National Association for Information Destruction, Inc.
3420 East Shea Blvd., Suite 115, Phoenix, Arizona 85028
Phone: (602) 788-6243 Facsimile: (602) 788-4144
Email: exedir@naidonline.org Website: www.naidonline.org

May 31, 2009

BY ELECTRONIC FILING

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

To the Commission:

The National Association for Information Destruction, Inc. ("NAID") submits these comments on the Federal Trade Commission's ("FTC" or "Commission") proposed rule requiring notification when the security of personal health records has been breached.[1] The National Association for Information Destruction, Inc. ("NAID") is the international, non-profit trade association of the information destruction industry. NAID's members include individuals as well as large and small businesses that provide information destruction services. NAID and its members are expert in, and committed to, the proper destruction of both paper records and computerized data containing sensitive personal information that could be misused. NAID's mission is to champion the responsible destruction of confidential information and materials by promoting the highest standards and ethics in the industry.

Introduction

Advances in health information technology provide the potential for improving the delivery of health care while reducing associated costs. An important aspect of such developments are services that enable the creation of personal health records ("PHRs"). PHRs will allow patients to provide their doctors with valuable information that can help improve the quality of care they receive. A PHR can also help reduce or eliminate duplicate medical tests and allow patients to receive faster, safer treatment and care in case of an emergency. Yet, PHR developments and acceptance will be thwarted if the privacy and security of PHRs is not protected and if subjects of PHRs are not notified when there has been a breach of their PHR.

[1] 74 Fed. Reg. 17914 (April 20, 2009).

NAID commends the FTC for promptly proposing rules to notify patients when their PHRs may have been compromised. The following are a few suggested revisions to the proposed rule.

Breach of Security

A critical issue in the proposed regulations is setting the appropriate trigger for when breach notification will be required. In general, NAID supports the proposed definition found in Section 318.2(a),[2] as it addresses situations in which PHRs have been acquired as well as situations in which it is known that there has been access to PHRs, along with a presumption in the latter case that PHRs have been acquired unless the presumption can be rebutted by a showing that the PHRs were not or could not have been acquired.

However, the examples provided in the preamble and proposed rule do not address the all too common situation in which PHRs *may* have been accessed. For instance, a PHR-related entity may discover that for 3 months PHR information was posted through an obscure link on its website. If web logs were not maintained, it could not be established whether or not anyone had either accessed or "acquired" the information. Yet, a risk existed that potentially highly sensitive PHRs were accessed and acquired. The rebuttable presumption of acquisition should clearly be applied in these cases as well. In other words, where information could have been accessed, the rebuttable presumption should be that it was. Of course, in this example, if the entity had maintained web logs and could determine that no one had clicked on the link, the presumption of acquisition would be rebutted and no breach notification would be required.

Another scenario in which this potential unauthorized exposure of PHR could occur would be computer hard drives or other electronic storage media that had been being unsecurely discarded for several months in a manner that would permit unauthorized access and acquisition to stored information. Again, it might be impossible to determine if anyone had accessed or acquired the information, but individuals whose PHRs were on the hard drives or other media were certainly at risk of unauthorized acquisition of their information. There is no reason they should not be notified that they are at risk unless it could be shown that the information was never read.

Both of these examples are substantially similar to the unexplained loss of unencrypted computer tapes, wherein there is the possibility that personal information could have been improperly accessed. Such events put personal information at risk and have frequently resulted in notification events under state data security breach laws.

---

[2] Proposed Section 318.2(a) states:

> 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.

Failure to impose a notification duty under these circumstances would also unfairly reward companies that permitted systems vulnerabilities and yet did not adopt sufficient intrusion detection and tracking to permit them to determine when improper access had taken place and what information was accessed. Accordingly, to create the proper incentives to protect PHRs, and properly dispose of PHRs, NAID proposes the definition of breach be modified 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 (including disposal of such information without its having been rendered unusable, unreadable or indecipherable) 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

Following the definition in the American Recovery and Reinvestment Act of 2009[3] which directed the FTC to promulgate these breach notification rules, the proposed definition of "personal health record"[4] references *electronic* health records. In the preamble to the proposed rule, the Commission recognizes that there may be covered unauthorized access to not only electronic versions of PHRs, but also that the "the theft of *hard copies* of such records"[5] would also constitute a triggering breach. It would not make sense to protect sensitive health records only when in electronic form while permitting a provider of PHR services to print those same records but not accord the same level of protection to the printed versions. However, it may not be clear that the proposed definition of "personal health record" applies to printed versions of electronic records. Thus, for purposes of clarity, NAID proposes that the definition be revised to make clear that printed hard copies of electronic records are covered:

> *Personal health record* means an electronic record of PHR identifiable health information, or a copy of such information in any medium, on an individual that

[3] Pub. L. 111-5.

[4] Proposed Section 318(d) states:

> *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.

[5] 74 Fed. Reg. at 17915 (emphasis added).

can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

Third Party Service Provider Notice Obligations

The proposed rule requires third party service providers to provide notice to PHR vendors following discovery of a breach. A breach is treated as "discovered as of the first day on which such breach is known to a . . . service provider . . . or should reasonably have been known . . . to have occurred."[6] While a determination of whether a breach has occurred may seem to be a simple matter, in fact it can often require an extensive investigation, interviews, review of audit trails and videotapes, forensic computer examination, and many other steps. Diligent efforts to determine whether or not a breach has occurred may take days or more. The proposed standard of when a "breach is known" does not clearly capture this challenge and complexity.

Accordingly, NAID recommends that the timing of when a breach is known be clarified to take into account the need in many cases to conduct an investigation:

> *Breaches treated as discovered.* A breach of security shall be treated as discovered as of the first day on which, following a reasonable investigation if necessary, such breach is known to a vendor of personal health records, PHR related entity, or third party service provider, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider, respectively) or should reasonably have been known to such vendor of personal health records, PHR related entity, or third party service provider (or person) to have occurred.

* * * * *

Again, we commend the Commission's efforts to encourage the safe and secure development of PHRs by mandating notification of breaches to the subjects of those PHRs. We respectfully request that the FTC consider our proposed clarifications and modifications, which we believe will further serve the laudable goal of protecting the privacy and security of sensitive health information.

Respectfully submitted,

Robert Johnson, Executive Director

[6] Section 318.3(c).