Commission's thinking on this issue.

PHR identifiable health information – In response to the Commission's query regarding whether "there may be additional instances where, even though the standard for de-identification under 45 CFR 164.514(b) is not met, there is no reasonable basis to believe that information is individually identifiable," we have included as Appendix A here ACRO's May 20, 2009 comment regarding the "guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals…." As you will

see in the comment, we believe that, when properly implemented with a data use agreement between two parties, a "limited data set" as defined at 45 CFR 164.514(e) would not provide a reasonable basis for assuming that a given individual whose data elements have been acquired by an unauthorized individual could have been re-identified, and therefore that the limited data set should be considered "not unsecured" and excepted from breach notification requirements.

PHR related entity – We appreciate the examples provided by the Commission here, and will comment briefly.

We agree that, because of the nature of the health information that it will access or collect in order to perform its function, a "web-based application that helps consumers manage medications" is a "related entity." (In fact, in some instances, such an application may be a PHR.)

Given the expansive definition of PHR identifiable health information, it may well be that "a website offering an online personalized health checklist" is a related entity but, again, we suggest that breach notification requirements should be tailored to reflect the actual level of risk to the "security and privacy" of information offered by an individual consumer, especially if such information is 'low risk' on its face.

While we recognize that a "brick-and-mortar company advertising dietary supplements online" may meet a related entity definition, (by offering such advertising on the website of a PHR, for instance,) unless the company collects or maintains PHR identifiable health information, we are unclear as to how and why the breach reporting requirements of the proposed rule would apply.

Unsecured – Please see our comments regarding "limited data sets" at Appendix A below.

<u>Proposed Section 318.3: Breach notification requirement</u>

Proposed paragraph 318.3(b) requires that a third party service provider's notification to a PHR vendor or related entity of a breach shall include "the identification of each individual" whose information "has been, or is reasonably believed to have been acquired during such breach." Again, ACRO asks the Commission to review our comment at Appendix A, which outlines some of the very significant difficulties that will be faced by third party providers, and the PHR vendors and related entities they work for, in making such "identification of each individual" if sound information management principles have been followed in the first place. That is, if the third party provider is accessing or using only as much PHR identifiable health information as is required for a given task, such as billing, such "identification" of individuals may not be easy, or even possible. Put another way, if only what HIPAA calls "minimum necessary" information or a "limited data set" has been disclosed to the third party service provider, not only will the PHR vendor or related entity have the burden of breach notification but it may well have the task of 're-identifying' individuals as well. This re-identification process, undertaken solely for the purpose of sending breach notices about data whose compromise poses extremely low risk, would not only be expensive and burdensome, but also would expose the data subjects to new risks based on the re-identification of their data.

Proposed Section 318.5: Methods of notice

Proposed paragraph 318.5(a)(1) requires notification of individuals by first-class mail "or, if the individual provides express affirmative consent, by electronic mail." In its analysis, the Commission goes on to explain that "entities may obtain such consent by asking individuals, when they create an account [emphasis added], whether they would prefer… first-class mail or e-mail." With an effective date of September 18, 2009, we do not see any transition provisions in the proposed rule – which moves us to ask, in the case of a PHR or related entity that is currently offering services to thousands or even millions of individuals, would the Commission have those entities send an e-mail to each requesting a consent to receive an e-mail in the case of a breach? And would the Commission further require that the accounts of the 10 or 20 or 50 percent of individuals who did not reply to the e-mail asking for consent to receive e-mails be closed? We suggest that the requirement of "express affirmative consent" should apply to accounts opened after the effective date of the final rule.

At 318.5(a)(1) the Commission further states that it "does not regard pre-checked boxes or disclosures that are buried in a privacy policy or terms of service agreement to be sufficient to obtain consumers' express affirmative consent." ACRO believes that in an online environment, in which all interactions between the consumer and the entity take place electronically, the proposed standard for express consent is too strict. Certainly, affirmative consent should not be "buried" but it seems unreasonable for the Commission to prohibit online entities that communicate with customers only electronically from including in their terms of service a clear and conspicuous statement such as, "this service operates only online – we do not collect mailing addresses – whenever we communicate with you, including if we need to notify you of a breach in which information was acquired by an unauthorized party, we will do so by e-mail."

318.5(a)(4)(i) states that if 10 or more individuals cannot be reached by first-class mail, e-mail, telephone, or other methods, the PHR vendor or related entity may use two substitute methods of notice, including "through a conspicuous posting for a period of six months on the home page of its website." While we think that, particularly for online services, this method of substitute notice is preferable to the alternative of a posting in "major print or broadcast media," the period of six months seems to us both arbitrary and excessive – we would suggest, instead, 30 days or 60 days.

For reasons of both pragmatism and policy, ACRO would suggest that proposed paragraph 318.5(c) be modified to state that the "annual log" of breaches of fewer than 500 individuals be submitted to the FTC in each calendar year in which any breaches occur. The proposed rule 'starts the clock' from the date of an entity's first breach, which could mean hundreds of different starting dates for these annual logs. We think it would be far simpler, and of more value to consumers, for a PHR vendor or related entity to report that it had xx breaches in the last calendar year. This method of reporting would permit the Commission to aggregate the number of breaches reported across all entities in its jurisdiction for any given year.

Proposed Section 318.6: Content of notice

This section mirrors the requirements laid out in ARRA 13402(f). Without making extensive comment, we will note that the content of the notice required at 318.6(b) and (c) will vary wildly, depending upon the kind of PHR identifiable health information at issue. That is, one notice will say, "Your name, Social Security number, date of birth, and health insurance information were acquired by an unauthorized individual, and you should now be careful of identity theft, request credit reports, etc." while another would say, "Your name, daily weight, and log of miles run over the last 30 days was accessed by an unauthorized individual, but we do not believe there are steps you need to take to protect yourself from harm at this time." Both of these 'breaches' would require a notice by the PHR vendor or related entity application, along with attendant costs – yet, the first notification could provide real value to the individual, while it is difficult to see any particular utility to the consumer in the second. Such 'equivalence' lacks any real 'proportionality' and, again, we urge the Commission to be very judicious in its enforcement of the final breach notification rule.

ACRO thanks the FTC for its very timely issuance of this proposed rule. We appreciate the opportunity to provide comments and look forward to working with the Commission in the future, as our member companies develop new online and consumer-facing services that will help us facilitate clinical and health research.

Please do not hesitate to contact ACRO for additional information.

Sincerely,

Douglas Peddicord, Ph.D.
Executive Director

Appendix A

May 20, 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 Act) of the American Recovery and Reinvestment Act of 2009; Request for Information"

Dear Secretary Sebelius:

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research organizations (CROs). Our member companies provide a wide range of specialized services across the entire spectrum of development for new drugs, biologics and medical devices, from pre-clinical, proof of concept and first-in-man studies through post-approval and pharmacovigilance research. With more than 70,000 employees engaged in research activities around the world, ACRO advances clinical outsourcing to improve the quality, efficiency and safety of biomedical research.

In general, CROs are neither covered entities (CEs) nor business associates (BAs) under HIPAA. While we may collect, transmit, analyze, use and disclose protected health information (PHI) in the course of a clinical trial, we do so with the research participant's informed consent and a HIPAA authorization. Though we are generally not subject to HIPAA, we frequently receive PHI from physicians, hospitals and other covered entities that are, and we are fully committed to protecting the security and confidentiality of individual health data. Further, beyond our work in clinical trials, the member companies of ACRO regularly use de-identified data and limited data sets in the course of late-phase work, including safety surveillance and epidemiology studies, patient registry and health outcomes analyses, comparative effectiveness research (CER), and the like. Thus, we are pleased to submit comments on the above-referenced Guidance and Request for Information.

Scope of the Guidance

Section 13402 of the American Recovery and Reinvestment Act (ARRA) (Pub. L. 111-5) requires HIPAA covered entities (CEs) and their business associates (BAs) to provide for notification to individuals (by CEs) and to covered entities (by BAs) in the case of breaches of unsecured protected health information (PHI). Section 13407 of the Act similarly provides that vendors of personal health records (PHR vendors) and certain other entities will provide notification to individuals, and third party service providers that provide services to PHR vendors will provide notification to the PHR vendor in the event of a breach of unsecured PHR identifiable health information.

The Guidance explains the Department's current best thinking regarding technologies and methodologies that render PHI, and PHR identifiable health information, "unusable, unreadable, or indecipherable to unauthorized individuals" – and thereby not "unsecured" PHI or PHR identifiable health information. Application of technologies and methodologies specified in the Guidance render PHI not "unsecured" and will provide a safe harbor for breach notification requirements to be issued by HHS in interim final regulations by August 17, 2009, as well as the breach notification requirements announced by the Federal Trade Commission (FTC) in a notice of proposed rulemaking (NPRM) under 16 CFR Part 318 issued on April 16, 2009.

ACRO thanks the Department for issuing this Guidance.

Comments on the Guidance

The Guidance specifies two technologies that render PHI not "unsecured": 1) **encryption** and 2) for the media on which PHI is stored or recorded, **destruction** such that paper, film or other hard copy media cannot be read or otherwise reconstructed, and electronic media have been cleared, purged, or destroyed. The Department states that these two technologies or methodologies are "intended to be exhaustive and not merely illustrative" but asks for public input on whether there are other specific technologies and methodologies that should be included as ways to render PHI not unsecured.

The Guidance uses the HIPAA Security Rule definition of encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. The Guidance specifies that encryption processes tested by the National Institute of Standards and Technology (NIST) meet this definitional standard and provides specific references to NIST publications that stipulate valid encryption processes for "data in motion" and "data at rest"; NIST guidelines for electronic media sanitization are also referenced. (Future iterations of the Guidance will apply to recommendations of the HIT Policy Committee concerning the development of technologies that will allow PHI to be not "unsecured" specifically when it is transmitted within a nationwide health information network or physically transported outside the "secured physical perimeter of a health care provider, health plan, or health care clearinghouse.")

The Guidance notes that successful use of encryption depends upon two factors: the strength of the encryption algorithm, and the security of the decryption key or process – **as it revises the Guidance, ACRO suggests that the Department consider including a best practice recommendation: that encrypted data and any encryption key or process be maintained separately, for instance on separate servers, in order to lessen the chances of unauthorized access to both encrypted data and the decryption key at the same time**.

Setting aside for the moment the issue of the limited data set (which will be taken up in the sections below,) we are not aware of other current alternatives to the technologies and methodologies (encryption and destruction) for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. However, we do note that in specifying these methods only, the Department has chosen to not include the alternative option articulated by Congress at Section 13402 (h)(1)(B) as a technology standard that "is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute." We recognize that in promulgating this Guidance in timely fashion, the Department was not required to include such a 'default' option. However, since neither the Department nor the other Federal information security experts it consulted can be aware of all technologies and methodologies for rendering data secure that may be developed in the future, we question whether the categorical commitment to *encryption* and *destruction* stated in the Guidance may have the effect of discouraging future innovation in information security.

We are also concerned that in declaring encryption and destruction the only acceptable methods for rendering PHI "not unsecured" the Guidance conflicts with the HIPAA Security rule, which provides significant flexibility to covered entities. 164.306(b)(1) specifically provides that CEs "may use *any* [emphasis added] security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications of the subpart" and 164.306(a)(1) requires that in looking to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits" the CE's decision regarding which security measures to use [at 164.306(b)(2)] must factor in issues such as: "(i) the size, complexity, and capabilities of the covered entity; (ii) the covered entity's technical infrastructure, hardware, and software security capabilities; (iii) the costs of security measures; and (iv) *the probability and criticality of potential risks* [emphasis added – please see the discussion in the next section relating to a covered entity's "reasonable belief" regarding such risks in the case when a limited data set may have been breached] to electronic protected health information."

In light of the potential negative impact on innovation, and the unnecessary confusion of a covered entity's obligations under the HIPAA Security Rule, ACRO recommends that, in addition to *encryption* and *destruction* the Department include among the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals such technology standards that are "developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute" in future iterations of the Guidance.

ACRO does not support the Department's decision to make the Guidance effective upon issuance. Simply, the Guidance is preliminary to breach notification requirements that will likely not take effect until September 17, 2009, and the Department is soliciting public input on the Guidance, so it is premature to announce that the Department recognizes PHI 'secured' by encryption or destruction only as providing a safe harbor against breach reporting requirements that have not taken effect. While the practical effect of making the Guidance effective immediately is meant, we presume, to provide encouragement to CEs, BAs, PHR vendors, 3rd party service providers, and other entities to move promptly toward encrypting or securely destroying PHI (and PHR identifiable health information) whenever and wherever practicable, for the reasons noted above ACRO objects to the characterization of *encryption* and *destruction* as "exhaustive" and believes the Guidance should be revised before being finalized.

Consideration of the Limited Data Set as an Additional Methodology of Rendering PHI "Not Unsecured"

In developing the Guidance the Department considered whether PHI in a limited data set (LDS) should be treated as unusable, unreadable, or indecipherable to unauthorized persons for purposes of breach notification. The Department noted that including the LDS as a methodology would better align the Guidance with state breach notification laws and would mitigate administrative and legal difficulties that covered entities could face in attempting to notify individuals of a breach in light of limited contact information and requirements in data use agreements. While articulating a decision to exclude the limited data set as a methodology for securing PHI, the Guidance solicits comment on whether the risk of re-identification of an LDS warrants this exclusion and inquires about administrative and legal concerns regarding the ability to comply with breach notification requirements when direct identifiers have been removed from PHI.

We believe that there are a number of compelling reasons for including the limited data set as a methodology for securing PHI and a safe harbor in relation to breach notification requirements.

First, as the Guidance notes, when an 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. In establishing the limited data set as a tool to be utilized without an authorization from the individual for legitimate research, public health, and health care operations activities, 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 the decision of the HIPAA Privacy Rule to treat the LDS as "not fully-identifiable PHI" in the context of accounting for disclosures, ACRO believes it is inconsistent for the Department to suggest now that the LDS is, for all intents and purposes, "fully-identifiable" PHI for breach reporting requirements**.

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* [emphasis added], accessed, acquired, or disclosed during such breach"; Section 13402 (b) similarly outlines the requirement for business associates to notify covered entities of breaches**. If, as we suggested above in recommending that encryption processes and decryption keys be maintained separately, a covered entity, in addition to including all the required elements of a data use agreement specified in 164.514 (e)(4), maintains the 'key' that could be used to re-identify individuals from the data elements included in the LDS and does not provide that key to the LDS recipient researcher or business associate, we would assert 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.**

The Guidance solicits feedback concerning 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 such a breach is known to the entity. We will cite a few examples:

Section 13402 (b) requires a BA to notify a CE of a breach and to identify for the CE the individuals whose "unsecured PHI" has been, or is reasonably believed to have been, breached. If the recipient BA (which could be a CRO performing health outcomes research for a CE under the rubric of *health care operations*) does not have a 'key' with which it could identify the individuals whose data elements, (not including any direct identifiers,) are included in the LDS, we are at a loss as to how the BA could, in fact, identify "each individual" as required by this section. Since the recipient BA cannot identify specific individuals within a limited data set and since a limited data set contains only data elements, such as birth date or treatment date or diagnosis, it is likely that a covered entity would have to "re-identify" all of the individuals whose data elements were contained in the LDS and send a breach notice to each of those persons, unless it makes a determination, as we suggested above, that it does not have a "reasonable" belief that the breach compromised the security and privacy of specific individuals.

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". We are doubtful 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 birth dates and the date of hospital admission of xxx individuals was created for public health or research purposes as permitted by law and was disclosed by us (the covered entity) 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 covered entity) have been notified that the data set, and your birth date or date of hospital admission, 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 tool 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 requirements in place, we strongly believe 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 and BAs in regard to breach notification to individuals**.

Policy Implications of the Exclusion of Limited Data Sets as a Method for Securing PHI

Increasingly, health research involves queries of large data sources, including electronic health records, patient registries, claims databases, public health data sets, and the like; these multiple data environments are utilized, then, for outcomes and populations research, drug and patient safety analyses, and comparative effectiveness studies, among other things. Typically, this research does not involve fully-identified PHI but rather utilizes limited data sets.

The federal government has been strongly supportive of research using health care databases. For instance, ARRA provides $1.1 billion in new funding for comparative effectiveness research; among the stated purposes of this provision is to "encourage the development and use of clinical registries, clinical data networks, and other forms of electronic health data that can be used to generate or obtain outcomes data." Similarly, the FDA Sentinel Initiative, established by the Food and Drug Administration Amendments Act (FDAAA) of 2007, requires the Secretary of HHS to: 1) develop methods to obtain access to disparate data sources; and 2) to develop validated methods for the establishment of a post-market risk identification and analysis system to link and analyze safety data from multiple sources, with the goals of including, in aggregate, at least 25 million patients by July 1, 2010 and 100 million patients by July 1, 2012. The language of Section 905 of the FDAAA – no one should "disclose individually identifiable health information when presenting drug safety signals and trends or when responding to inquiries regarding drug safety signals and trends" – clearly reflects a commitment to the use of limited data sets, rather than fully-identifiable PHI, to the widest extent possible.

As research organizations, the companies of ACRO are very deeply concerned that the decision of the Guidance to exclude the limited data set from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, along with several other provisions of ARRA, establishes significant disincentives to the creation, disclosure, and use of limited data sets by covered entities, business associates, and researchers.

With the general prohibition against remuneration for "sale" of PHI (which includes limited data sets) established by Section 13405(d), the requirement of Section 13405(b) that the minimum necessary principle apply to research uses of PHI (including for *preparatory to research* activities), and a potential interpretation of Section 13408 that would require independent researchers (and CROs, possibly) to become business associates, it is difficult to see why any covered entity would allow for the creation, disclosure, and use of limited data sets for public health, research or health care operations purposes, since to do so would expose them to the new

liabilities (and untold costs) of breach reporting without attendant benefit. Simply, the liabilities and costs of breach reporting fall upon covered entities – and we are very much concerned that covered entities will move in the direction of either requiring individual authorization for data use or, alternatively, a waiver of authorization by an institutional review board (IRB). The latter option can, of course, be utilized to permit the use of fully-identified PHI, in which case more patient-identifiable data will be used, with less privacy protection than is the case today.

ACRO views the exclusion of limited data sets from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals as inimical, to cite just two examples, to the comparative effectiveness research called for in ARRA and the active safety surveillance programs established by FDAAA – and we again call upon the Department to revise the Guidance so that health policy goals can be accomplished even as protection for the security of health information is maintained.

Concluding Comments

ACRO thanks the Department for promptly issuing this Guidance relating to technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. We applaud the decision to incentivize *encryption* and *destruction* of unsecured PHI – but believe **the Guidance as currently stated ignores an opportunity to encourage not lesser but much greater use of *limited data sets* as a bedrock principle for making PHI secure**. We are concerned that the impact of this decision will negatively impact public health and research activities.

The member companies of ACRO are, in general, neither covered entities nor businesses associates – however, we work with CEs and BAs every day, and we are concerned that the new breach reporting requirements of Section 13402 will further disincentivize their participation in clinical and other health research. We urge the Department to revise the Guidance before issuing a draft regulation.

Please feel free to contact ACRO at any time for additional input.

Respectfully submitted,

Douglas Peddicord, Ph.D.
Executive Director