SPAN
35 Halsey Street 4th Floor
Newark, NJ 07102
(973) 642-8100
(973) 642-8080 – Fax
E-Mail address: Hspan@spannj.org
Website: Hwww.spannj.orgH

Statewide Parent Advocacy Network, Inc.

Empowered Families: Educated, Engaged, Effective!

Family Voices-NJ Comments on the FTC Health Breach Notification Rule 5/26/09

Thank you for the opportunity to comment on the Federal Trade Commission proposed rule on Health Breach Notifications. Family Voices is a national network that advocates on behalf of children with special healthcare needs and our NJ Chapter is housed at the Statewide Parent Advocacy Network (SPAN), New Jersey's federally funded Parent Training and Information Center which is also NJ's Family-to-Family Health Information Center and a chapter of the Federation of Families for Children's Mental Health. The Family Voices Coordinator also serves as the NJ Caregiver Community Action Network representative for National Family Caregivers Association in a volunteer capacity.

We strongly support the stipulations in the ARRA (American Recovery and Reinvestment Act) which strengthen privacy and protections of health information. The proposed interim rules are a step in this direction regarding HIPPA covered entities such as hospitals, physicians' offices, and health insurance plans as well FTC regulated entities that engage in activities as business associates of HIPPA covered entities. We strongly support the FTC consultation with HHS for consistency between the proposed rules.

Section 318.1 Purpose and scope

Relevant Statutory Authority

We agree that under ARRA, the FTC "must issue rules requiring vendors of personal health records and related entities to notify individuals when the security of their individually identifiable health information is breached." We support this additional protection in keeping with the spirit of the HIPAA law.

Covered Entities

We agree that this rule covers entities beyond FTC's traditional jurisdiction such as "vendors of personal health records and online applications that interact with such personal health records." It would also apply to "non-profit entities that offer personal health records or related products and services, as well as non-profit third party service providers." Clarification is needed on vendors who serve in a dual role "as a business associate of a HIPAA-covered entity and a direct provider of personal health records to the public". Consumers would be concerned if they received multiple notices, or a notice from an "unexpected entity." We urge consideration of this factor and a plan to address it.

Clarification of HIPPA
We agree with the clarification that this does not apply to HIPAA covered entities or activities as a business associate of a HIPAA covered entity. We would urge the FTC to align the regulations with HIPAA for uniformity.

Section 318.2 Definitions

Breach of security
We agree that the definition should be the acquisition on information "without the authorization of the individual." Examples include theft of a laptop, hard copies, and downloading/transferring files, and hacking. We support the distinction between access and acquisition and the example is given of an employee inadvertently accessing and immediately exiting a database in error. We agree that the entity that experienced the breach can determine whether unauthorized acquisition has occurred, but are concerned that there may be a financial disincentive to disclose. For example, a forensic analysis of a recovered laptop can reveal "that files were never opened, altered, transferred, or otherwise compromised."

Business Associate
We agree that the definition means an associate under HIPAA which includes those that provide "certain functions or activities on behalf of a HIPAA-covered entity or…legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services".

HIPPA-covered entity
We agree with using the HIPAA definition which includes health care provider, health care clearinghouse (data processing), and health plans.

Personal Health Record and *PHR identifiable health information*
We agree that the PHR is defined as an electronic record of PHR identifiable health information on an individual, but urge that you broaden this definition to include hard copies as well. We agree that the PHR individually identifiable health information is from a "health care provider, health plan, employer, or health care clearinghouse…past, present or future physical or mental health or condition of an individual…" We were pleased to see the recognition of the importance of confidentiality particularly as it relates to mental health and would suggest the additional protections for mental health and substance abuse and exemptions to disclosure that appear on page 12 of the summary of federal HIPAA regulations. We agree that this privacy includes products and services that relate to particular health conditions (e.g. HIV).

PHR related entity
We support the definition as including non HIPAA covered entities, non HIPAA covered entities that offer products or services through websites of HIPAA covered entities, and non HIPAA covered entities that "access information in a personal health record or send information to a personal health record."

Third party service provider
We agree this covers third parties which "provide services to a vendor of personal health records…and accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information…"

Proposed section 318.3 Breach notification requirement
We support that "upon discovery of a breach of security, to notify U.S. citizens and residents…and to notify the FTC." We also support adding language "to provide notice to a senior official of the vendor or PHR related entity." We agree that it "shall be treated as discovered as of the first day on which such breach is known to a vendor…" We support the notion "reasonably should have been known" and the use of breach detection measures.

Proposed section 318.4 Timelines of notification
We strongly oppose that 60 days notice to consumers is "without unreasonable delay". We agree that reasonable attempts include email, letters, and phone calls based on consumer preference. We also agree if 10 or more individuals cannot be reached, it will be necessary to provide information on the homepage of the website or through the media. However, the notification to consumers should be the same timeframe as notice to the Commission, which is five business days. Much damage can be done in 2 months time with the use of this information which could affect individuals personally, such as in the case of divorce, or professionally, such as employers basing hiring or firing practices on confidential healthcare information of current or prospective employees. We also agree that if the information included social security numbers, consumers must be given information on how to prevent fraud and identity theft.

Paperwork Reduction Act
We agree with the cost burden associated with breach notification requirements. However, we see no information such as sanctions or reimbursement to consumers. We strongly disagree that unauthorized disclosure of health information resulting in merely "the likely harm will be personal embarrassment". We have seen cases where misuse of unauthorized health information affected families in courts dealing with custody issues. We have seen outdated and unauthorized mental health information affect families dealing with police, parenting time, DYFS, children's mental health services, schools, and doctors refusing to communicate information to custodial parents. We've heard cases where employers heard children had special needs so either dropped their coverage, fired their parents, or refused to hire their parents solely due to their child's medical condition, rather than the qualifications of the employee. There should be fines associated with breaches, reimbursement to families, and increased sanctions for repeat offenses.

In general, we would recommend one additional area for possible clarification: the relationship between HIPAA, FTC, and FERPA, the Family Educational Rights and Privacy Act. There are entities, such as early intervention located in Department of Health, which are bound by both HIPAA and FERPA, and also consult with third parties as well as utilizing a statewide database. Unfortunately, the privacy laws are not always

consistent, sometimes leading to lack of clarity regarding applicability of laws and which law "trumps" the other in the case of inconsistency. We recommend that a review of the provisions of these laws be conducted and any inconsistencies or lack of clarity be addressed.

Thank you for the opportunity to comment on the proposed FTC rule on Health Breach Notification.

Sincerely,

Lauren Agoratus, M.A.-parent
NJ Coordinator- Family Voices at the Statewide Parent Advocacy Network
NJ Caregiver Community Action Network-Nat'l Family Caregivers (volunteer)
35 Halsey St., 4th Fl.
Newark, N.J. 07102
(800) 654-SPAN ext. 110
Email familyvoices@spannj.org
Website www.spannj.org