NAMIC®

NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

June 1, 2009

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Health Breach Notification, Rulemaking, Project No. R911002

Dear Sir/Madam:

The National Association of Mutual Insurance Companies ("NAMIC") is pleased to offer comments on proposed rules requiring vendors of personal health records and related entities to notify individuals when the security of their individually identifiable health information is breached for purposes of Section 13407(g)(1) of the American Recovery and Reinvestment Act of 2009 ("ARRA"). [1]

NAMIC is the largest full-service national trade association serving the property/casualty insurance industry with more than 1,400 member companies that underwrite more than 40 percent of the property/casualty insurance premium in the United States. NAMIC members are small farm mutual companies, state and regional insurance companies, risk retention groups, national writers, reinsurance companies, and international insurance giants.

NAMIC appreciates the opportunity to offer comments on the breach notification provisions relative to the issuance by the Federal Trade Commission ("Commission") of the Health Breach Notification Rule ("Rule"). That Rule addresses notification

[1] Public Law 111-005, February 17, 2009

requirements in the event of a breach of the security of information held by vendors of personal health records, personal health record ("PHR") related entities, and third party service providers, without regard to whether such entities fall within the FTC's enforcement jurisdiction. This guidance is critical for our member companies to determine under what circumstances breach notification is required

Background

Section 13407(g)(1) of the ARRA requires the Commission to promulgate, within 180 days of enactment, temporary regulations requiring covered entities to notify consumers when the security of their health information is breached. In addition, the Commission, in coordination with the Department of Health and Human Services ("HHS"), is directed to conduct a study and report on potential privacy, security, and breach notification requirements for vendors of personal health records and related entities.

The Commission, on April 20, 2009, issued temporary guidance and requested public comment. [2] The guidance requires vendors of personal health records and related entities to provide notice to consumers and the Commission following a breach. The proposed rule contains additional requirements governing the standard for what triggers the notice, as well as the timing, method, and content of the notice. It also requires covered entities to notify the Commission of any breaches applicable to its regulated entities. The Rule applies to breaches of security discovered on or after September 18, 2009.

The legislative history is clear that lawmakers do not intend to include life and property/casualty insurers as vendors of personal health records. As such, NAMIC believes that the Commission's expanded jurisdiction does not extend to insurers maintaining or accessing personal health records managed by or primarily for commercial enterprises. Notwithstanding our position that the proposed Rule does not apply to insurers in possession of personal health records created or managed primarily for commercial uses, NAMIC offers language we believe is needed to clarify the scope of the Rule to avoid unintended application. Specifically, NAMIC offers recommendations with respect to key definitions set forth in the guidance to prevent inadvertent application of the Rule to property/casualty insurers. NAMIC appreciates the opportunity to comment on the various definitions and notice provisions of the Rule.

[2] 74 Fed. Reg. 17914-17925

Definitions

Section 318.2 of the proposed guidance sets forth a series of definitions. The definitions of relative terms are important to NAMIC members and we offer comments on the proposed definitions of several specific terms.

§318.2(a) - Breach of Security

The proposed regulations define breach of security, with respect to unsecured PHR identifiable health information of an individual in a personal health record, as an "acquisition of such information without the authorization of the individual." The first part of the definition follows the definition of ARRA. The Rule expands the definition by adding language to provide 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 unauthorized acquisition of such information."

The Commission correctly recognizes that the entity that experiences the breach is in the best position to determine whether in fact an unauthorized acquisition has taken place. The proposed rule creates a rebuttable presumption that the information has been acquired. Thus, 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. NAMIC commends the Commission for recognizing that access to information does not necessarily imply that protected information has in fact been obtained. We encourage the Commission to retain the rebuttable presumption provisions.

§318.2 (d) Personal Health Record

The Rule defines PHR as "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." The definition of PHR is overly broad and NAMIC is concerned that without further clarification could be interpreted to apply to a host of situations outside the scope of the legislative intent.

The Conference Report to accompany the ARRA directly addresses the issue of the definition of PHR. The conference report clarifies the statutory definition of PHR. The statute defines covered records as those "controlled by or primarily for the individual." The conference report clearly separates "individual" records from commercial use records and excludes those records "managed by or primarily for commercial enterprises" from the definition of PHR. As an example of commercially managed records, the conference report cites records maintained by life insurance companies for their own business purposes and notes that as such the insurer would not be considered a PHR vendor. [3] NAMIC believes the same rationale is true for property/casualty insurers which maintain health information records for their commercial use.

The Commission itself acknowledges the limited set of covered entities to which the Rule should apply. In its submission to the Office of Management and Budget in compliance with the Paperwork Reduction Act, the Commission estimates that 200 vendors of PHR and 500 PHR related entities will be covered by the rules, along with an additional 200 third-party services providers. Clearly the Commission did not envision ensnaring the thousands of insurers, both life and property/casualty, holding PHR for commercial uses into the definitions of covered entities. We urge the Commission to clarify the definition of PHR to give full force and effect of law to the congressional intent to exclude legitimate commercial use by insurers from the definition of PHR.

§318.2 (i) Vendor of personal health records

The proposed regulations define vendor of personal health records as "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record." NAMIC is similarly concerned that the definition of vendor of personal health records as defined will lead to confusion and could inadvertently undermine congressional intent and include insurers that maintain records for commercial use. NAMIC recommends that the definition of vendor of personal health information be amended to read as follows:

> Vendor of health information means an entity, other than a covered entity, that offers to or maintains for a covered entity a personal health record.

[3] H.R. Conf. Rep. No. 111-16. at 497 (2009)

As previously noted the Conference Reports makes clear that Congress did not intend for insurers maintaining PHRs for commercial use to be included in the definition of vendor of personal health records. Similarly, the Commission anticipates a limited number of covered entities. The estimate of covered entities would imply a clearly delineated definition of vendor and PHR. NAMIC urges the Commission to avoid overly broad definitions that could inappropriately sweep thousands of property/casualty insurers into the regulatory regime.

Breach Notification

Title XIII of the ARRA establishes the "Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). Section 13402 creates new federal breach notification requirements. Vendors of personal health records and PHR related entities are required to notify affected individuals of a breach of their personal health information within 60 days following the discovery of a breach.

Individual Notices

Section 13402(e)(1)(A) of the ARRA requires covered entities in the event of a breach to provide "written notification by first-class mail" or "if specified as a preference by the individual, by electronic mail." Section 318.5(a)(1) proscribes requirements for written notification and electronic notification as a preference of the individual. Section 318.5(a)(3) provides for notification by the "consumer's less preferred method" if after making reasonable efforts to contact the individual utilizing the preferred method, the covered entity find the methods is inefficient or out-of-date

The regulations imply that covered entities could be required to maintain a listing of individual preferences in terms of delivery methods with respect to breach notifications. The regulations imply that covered entities could be required to maintain a listing of individual preferences in terms of delivery methods with respect to breach notifications. A regulatory requirement to offer alternative communication methods and maintain a database of consumer preferences would impose a substantial, costly and unwieldy burden on covered entities. NAMIC urges the Commission to provide flexibility in notification by amending Section 318.5(a)(3) as follows:

> (3) If, after making reasonable efforts in accordance with paragraph (a)(1), the vendor of personal health records or PHR related entity finds that its contact information is out-of-date, 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 notice by telephone.

Web Posting

Section 13402(e)(1)(B) requires that in the case of 10 or more individuals for which there is insufficient or out-of-date contact information, covered entities conspicuously post notice of the breach on the home page of the entity's web site or publish the notice in major print or broadcast media. The Rule expands the notification requirement to include a six-month timeframe. The Commission believes that six months is an appropriate time period for posting of the notice to ensure that individuals who intermittently check their accounts obtain notice and asserts that the requirement is not unduly burdensome.. NAMIC disagrees with the Commission's assertion that such a requirement would not be unduly burdensome for businesses. The six month requirement is an arbitrary timeframe that could interfere with businesses efforts to update web sites and/or to highlight other important consumer information. NAMIC urges the Commission to remove the six-month posting requirement and to permit covered entities to determine the appropriate posting timeframe based on the extent and severity of the breach.

Media Notice

Section 13402(e)(2) of the ARRA requires covered entities to provide notice to prominent media outlets serving a State or jurisdiction if the protected health information of more than 500 residents has been accessed, acquired or disclosed. The Rule at Section 318.5(b) appropriately limits the media notification to instances in which the information of more than 500 residents has been acquired in a security breach. NAMIC appreciates the Commission's recognition that notices should be limited to situations in which personal health information has been acquired. The statute and Rule provide for notification of media outlets serving a State or "jurisdiction." It is unreasonable to expect entities to notify all major U.S. media outlets simply because one or more individuals affected by the breach live in such jurisdictions. NAMIC recommends that the Commission define "jurisdiction" as the District of Columbia and any U.S. territory or possession. Such a definition would clarify that the term jurisdiction is not meant to include broad geographical regions encompassing more than one state.

Notice to Government

Section 13402(e)(3) of ARRA requires that in the case of breaches affecting information of more than 500 individuals that covered entities provide notice to the federal government. In the case of breaches impacting less than 500 individuals, covered entities would be directed to submit an annual log to the federal government documenting the breaches. The Rule in Section 318.5(c) provides that notification be given to the Commission "as soon as possible and in no case later than five business days following the date of discovery of the breach." The Rule further provides that logs of breaches be maintained for a twelve month period and that logs submitted to the Commission should document all breaches for the preceding year. Under the Rule, covered entities would submit logs to the Commission one year from the date of the entity's first breach. NAMIC agrees with the Commission's assertion that providing a date for submission of logs will simplify compliance, but believes that submission dates based on calendar years would provide greater simplification. Rolling compliance dates based on an entity's first breach will needlessly complicate the compliance requirements. This is particularly true for consolidated entities.

NAMIC urges the Commission to require the submission of logs only in years in which a covered entity has experienced a breach and to require entities to maintain and submit logs on a calendar year basis

Conflicting Breach Notification Standards

The Commission invites comments on the overlap of the Rule with other federal statutes, rule or policies. NAMIC encourages the Commission to coordinate the Rule with the requirements of the HHS rules governing breach notification for HIPAA-covered entities. NAMIC submitted comments to the HHS on various aspects of the regulations, including data security standards and is including these comments as an attachment to our comments. NAMIC likewise encourages the Commission to harmonize notification requirements with state breach notification laws.

For a number of years individuals and businesses handling personal health information have been subject to various state breach notification laws. On the state level, 45 breach statutes apply addressing breach of personally identifiable information--- primarily to address identity theft and protect consumers from financial and other elements of personal risk. These laws, in general, address the unauthorized acquisition of and access to unencrypted sensitive, personal information. Many NAMIC member

companies operate on a national or multi-state basis and are responsible for complying with federal and state law requirements.

California and Arkansas currently require notification in the event of a compromise of health information data security under their "breach laws." The vast majority of state laws, however, look to the electronic computerized records of personally identifiable and "sensitive" information. This new federal law establishes a national standard that would require notification regardless of how records of personally identifiable health information are stored—electronic, paper or other media. The differences between state and federal laws requiring notification following a data breach, as well as variances in federal and state safe harbor standards, raise concerns for NAMIC members. The conflict between the federal and state standard could create difficulties for covered entities and consumers.

NAMIC supports the goals of the Commission in providing guidance regarding of when a breach notification should be issued under the HITECH Act. We urge the Commission to work with state insurance functional regulators to harmonize the form of breach notification so as to avoid multiplicative, inconsistent and confusing notifications that would add unnecessary cost and confuse consumers. Our member companies look forward to working with the Commission to improve the breach notification process in order to protect their customers, as well as making that process workable.

Conclusion

Our nation's property/casualty industry is fully committed to protecting policyholder and claimant privacy and maintaining the security of their personal information. Our member companies remain concerned about how this new guidance may impact the notification obligations of property/casualty insurers.

NAMIC believes the legislative history of the statute clearly defines personal health records to exclude records created and held for commercial activities, such as those created and used by life and property/casualty insurers. As such, insurers should be excluded from the definition of vendor.

NAMIC supports the harm standard as set forth in FTC Proposed section 318.2, which allows the presumption of unauthorized acquisition of protected information to be rebutted with reliable evidence showing that the information could not reasonably have been acquired.

We look forward to working with the Commission to establish appropriate notification requirements covering personal health records managed, shared, and controlled by or primarily for an individual and appropriately excluding commercial use records.

Sincerely,

National Association of Mutual Insurance Companies
122 C Street, N.W.
Suite 540
Washington, D.C. 20001
202-628-1558

NAMIC®

NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

May 21, 2009

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

RE: 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 Sir/Madam:

The National Association of Mutual Insurance Companies ("NAMIC") is pleased to offer comments on 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 – "HITECH ACT") of the American Recovery and Reinvestment Act of 2009. [1]

NAMIC is the largest full-service national trade association serving the property/casualty insurance industry with more than 1,400 member companies that underwrite more than 40 percent of the property/casualty insurance premium in the United States. NAMIC

[1] Public Law 111-005, February 17, 2009

members are small farm mutual companies, state and regional insurance companies, risk retention groups, national writers, reinsurance companies, and international insurance giants.

NAMIC appreciates the opportunity to offer comments on the breach notification provisions relative to the issuance by the Secretary of Health and Human Services ("HHS") of information security guidance ("guidance"). That guidance addresses safeguards which, if implemented, render protected health information ("PHI") and personal health records ("PHR") unusable, unreadable or indecipherable to unauthorized individuals. This guidance is critical for our member companies to determine under what circumstances breach notification is required.

Background

The American Recovery and Reinvestment Act of 2009 was enacted on February 17, 2009. Title XII of Division A and Title IV of Division B, the HITECH Act, at Section 13402(b) defines "unsecured protected health information" to mean protected health information that is not secured through the use of a technology or methodology identified by the Secretary of HHS in connection with guidance to be issued no later than 60 days after enactment. The aforesaid guidance is to specify the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized persons. The HITECH Act further required guidance to be issued by HHS defining whether personally identifiable health information would be considered "secured" and when unauthorized access should be subject to the new federal breach law notification process.

The Secretary issued guidance and requested comment on April 27, 2009. [2] The guidance relates to two forthcoming breach notification regulations – guidance issued by HHS for covered entities and their business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Sec. 13402 of HITECH) and guidance to be issued by the Federal Trade Commission (FTC) for vendors of personal health records and other non-HIPAA covered entities (Sec. 13407 of HITECH).

Covered entities that apply the technologies and methodologies specified in the guidance will not be required to provide the notifications required by the regulations in the event the information is breached. As such the guidance is particularly important to NAMIC members.

[2] 74 Fed. Reg. 19006-19010

The HITECH Act requires guidance to be issued by HHS in defining whether personally identifiable health information would be considered "secured" and when unauthorized access should be subject to the new federal breach law notification process. HHS in its guidance has outlined two means of securing PHI and PHR - encryption and destruction.

Encryption

The guidance provides that PHI and PHR will be considered unusable, unreadable or indecipherable if the information has been encrypted.

Under most state laws, the term "encrypted" has not been defined. But those states that have commented upon a security approach have included the following elements of encryption:

- Any recognized algorithmic process to transform data into a form in which the data is unreadable or unusable without the use of a confidential process or key;
- Any protective or disruptive measure, including, cryptography, enciphering, encoding or computer containment that is designed to (a) impede, delay or disrupt the personal information; (b) make the information unusable or unintelligible; or (c) prevent, impede or disrupt any device on which the information is stored.

Such definitions afford the requisite flexibility which is essential in today's business environment.

The guidance attempts to more directly define encryption. Encrypted data is defined in the guidance to include electronic PHI which has been encrypted as specified in the HIPAA Security Rule. The HIPAA Security Rule defines "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 the use of a confidential process or key." [3] The guidance further provides that encryption processes for data at rest should be *consistent* with National Institute of Standards Technology ("NIST") Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.* [4] For data in motion, valid

[3] 45 CFR 164.304, definition of "encryption."
[4] http://www.csrc.nist.gov/.

encryption processes are defined as those that *comply* with the requirements of Federal Information Processing Standards (FIPS) 140-2. [5]

NAMIC is pleased HHS recognizes the current HIPAA Security Rule definition of encryption. This definition should be preserved. The flexible definitions or standards for encryption provided by the HIPAA Security Rule and state laws have served the business community and consumers well thus far. Accordingly, there is no need to "raise the bar" to a difficult, if not impossible standard (from a practical standpoint) to meet. The guidance, NAMIC believes, should continue to embrace this high level definition of encryption because this standard is both achievable and an evolving standard.

With respect to the references to NIST Publication 800-111, NAMIC urges that the *consistency* benchmark be interpreted as an example. Consistency should be considered in the context of a general reference to the HIPAA "algorithmic process" and Publication 800-111 not be viewed as a limiting or proscriptive standard. In order to preserve the needed flexibility, as to the use of encryption, NAMIC specifically recommends references to data at rest be amended to include provision for "a comparable alternative standard and/or industry best practices."

Similarly as to the example of the FIPS 140-2 for data in transit, such standard should not require literal adherence, but should be recognized as an example of a reasonable process following the general "algorithmic process" standard of the HIPAA Rule as a means of achieving information security. NAMIC urges that HHS amend the reference to *compliance* with FIPS 140-2 and replace with language providing recognition of "valid encryption processes for data in motion *consistent* with the requirements of Federal Information Processing Standard, (FIPS) 140-2, a comparable alternative standard and/or industry best practices."

In addition, we recommend that HHS add a third definition as subsection (a) (iii), to provide that: "Valid encryption processes for either data at rest or data in motion also include the use of any other recognized algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key."

---

[5] These include, as appropriate, standards described in NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated; http://www.csrc.nist.gov/.

The definitions and standards established by HHS should be written to permit compliance within the context of an ever evolving technology platform. The standards outlined in Special Standard 800-111and Process Standard 140-2 should not be preclusive of other technologies or innovations in securing information.

The HIPAA Security Rule and state breach law "elements" of encryption have served the consumer and business community well. NAMIC believes there is no need to mandate a level not achievable by all or most of our member companies.

Destruction

The second category of security relates to the destruction of information. The guidance provides that PHI will be deemed to have been rendered unusable, unreadable, or indecipherable to unauthorized individuals if the information has been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization,* such that the PHI cannot be retrieved. [6]

As with encryption, NAMIC urges HHS to provide entities with flexibility. NIST Special Publication 800-88 is a reasonable standard for purging electronic media. However, this publication should be used an example and not the only means of attaining a safe harbor in securing PHI or PHR by destruction. NAMIC urges HHS to preserve the consistency standard and to recognize comparable alternative standards and industry best practices. Comparable alternative standards should be available for use and industry current best practice should also be recognized in terms of encryption and destruction of personally identifiable information. The recognition of comparable alternative standards and industry best practices are essential in the rapidly evolving world of technology. Federal standards must be flexible enough to keep pace with technological and business process developments.

[6] http://www.csrc.nist.gov/.

Other Technologies and Methodologies

HHS seeks comments on new technologies and methodologies. As previously noted, NAMIC believes it is essential that HHS develop definitions and standards that are flexible and dynamic enough to permit improvements and innovations in data security and protection. In addition, NAMIC urges HHS to specifically include provisions for redaction and data masking.

Although electronic collection, storage, maintenance, and sharing of information are encouraged, HHS must recognize that in certain instances PHI and PHR may be maintained in paper form. For health information maintained in paper form, we believe that proper redaction should be recognized as an acceptable method of rendering the information unusable, unreadable, or indecipherable to unauthorized individuals.

Similarly, NAMIC believes that data masking and two-factor authentication should be considered as effective security standards. Data masking – cloning mechanisms that replace true data with false data – significantly reduces the risk posed by data breaches. Two-factor authentication, such as combinations of multiple passwords or passwords and biometric identifiers, likewise should be considered an effective security standard.

Breach Notification

NAMIC commends HHS for requesting public comment on the breach notification provisions of the HITECH Act in anticipation of future rulemaking.

For a number of years individuals and businesses handling PHI have been subject to various state breach notification laws. These laws, in general, address the unauthorized acquisition of and access to unencrypted sensitive, personal information. Many NAMIC member companies operate on a national or multi-state basis and are responsible for complying with federal and state law requirements.

Section 13402 of the HITECH Act establishes federal breach notification requirements. Under the act, notification to affected individuals is required within 60 days following the discovery of a breach. On the state level, 45 breach statutes apply addressing breach of personally identifiable information--- primarily to address identity theft and protect consumers from financial and other elements of personal risk.

California and Arkansas currently require notification in the event of a compromise of health information data security under their “breach laws.” The vast majority of state

laws, however, look to the electronic computerized records of personally identifiable and "sensitive" information. This new federal law establishes a national standard that would require notification regardless of how records of personally identifiable health information are stored—electronically, paper or other media. The differences between state and federal laws requiring notification following a data breach, as well as variances in federal and state safe harbor standards, raise concerns for NAMIC members. As example, New Jersey law requires entities to report any breach to the security Division of State Police and receive clearance from the agency prior to notification. [7] The conflict between the federal and state standard could create difficulties for covered entities and consumers.

In evaluating breaches, NAMIC urges HHS to adopt a "harm standard." The guidance should give deference to the covered entity's determination of the state of the data at the time of the breach and whether an actual unauthorized acquisition has taken place. NAMIC recommends that HHS follow the lead of the Federal Trade Commission ("FTC") and recognize that access to information does not necessarily imply that protected information has in fact been obtained. The FTC appropriately recognizes that the entity that experiences the breach is in the best position to determine whether an unauthorized acquisition has taken place. As such, the definition of breach creates a presumption that unauthorized persons have acquired information if they have access to it, this presumption can be rebutted with reliable evidence showing that "there has not been, or could not reasonably have been, any unauthorized acquisition of such information." [8]

NAMIC supports the goals of HHS in providing a workable security standard and safe harbor for guidance in terms of when a breach notification should be issued under the HITECH Act. We urge that HHS work with state insurance functional regulators to harmonize the form of breach notification so as to avoid multiplicative, inconsistent and confusing notifications that would add unnecessary cost and confuse consumers. Our member companies look forward to working with HHS to improve the security and breach notification process in order to protect the insurance customers of our member companies as well as making that process workable for our member companies.

[7] N.J.S.A. §§56:8-163.
[8] Federal Trade Commission proposed regulations implementing the American Recovery and Reinvestment Act of 2009; Health Breach Notification Rulemaking; 74 Fed. Reg. 17914, 17915 (April 20, 2009)

Safe Harbor Protection

Under the guidance, if at the time of any breach an entity's data security meets the protection standards outlined by HHS, a safe harbor applies and the notification requirements will not be triggered. NAMIC reminds HHS of the importance of such safe harbor protection for entities following appropriate and workable standards.

The proposed guidance indicates that the outline of information safeguards is intended to be exhaustive. But we would urge that comparable technologies and safeguards if used should "create the functional equivalent of a safe harbor" with respect to the notification obligations of the HITECH Act.

The sanctioned technologies and methodologies which render PHI unusable, unreadable, or indecipherable to unauthorized individuals are extremely important. If PHI is deemed secured by one of the authorized means, the breach notification requirements are inapplicable. In essence, the use or implementation of one of the authorized technologies or methodologies provides the all important "safe harbor" for individuals and businesses subject to the Act. We strongly believe reasonable security guidance and a meaningful safe harbor approach are needed to avoid unnecessary and overly broad notification. The absence of such guidance will result in costly notifications, which needlessly confuse consumers and customers and render the breach notification process redundant and trivial.

Conclusion

Our nation's property/casualty industry is fully committed to protecting policyholder and claimant privacy and maintaining the security of their personal information. Our member companies remain concerned about how this new guidance for security measures impacts not only PHI, but also PHR; especially to the extent PHR may impact the notification obligations of property/casualty insurers.

NAMIC fully supports the efforts of HHS to encourage the protection of PHI through the use of encryption and encourages HHS to define encryption broadly enough to encompass baseline industry standards and best practices, and allow for technological advances. Raising the bar beyond anyone's practical reach is not warranted and it effectively serves to eliminate the needed flexibility. NAMIC reiterates the importance of the safe harbor and encourages HHS to follow the lead of the Federal Trade Commission and adopt a harm standard as set forth in FTC Proposed section 318.2, which allows the presumption of unauthorized acquisition of protected information to be

rebutted with reliable evidence showing that the information could not reasonably have been acquired.

We look forward to working with HHS to establish appropriate security standards which serve to render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Sincerely,

National Association of Mutual Insurance Companies
122 C Street, N.W.
Suite 540
Washington, D.C. 20001
202-628-1558