ACLI
Financial Security. For Life.

Roberta Meyer
Vice President & Associate General Counsel
(202) 624-2184 t (866) 953-4096 f
robbiemeyer@acli.com

June 1, 2009

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

Re: Health Breach Notification Rulemaking - Project No. R911002

Ladies and Gentlemen:

The American Council of Life Insurers ("ACLI") is pleased to provide comments to the Federal Trade Commission ("Commission") in response to its request for comments regarding its proposed Health Breach Notification Rule ("Commission's proposed rule"),[1] required under section 13407 of the Health Information Technology for Economic and Clinical Health ("HITECH") Act of the American Recovery and Reinvestment Act of 2009 ("Recovery Act"). [2] ACLI is the principal trade association of life insurance companies, whose 353 member companies account for 93 percent of the life insurance industry's total assets and 94 percent of life insurance premiums in the United States. ACLI member companies are also major participants in the long term care insurance, disability income insurance, pension, and reinsurance markets

Many ACLI member companies are long term care insurers, that are "covered entities" under section 13400(3) of the Recovery Act, that will be subject to the interim final regulations for breach notification of the Department of Health and Human Services ("HHS rule"), required under Recovery Act section 13402. Also, ACLI member company life and disability income insurers, that are business associates of long term care insurers or other covered entities, will be subject to the HHS rule when section 13404 of the Recovery Act is effective on February 17, 2010. ACLI submitted comments to HHS in response to its request for comments regarding the proposed HHS rule and the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,[3] by letter dated May 21, 2009, a copy of which is attached.

ACLI submits these comments regarding the Commission's proposed rule to underscore the need for uniform national standards for health breach notification and to strongly urge the Commission and HHS to continue to coordinate in the development of their breach notification rules, so that that the interim final rules of both agencies and the resulting consumer protections will be as consistent as possible. ACLI also submits these comments to urge important clarification of the scope and applicability of the Commission's proposed rule.

---

[1] 74 *Fed.Reg.*17914(April 20, 2009)
[2] American Recovery and Relief Act of 2009, Pub.L. 111-5
[3] 74 *Fed.Reg.* 19006 (April 27, 2009)

ACLI Legislative Principles Relating to Security Breach Notification

ACLI member companies support the following legislative principles relating to the security of personal information, that provide the basis for ACLI's views regarding the proposed breach notification rules. ACLI member companies support legislation that provides uniform preemptive national standards for notification to individuals whose personal information has been subject to a security breach. ACLI member companies also support legislation that avoids needlessly alarming individuals and undermining the significance of notification of a security breach, by requiring notification only when the security and confidentiality of personal information is truly at risk. ACLI member companies believe that legislation should not require notification if personal information is protected by encryption or some other means that makes the information unreadable or unusable, or if the information is not otherwise likely to be misused.

In view of these principles and the importance of a uniform national standard for health breach notification and consistency between the Commission's and HHS' breach notification rules, ACLI member companies strongly urge the Commission to take the following comments into account. With the exception of the comments that seek clarification as to the scope and applicability of the Commission's proposed rule, the comments set forth below are as consistent as possible with the comments made in ACLI's May 21, 2009 letter to HHS.

Definitions

"Breach of Security"

Section 318.2(a) of the Commission's proposed rule defines "breach of security" as follows:

> Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. 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 unauthorized acquisition of such information.

The definition appropriately excludes unauthorized access of PHR identifiable health information that is unlikely to result in harm or misuse of PHR identifiable health information. As a result, notification of breaches of security will not be required under the Commission's proposed rule if the security of the PHR identifiable health information is not truly at risk, and consumers will not be sent unnecessary notices likely to undermine the significance of breach notification.

However, ACLI urges the Commission to slightly modify the language of the second sentence of the definition to read more clearly as follows *(Language proposed to be added is underlined; language proposed to be deleted is stricken.):*

> Unauthorized acquisition will be presumed <u>not</u> to include unauthorized access to unsecured PHR identifiable health information <u>if</u> ~~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 unauthorized acquisition of such information.

"Personal Health Record"

Because the definition of "personal health record" underlies the definition of "vendor of personal health records," and, as a result, the scope and applicability of the Commission's proposed rule, the definition of "personal health record" is critically important. Although the language of the definition, set forth in Section 318.2(d) of the Commission's proposed rule, is substantially similar to the statutory definition set forth in Recovery Act section 13400(11), there is concern it could be misconstrued to include records not intended by the Congress to be "personal health records."

The Conference Report of the Recovery Act reads in pertinent part as follows:

> Another set of such modifications pertains to the definition of Personal Health Records. Specifically, the report clarifies that Personal Health Records are "managed, shared, and controlled by or primarily for the individual." The technical change clarifies that PHR's include the kinds of records managed by or for individuals, but does not include the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes. By extension, a life insurance company would not be considered a PHR vendor under this title ....[4]

In view of the above, ACLI strongly urges that the definition of "personal health record" be modified to read as follows *(Language proposed to be added is underlined.)*:

> Personal health record means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual <u>Personal health record does not include the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes.</u>

If the Commission decides not to modify the definition of "personal health record," as urged above, at a minimum, ACLI strongly urges the Commission to include within its final rule an explanatory note that contains the language of the Conference Report of the Recovery Act, quoted above.

"PHR related entity"

While the definition of "PHR related entity," set forth in section 318.2(f) of the Commission's proposed rule, generally tracks the language of clauses (ii), (iii), and (iv) of Recovery Act section 13424(b)(1)(A), there is concern with subsection 318.2(f)(3), that would make an entity that "accesses information in a personal health record," a "PHR related entity." The modification to the definition of "personal health record," urged above, is sought to eliminate any possibility that the records of a company, such as a life insurer, that maintains records for its own business purposes, could be construed to be "personal health records," or that such a company could be construed to be a "vendor of personal health records." However, there is concern that even if that modification is made, a life insurer or other company that

---

[4] Conference Report to Accompany H.R. 1, page 490.

maintains records for its own business purposes still could be inappropriately construed to be a "PHR related entity."

Even if the definition of "personal health record" is modified as urged above, the term still could be broadly construed to include additional records not intended by Congress to be "personal health records," such as traditional electronic doctors' records. As a result, there is concern that a company, such as a life insurer, that accesses such doctors' records, could be inappropriately construed to be a "PHR related entity." Such a construction would appear to be contrary to Congressional intent, and unnecessary given the provision for a "Study and Report on Application of Privacy and Security Requirements to Non-HIPAA Covered Entities," required under Recovery Act section 13424.

Accordingly, in addition to modification of the definition of "personal health record," ACLI also urges that subsection 318.2(f)(3) of the definition of "PHR related entity" be modified to read as follows *(Language proposed to be added is underlined)*:

(3) accesses information in a personal health record <u>without authorization</u> or sends information to a personal health record.

Such amendment would ensure that access to an individual's personal health record will be appropriately controlled by the individual. Also, a life insurer only obtains an individual's health information with the individual's authorization.

"Vendor of personal health records"

The definition of "vendor of personal health records," set forth in section 318.2(i) of the Commission's proposed rule also generally tracks the underlying statutory definition set forth in Recovery Act section 13400(18). However, given the lack of clarity with respect to the underlying definition of "personal health record," if the Commission does not modify the definition of "personal health record," as urged above, ACLI again strongly urges the Commission to include in its final interim rule an explanatory note, that contains the language of the Conference Report of the Recovery Act, quoted above, that is applicable to scope of the definition of "vendor or personal health records" as well as to the definition of "personal health record." Again, the language of the Conference Report reflects Congressional intent not to include within the scope of the definition of "personal health record" the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies, and by extension, not to include life insurance companies, and presumably other commercial enterprises, that also maintain records for their own commercial purposes, within the scope of the definition of "vendor of personal health records."

<u>Methods of Notice – Individual Notice</u>

In section 318.5(a)(1) of the Commission's proposed rule, the requirement of "express affirmative consent" as a prerequisite to provision of individual notice by electronic mail appears to go beyond the underlying statutory language of Recovery Act sections 13407(c) and 13402(e)(1), that permit notice by electronic mail "if specified as a preference by the individual." The language of section 318.5(a)(1) could be construed to require special consent to provide notice of a security breach by electronic mail, and therefore a company could not rely on general permission (or consent) provided by the individual for communications from the company to be made by electronic mail.

Accordingly, ACLI urges that the language of section 318.5(a)(1) of the Commission's proposed rule be modified to read in pertinent part as follows *(Language proposed to be added is underlined; language proposed to be deleted is stricken)*:

(1) Written notice by first-class mail to the individual or, if specified as a preference by the individual, ~~provides express affirmative consent,~~ by electronic mail.

With respect to section 318.5(a)(3) of the Commission's proposed rule, there is concern that the references to an individual's "preferred" and "less preferred" methods of notice could be construed to require companies to maintain a list of their customers' preferred methods of notice, again, beyond that which is required under Recovery Act sections 13407(c) and 13402(e)(1)(B). It would be extremely burdensome, if not impossible, for companies to create and maintain a list of such preferences for possibly tens of thousands of policyholders and insureds, without commensurate enhanced consumer benefit.

Accordingly, ACLI urges that the language of section 318.5(a)(3) be modified to read as follows *(Language proposed to be added is underlined; language proposed to be deleted is stricken)*:

(3) If, after making reasonable efforts to contact the individual ~~through his or her preferred form of communication~~ as required under paragraph (a)(1), the vendor of personal health records or PHR related entity finds ~~such preferred form of communication~~ that there is insufficient or out of date contact information that precludes written or, if specified by the individual, electronic notification, the vendor of personal health records or PHR related entity shall attempt to provide the individual with a substitute form of actual notice, which may include ~~written~~ notice by ~~the consumer's less preferred method or~~ telephone.

In section 318.5(a)(4) of the Commission's proposed rule, the threshold for providing substitute notice through conspicuous posting on the business's website or in major print or broadcast media is ten or more individuals. Given this very low threshold, ACLI believes that the alternative of posting notice on the business's website for 6 months is overly long, and urges the Commission to modify this alternative to provide for posting for 3 months.

In section 318.5(a)(4)(ii) of the Commission's proposed rule, the meaning of the phrase "which shall be reasonably calculated to reach the individuals affected by the breach" is unclear, nor is this phrase included in the underlying statutory language of Recovery Act sections 13407(c) or 13402(e)(1)(B). Accordingly, ACLI urges the Commission to delete this phrase.

Recovery Act sections 13407(c) and 13402(e)(1) require written notice by first-class mail to next of kin if the individual is deceased. There is no reference to this requirement in section 318.3(a)(1) of the Commission's proposed rule. However, given the fact this is a statutory requirement under the Recovery Act, ACLI urges that section 318.3(a)(1) of the Commission's proposed rule be modified by adding language to the effect that the requirement to notify next of kin only applies if the vendor of personal health records or the PHR related entity has an address for the next of kin.

Methods of Notice – Notice to the FTC

In section 318.5(c) of the Commission's proposed rule, regarding required notice to the Commission for breaches involving the unsecured PHR identifiable health information of fewer than 500 individuals, "the

vendor of personal health records or PHR related entity may maintain a log of any such breach occurring over the ensuing twelve months and submit the log to the Federal Trade Commission documenting the breaches from the preceding year."

ACLI urges that the language of section 318.5(c) be modified to permit such logs to be maintained on a calendar year basis rather than for the twelve months after a breach. This would not provide less consumer protection, and would impose much less of an administrative burden on businesses. Also, it would be in line with the underlying statutory requirement in Recovery Act sections 13407(c) and 13402(e)(3), that permits such a log to be submitted *annually*.

Effective Date

Notwithstanding the effective date required under Recovery Act section 13407(g), ACLI urges the Commission to provide for an extension of the date for compliance with the Commission's interim final rule, as ACLI urged HHS with respect to its interim final rule. Such an extension would allow businesses subject to the Commission's rule adequate time to take into account the HHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, that will determine what information constitutes "unsecured PHR identifiable information," under section 318.2 (e) of the Commission's rule, and provide time for businesses to make other necessary preparations to comply with the rule.

ACLI also urges the Commission and HHS to provide the same compliance date for both agencies' interim final rules.

ACLI appreciates and thanks the Commission for its consideration of ACLI's views on its proposed Health Breach Notification Rule.

Sincerely,

Roberta B. Meyer

Attachment

cc

U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, DC 20210
Re: HITECH Breach Notification

ACLI
Financial Security. For Life.

Roberta Meyer
Vice President & Associate General Counsel
(202) 624-2184 t (866) 953-4096 f
robbiemeyer@acli.com

May 21, 2009

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

Re: HITECH Breach Notification

Ladies and Gentlemen:

The American Council of Life Insurers ("ACLI") is pleased to provide comments to the Department of Health and Human Services ("Department") in response to its request for comments regarding the guidance and breach notification regulations,[1] required under section 13402 of the Health Information Technology for Economic and Clinical Health ("HITECH") Act of the American Recovery and Reinvestment Act of 2009 ("ARRA").[2] ACLI is the principal trade association of life insurance companies, whose 353 member companies account for 93 percent of the life insurance industry's total assets and 94 percent of the life insurance premiums in the United States. ACLI member companies are also major participants in the long term care insurance, disability income insurance, pension, and reinsurance markets

Many ACLI member companies are long term care insurers, that are "covered entities" under ARRA section 13400(3), subject to the interim final regulations for breach notification, required under ARRA section 13402. Also, ACLI member company life and disability income insurers, that are business associates of long term care insurers or other covered entities, will be subject the interim final regulations for breach notification when ARRA sections 13401 and 13404 are effective on February 17, 2010.

ACLI LEGISLATIVE PRINCIPLES RELATING TO SECURITY BREACH NOTIFICATION

ACLI member companies support the following legislative principles relating to the security of personal information, that provide the basis for ACLI's views regarding the guidance as well as the breach notification regulations. ACLI member companies support legislation that provides uniform preemptive national standards for notification to individuals whose personal information has been subject to a security breach. ACLI member companies also support legislation that avoids needlessly alarming individuals and undermining the significance of notification of a security breach, by requiring notification only when the security and confidentiality of personal information is truly at risk. ACLI member companies believe that legislation should not require

[1] 74 *Fed. Reg.*19006 (April 27, 2009).
[2] American Recovery and Relief Act of 2009, Pub.L. 111-5.

notification if personal information is protected by encryption or some other means that makes the information unreadable or unusable, or if the information is not otherwise likely to be misused.

In light of these principles and the need for a uniform national standard for breach notification, ACLI member companies strongly urge the Department and the Federal Trade Commission ("FTC") to continue to coordinate in the development of the breach notification rules, required under ARRA Sections 13402 and 13407, respectively, so that the rules of both agencies and the resulting consumer protections will be as consistent as possible.

GUIDANCE

ARRA section 13402(a) requires notification of a breaches in the security of "unsecured protected health information." ARRA section 13402(h)(1)(A) provides that " ... the term 'unsecured protected health information' means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2)." ARRA section 13402(h)(2) requires the Secretary to " ... issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Services Act, as added by section 13101 of this Act." In its request for comments, the Department notes that while adherence to the guidance is not required of covered entities and business associates, if the guidance is used, it will " ... create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required by section 13402 in the event of a breach."

In view of the importance of the effective safe harbor to be granted under the guidance, and in response to the Department's request for comments regarding the guidance, ACLI submits the following comments:

Data at Rest

Under guidance section B(a)(i), for an encryption process for data at rest to be valid, it must be " ... consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*" ACLI believes that this standard is overly narrow, more restrictive than necessary, and too tied to a particular technology. First, NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* does not relate to all data at rest. It only addresses data that is maintained in end user devices, and does address other data at rest, such as that maintained in a company data base. Moreover, covered entities and business associates should be permitted the flexibility to use the most effective processes available to protect data at rest. They should not effectively be required to use a particular type of technology or to wait until the guidance is updated to use the most effective technology available. The standard for data at rest should be risk-based, and technology neutral -- so that notification will not be required in connection with breaches of the security of data at rest when there is little likelihood of harm or misuse of the information.

Accordingly, ACLI urges that guidance section B(a)(i) be modified to read as follows *(Language proposed to be added is underlined)*:

(i) Valid encryption processes for data at rest comparable to or consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, used as an example of a valid encryption process for data at rest.

Redacted Data

In response to the question #3, as to whether there are other methods generally the Department should consider for rendering protected health information ("PHI") unusable, unreadable, or indecipherable to unauthorized individuals, ACLI believes that when identifying information has been redacted from PHI maintained on paper, film, or other hard copy media, so that the identifying information cannot be read or reconstructed, the PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals.

Accordingly, ACLI urges the Department to modify the guidance by adding a new section B(c) that reads as follows:

(c) Identifying information has been redacted from PHI maintained on paper, film, or other hard copy media, so that the identifying information cannot be read or reconstructed.

Limited Data Sets

In response to question #5, ACLI does *not* believe the risk of re-identification of a limited data set warrants its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. It generally is very difficult for identifying information removed from a limited data set to be reconstructed.

Accordingly, ACLI urges that limited data sets be added to the guidance's list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Off-the-Shelf Products

In response to question # 7, ACLI strongly believes that future guidance should *not* specify which off-the-shelf products, if any, meet the encryption standards identified in the guidance. As noted above, the guidance should be risk-based and technology neutral, to avoid requiring notices when harm or misuse of the information is unlikely, and to avoid precluding use of the most effective technologies. Given the speed with which new technologies are developed, it would be virtually impossible to keep a list of off-the-shelf products current.

BREACH NOTIFICATION PROVISIONS GENERALLY

In response to the Department's request for "comments concerning any other areas or issues pertinent to the development of its interim final regulations for breach notification," ACLI submits the following:

As indicated above, so that consumer protection in connection with breaches of security of health information will be as consistent as possible, ACLI member companies believe it is very important for the Department and the FTC to continue to take a coordinated approach in the development

of breach notification rules that are as consistent as possible. To that end, ACLI urges the Department to take into account the following comments regarding certain provisions of the proposed FTC breach notification rule ("proposed FTC rule"), published for comment in the *Federal Register* on April 20, 2009,[3] in the development of the Department's interim final regulations:

Definition of "Breach of Security"

Section 318.2(a) of the proposed FTC rule defines "breach of security" as follows:

> Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information with the authorization of the individual. 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 unauthorized acquisition of such information.

The definition appropriately excludes unauthorized access of PHR identifiable health information that is unlikely to result in harm or misuse of PHR identifiable health information. As a result, notification of breaches of security will not be required under the proposed FTC rule if the security of the PHR identifiable health information is not truly at risk, and consumers will not be sent unnecessary notices likely to undermine the significance of breach notification.

ACLI strongly urges the Department to include a similar threshold for notice in the definition of "breach" in its interim final regulations. If the Department uses the definition of "breach," set forth in ARRA section 13400(1) in its regulations, ACLI urges that subsection (1)(A) of the definition be modified to read as follows *(Language proposed to be added is underlined)*:

> (1) BREACH. --
> (A) IN GENERAL. -- The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. <u>Unauthorized acquisition will be presumed not to include unauthorized access to protected health information if the covered entity or business associate that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information.</u>

ACLI submits that the modification proposed above is particularly important given the breadth of the definition of PHI, set forth in ARRA section 13400(12), that incorporates the definition of PHI in 45 C.F.R. section 160.103. Because the definition of PHI underlies the definition of "breach" and the trigger for notice in ARRA section 13402(a), ACLI is concerned that notice will be required in connection with unauthorized acquisition of information, such as a policyholder's name, without a personal identification number or password that would permit access to the

[3] 74 *Fed. Reg.* 17914 (April 20, 2009).

policyholder's file. As a result, it is unlikely that the unauthorized acquisition of such limited information would give rise to harm or misuse. In this regard, the definition of PHI goes beyond the scope of the definition of "personal information," or similar term, that underlies the trigger for notification under many, if not most, state security breach laws.

Methods of Notice -- Individual Notice

In proposed FTC rule section 318.5(a)(1), the requirement of "express affirmative consent" as a prerequisite to provision of individual notice by electronic mail appears to go beyond the underlying statutory language of ARRA sections 13407(c) and 13402(e)(1), that permit notice by electronic mail "if specified as a preference by the individual." The language of section 318.5(a)(1) could be construed to require special consent to provide notice of a security breach by electronic mail, and therefore a company could not rely on general permission (or consent) provided by the individual for communications from the company to be made by electronic mail.

Accordingly, ACLI urges that the language of section 318.5(a)(1) in the proposed FTC rule be modified to read in pertinent part as follows in the Department's interim final regulations *(Language to be added is underlined; language to be deleted is stricken)*:

(1) Written notice by first-class mail to the individual or, if specified as a preference by the individual, ~~provides express affirmative consent,~~ by electronic mail.

With respect to proposed FTC rule section 318.5(a)(3), there is concern that the references to an individual's "preferred" and "less preferred" methods of notice could be construed to require companies to maintain a list of their customers' preferred methods of notice, again, beyond that which is required under ARRA sections 130407 and 13402(e)(1)(B). It would be extremely burdensome, if not impossible, for companies to create and maintain a list of such preferences for possibly tens of thousands of policyholders and insureds, without commensurate enhanced consumer benefit.

Accordingly, ACLI urges that the language of section 318.5(a)(3) in the proposed FTC rule be modified to read as follows in the Department's interim final regulations *(Language to be added is underlined; language to be deleted is stricken)*:

(3) If, after making reasonable efforts to contact the individual ~~through his or her preferred form of communication~~ as required under paragraph (a)(1), the covered entity ~~vendor of personal health records or PHR related entity~~ finds that there is insufficient or out of date contact information that precludes written or, if specified by the individual, electronic notification, the covered entity ~~vendor of personal health records or PHR related entity~~ shall attempt to provide the individual with a substitute form of actual notice, which may include ~~written~~ notice by ~~the consumer's less preferred method or~~ telephone.

In proposed FTC rule section 318.5(a)(4), the threshold for providing substitute notice through conspicuous posting on the business's website or in major print or broadcast media is ten or more individuals. Given this very low threshold, ACLI believes that the alternative of posting notice on the business's website for 6 months is overly long, and urges that, in the Department's interim final regulations, this alternative be modified to provide for posting for 3 months.

In FTC proposed rule section 318.5(a)(4)(ii), the meaning of the phrase "which shall be reasonably calculated to reach the individuals affected by the breach" is unclear, nor is this phrase included in the underlying statutory language of ARRA section 13402(e)(1)(B). Accordingly, ACLI urges that this phrase not be included in the corresponding provision in the Department's interim final regulations.

ARRA Section 13402(e)(1) requires written notice by first-class mail to next of kin if the individual is deceased. There is no corresponding provision in section 318.3(a)(1) of the proposed FTC rule. However, given the fact this is a statutory requirement under ARRA section 13402(e), ACLI urges the Department to include language in the regulation that corresponds to this section of the bill to the effect that the requirement to notify next of kin only applies if the covered entity has an address for the next of kin.

Methods of Notice -- Notice to the FTC

In section 318.5(c) of the proposed FTC rule, regarding required notice to the FTC for breaches involving the unsecured PHR identifiable health information of fewer than 500 individuals, "the vendor of personal health records or PHR related entity may maintain a log of any such breach occurring over the ensuing twelve months and submit the log to the Federal Trade Commission documenting the breaches from the preceding year."

ACLI urges that the language of section 318.5(c) in the proposed FTC rule be modified for use in the Department's interim final regulations to permit such logs to be maintained on a calendar year basis rather than for the twelve months after a breach. This would not provide less consumer protection, and would impose much less of an administrative burden on businesses. Also, it would be in line the underlying statutory requirement in ARRA section 13402(e)(3), that permits the covered entity to *annually* submit a log to the Secretary that documents the breaches involving less than 500 individuals that occurred during that year.

Effective Date

Notwithstanding the effective date required under ARRA section 13402(j), ACLI urges the Department to provide for an extension of the date for compliance with the interim final regulations to allow covered entities and business associates adequate time to take the guidance into account and to make other necessary preparations to comply with the regulations.

ACLI appreciates and thanks the Department for its consideration of ACLI's views on its guidance and the interim final regulations.

Sincerely,

Roberta B. Meyer