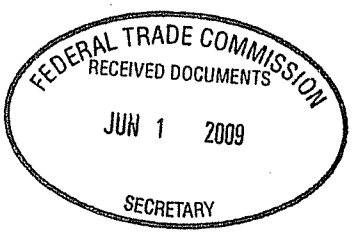
dossia



June 1, 2009

Donald S. Clark
Secretary
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

Dossia[1] was initiated by a consortium of large U.S. employers for the purpose of creating a national system to deliver personal health records for their employees and other individuals. Dossia represents nine large U.S. companies representing over five million employees and dependents.[2]

Dossia believes that personal health records can change U.S. healthcare by helping people to help themselves by directly connecting individuals with their personal health information – making every citizen a true stakeholder in our shared responsibility and mutual interest to manage the health and wellness of the nation.[3] Healthcare literacy is key to driving healthcare costs down and improving the quality of care for everyone. People can only act on what they know – giving them access to their own personal and private health data will help them be better healthcare consumers.

Too often, the U.S. healthcare system leaves patients confused and in the dark. They struggle to navigate a complex and bureaucratic system in which each clinician has only an incomplete and limited view of their relevant history, conditions, medications, and lab results, and lacks any practical means of getting complete medical records in time for clinical decision-making. Making matters worse, patients themselves rarely have access to their own

---

[1] Dossia Consortium is a 501(c)(6) not-for-profit organization focused on supporting policy that promotes the creation of personal health records and employee health and wellness. Dossia Foundation is a 501(c)(3) charitable organization focused on educating healthcare consumers about the utility and value of Personally Controlled Health Records and the development of meaningful architecture and standards to realize the goal of a national health record infrastructure. Dossia Service Corporation is a for-profit entity focused on creating, maintaining and providing Personally Controlled Health Records to individuals.

[2] Abraxis Bioscience, Applied Materials, AT&T, BP America, Inc., Cardinal Health, Intel, Pitney Bowes, sanofi-aventis and Wal-Mart.

[3] The benefits of this high-tech model can be seen in the speed with which healthcare providers and the Center for Disease Control and Prevention (CDC) have been able to analyze instances of H1N1 flu. For many years, states have been required to report potential epidemics to the CDC and have done so through paper-based systems, which were slow and inefficient. Now, electronic tools have begun to transform the reporting system, decreasing the reporting burden on healthcare providers and providing more instantaneous analysis of the instances and trends of the H1N1 flu.

important records unless they have exerted huge efforts to obtain and manage them. Medical decisions are thus often made on the basis of incorrect and incomplete information, with correspondingly poor outcomes.

It is our view that real change can only come about if the American healthcare consumer is empowered through access to their own information. We believe that empowering every citizen with access to their own personal health information will enable them to take charge and to take personal responsibility – to ask smarter questions and make smarter decisions about health and healthcare. We think that patient control and ownership of health data will ultimately facilitate competition, reduce costs, and lead to better health outcomes.

Dossia's Personally Controlled Health Record is a way for individuals to store copies of their personal health information. A Personally Controlled Health Record can assemble information from a multiplicity of sources into one place. Dossia's plan is to gather health data, at the individual's request, from both institutional sources – insurance claims, laboratory, pharmacy, hospital, physician – and personal sources – health devices, self-entered information, personal biometrics - and facilitate the transfer of electronic copies into the employee's personally controlled health record. HIPAA makes clear that everyone is entitled to a copy of their own data and ARRA took this a step further by entitling everyone to an electronic copy of their information sent to a destination of their choice.[4]

Dossia's system has been developed in collaboration with researchers at Children's Hospital Boston and Harvard Medical School. The Dossia system attempts to maximize use of existing data systems and networks and open interfaces in order to facilitate the population of such Personal Health Records.

Dossia is a non-tethered solution. Once gathered and securely stored in the Dossia database, the electronic summary of health information is portable. Dossia's intent is to make the PHRs continually available to individuals for life, even if they change employers, insurers, or healthcare providers.

We strongly believe that this model is critical to persuading individuals to invest their effort in using a lifelong health tool. Solutions that are tethered to one health plan or one health institution can only reveal a subset of the information for one person given the fragmented nature of the U.S. healthcare sector and the mobile nature of employees who regularly change jobs, health plans, doctors and pharmacies.

Dossia anticipates that we may provide Personally Controlled Health Records to individuals in different ways. For example, an employer may offer Dossia Personally

---

[4] ARRA Sec. 13405(c)(3); HIPAA 45 CFR 164.522(a)(1)(i)(A).

Controlled Health Records to its employees, and their families, who participate in the employer health plan. An employer also may directly offer Dossia Personally Controlled Health Records to all its employees, and their families, whether or not they participate in its health plan. An employer might even offer Dossia services in both ways simultaneously – offered by the health plan for those who participate, and offered directly by the employer for employees or family members who are not covered by the health plan. In one family, therefore, one parent might have a Dossia account offered by the health plan, while the spouse and children might have Dossia accounts offered directly by the employer. In addition, Dossia may eventually offer Personally Controlled Health Records to individuals directly, independent of any employer relationship. Indeed, the same individual might have a relationship with Dossia in several ways – she could participate as an employee of one company, then contract directly with Dossia upon leaving the company, and then again participate as part of another employer's health plan.

In all these situations, however, Dossia is acting on behalf of the individual, creating a repository of information about that individual. It is Dossia that will have the direct relationship with the individual, regardless of who "pays" for the Personally Controlled Health Record. When an individual interacts with her personal health record, wants to view information, or wants to authorize the collection or disclosure of information, she will be interacting with Dossia.

Importantly, Dossia believes that maintaining the privacy and security of an individual's healthcare information is critical to generating the trust that is necessary for individuals to use Personally Controlled Health Records. Dossia participants maintain control over the information that comes into their records – they decide if they want to share their information with others. In order to protect the personal health information in the Record, Dossia employs physical, administrative and technical controls.

Dossia appreciates this opportunity to comment generally on the breach notification provisions of the HITECH Act, and with respect to basic questions of jurisdiction and regulation and the important need for harmonization with HHS, non-duplication, direct notification as well as the need for preemption of conflicting state law requirements.

Breach Notification: Basic Questions of Jurisdiction and Regulation

In the HITECH Act, Congress recognized the importance and emergence of Personal Health Records and recognized that further study was needed with respect to the ultimate regulatory regime. Congress directed the Secretary of HHS, in consultation with the FTC, to study and submit a report within a year to Congress regarding appropriate privacy and security requirements for non-HIPAA entities and a determination as to which federal government agency is best equipped to enforce such requirements.

In the meantime, however, it appears that, for breach reporting purposes, Congress attempted to divide those involved with personal health information into two camps: those who are covered entities and their business associates governed by HIPAA breach regulations and other entities that would be subject to FTC temporary breach regulations.

Moreover, Congress made the decision that the entity with the relationship with the customer should be the entity that notifies the customer in case of a breach of their information. Thus, business associates notify the covered entity, which in turn notifies the consumer. Similarly, third-party service providers to PHRs notify the PHR vendor, which in turn notifies the customer.

It is, and may remain, unclear whether the FTC or HHS will ultimately have regulatory jurisdiction over all or part of Dossia, or over all or part of its operations. As explained above, Dossia may provide its Personally Controlled Health Records to individuals in different ways (i.e., Dossia may operate in several "modes"). By doing so, it might arguably be considered a business associate of a covered entity in some situations, such as if Dossia is offered as an adjunct to an employer's health plan, or a vendor of Personal Health Records in others, such as to an employee's family members who are not covered by the employer's health plan.

However, Dossia believes the crucial question of which regulatory framework applies, including which set of breach notice provisions apply, should not be controlled by whether particular users of the Dossia system are or are not covered by the aspect of Dossia services that may be subject to a business associate agreement with a health plan. Instead, Dossia believes that the guiding principle should be the basic question of "whose customer is it?" Whether provided by or through an employer or employer health plan, or directly to an individual from the Dossia website, or via a doctor or clinic, in each case Dossia establishes a direct relationship with the individual. In all these situations, Dossia is acting on behalf of the individual, creating a repository of information about that individual. It is Dossia that has the direct relationship with the individual, who authorizes the aggregation of information into the Dossia Personally Controlled Health Record and who decides whether, when and to whom to release any or all of such information from his Personally Controlled Health Record.

For these reasons, Dossia concludes:

(1) That the FTC and HHS should continue to gather information about the complexity of the operating framework and legal environment of "hybrid" PHRs such as Dossia that may, in certain deployments, offer services to employees as part of a business associate agreement with an employer health plan and simultaneously offer services directly to other individuals (even possibly in the same family) in a free-standing arrangement;

(2) That the complexity of such "hybrid" PHR entities underscores the urgent need for harmonization and simplification of all federal and state legal requirements affecting PHRs, including breach notice duties, substantive operating controls, information security, and which government entity will serve as the regulatory authority; and

(3) That, absent such harmonization and simplification, consumers may be harmed and confused by a multiplicity of breach notices from different entities (possibly even received by different family members arising from the same incident) and that the development of PHRs will be burdened and impeded by onerous legal costs and conflicting operational requirements.

Specifically, Dossia respectfully requests:

(1) **Harmonization**: The FTC and HHS should maximize the harmonization of their breach notice requirements (consistent with, and building on, Congressional direction to do so with respect to security requirements, timeliness, method and content of notification), making them identical wherever possible for all PHRs and PHR related entities regardless of whether the PHR is or is not subject to a business associate agreement.

(2) **Non-duplication**: The FTC should adopt its proposal that to the extent a PHR provider is considered a business associate it will be subject only to the HHS breach notification requirements and HHS should adopt a parallel rule that to the extent a PHR is not considered a business associate then only FTC breach notification requirements will apply.

(3) **Direct notification**: FTC (and HHS) regulations should provide that a PHR provider with a direct relationship with the consumer – such as Dossia's individual, portable relationships with enrolled individuals -- provide any notice of the breach of information to the individual in order to best protect consumers regardless of any business associate status or the desires to the contrary of the Covered Entity.

(4) **Legislation**: The FTC (and HHS) should pursue clarifying legislation, to the extent that the FTC (or HHS) does not believe it has the authority to achieve the three objectives above, or to fully preempt conflicting state breach notice and information security laws.

Comments on Selected Proposed Definitions

1. Breach of security.

An early need for regulatory consistency can be seen in provisions explaining when notification of a breach must be made. Vendors of Personal Health Records and other non-HIPAA covered entities must notify individuals when "unsecured PHR identifiable health information was acquired by an unauthorized person..."[5] At the same time, a HIPAA-covered entity must notify individuals "whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach."[6] In addition, the term "breach" includes several exceptions revolving around the unintentional acquisition, access or use of protected health information by an employee or individual acting under the authority of a covered entity.[7]

The FTC has done a commendable job of attempting to introduce some compatibility and consistency into these provisions. Specifically, the FTC proposes that an employee who "inadvertently accessed the database, realized that it was not the one he or she intended to view, and logged off without reading, using or disclosing anything" would not have "acquired" information, such that no breach notification would be required. Dossia suggests that the FTC further clarify and somewhat broaden this interpretation to include the exceptions noted in the statute under Section 13400(1)(B). Dossia also urges the FTC to urge Congress to adopt technical amendments to make the wording of these definitions identical to avoid future ambiguities and legal issues.

2. PHR identifiable health information.

The FTC's breach notification provisions apply to the unauthorized acquisition of unsecured PHR identifiable health information. Dossia believes that the FTC's proposed interpretation is both too narrow and too broad.

It is too narrow in that it might miss certain vendors of Personal Health Records. This is because the definition of "PHR individually identifiable health information" in ARRA includes a cross-reference to individually identifiable health information, as defined in Section 1171(6) of the Social Security Act (42 U.S.C. § 1320d(6)). This is information that "(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." ARRA further specifies

---

[5] Section 13407(f)(1).

[6] Section 13402(a).

[7] Section 13400(1)(B).

that with respect to an individual the information "is provided by or on behalf of the individual" and that it "identifies the individual...".

Dossia thinks this definition is too narrow in that a PHR might include information that is not created by entities covered under the definition above (e.g., a blood pressure check at the local grocery store) or is not received by such an entity (since Dossia itself would not be such an entity). Dossia does not believe that the statute intended to exempt an entity such as itself; rather, it was a case of an inartful drafting. For this reason, Dossia suggests the FTC propose somewhat more flexible regulations to encompass such situations and, further, that the FTC urge Congress to modify the definition in future legislation to avoid ambiguity about whether PHRs and related entities might inadvertently avoid regulation if they do not include information created or received by traditional healthcare entities.

Dossia also believes that using the above definition to cover a security breach of a database containing just names and credit card information, even if no other information was included, is a broad extension beyond what Congress likely intended. There are numerous other statutes covering collection and use of such credit card information – insofar as Congress seeks to impose a specific data breach notification requirement, it should do so explicitly as well. We suggest that the FTC state that the proposed rule would cover a security breach containing names and credit card information only if the credit card information was expressly tied to "payment for the provision of health care to an individual," not names and credit card numbers in isolation from healthcare payment.

3. Vendor of Personal Health Records.

ARRA defines a vendor of Personal Health Records to mean an entity "other than a covered entity [as defined in HIPAA] that offers or maintains a personal health record." The FTC's proposed regulations state that a vendor of Personal Health Records includes "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."

As an interim measure, Dossia supports the FTC's proposed definition – and regulatory scope – and also urges HHS to adopt a parallel rule that to the extent a PHR is not considered a business associate, then only FTC breach notification requirements will apply.

But, as we have explained above, this proposal defines the real problem rather than solves it. It does not address the fundamental issue of what <u>should</u> <u>be</u> the proper regulatory treatment of PHRs – like Dossia -- that are (1) always controlled by the consumer (2) with whom the PHR has a direct relationship and (3) may or may not sometimes operate (at least partially) in a business associate status.

To repeat, Dossia believes that the FTC (and HHS) should adopt regulations requiring a PHR provider with a direct relationship with the consumer to be the entity to provide any notice of the breach of information to the individual in order to best protect consumers regardless of any business associate status or the desires to the contrary of the Covered Entity.

Consider again just one example that illustrates the wisdom of such a requirement – Dossia enrolls a husband and wife and their son but only the mother participates in the employer's health plan. Absent the solution proposed here, even in the case of a single breach the mother would receive a notice from the employer while the husband and son would receive a different notice directly from Dossia. Such a confusing situation would frustrate consumers and, no doubt, inhibit them from participating in PHRs and thus realizing the benefits of having meaningful access to their health information in one place.

Moreover, the current rulemaking addresses only breach notification requirements. Our concern is greatly increased when we consider that the HIPAA/non-HIPAA dichotomy could be the basis for other future substantive regulation.

Another example makes the point. Business Associates essentially operate as vendors to, and at the pleasure of, Covered Entities. Consumer-facing PHRs operate in a direct contractual relationship with their enrollees and take direction from them and they control the uses and disclosure of information. Upon termination of a BA relationship, the BA must return or destroy the protected health information it has held on the CE's behalf. But for a consumer-facing PHR to return or destroy that data held in enrollees' PHR accounts would be to violate the PHRs' promises to let their enrollees control their data.

We strongly urge the FTC, working with HHS and Congress if necessary, to adopt a single set of regulations that will better fit PHRs than the mere extension of the traditional healthcare framework, and that will promote – not inhibit – the widespread use of PHRs.

Comments on Selected Proposed Breach Notification Requirements

As discussed above, Dossia believes that who should notify the consumer depends on whose customer it is. This is the best way to prevent consumer confusion and ensure responsiveness by individuals to breach notifications. The breach notification requirements should follow the business relationship expectations of consumers.

1. Timeliness of Notification

Pursuant to the statute, the FTC's Notice proposes notification to individuals and the media "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. This standard clearly contemplates, however, that there are

legitimate reasons for delaying such notification and Dossia believes the FTC should provide guidance in this regard. For example, an entity should be able to take the time necessary to determine the scope of the breach, prevent further disclosures, restore reasonable integrity of the system, or provide notice to law enforcement.

Dossia believes that providing notice to the FTC no later than 5 business days after a breach involving 500 or more individuals is too short and too inflexible a requirement. The FTC itself acknowledges that it may be receiving partial or incomplete information at that time.[8] Given that the FTC is unlikely to take any action on the basis of early, fragmented information knowing that it may be subject to change as more facts emerge, we do not believe that consumers would be benefited by companies giving the FTC preliminary and incomplete information at such an early date. Having to provide the FTC notice within 5 days would impose additional legal expenses and, worse, be an unhelpful distraction just at the crucial post-breach time when resources are needed for forensic investigation, harm mitigation, and response planning. Dossia believes a more reasoned approach would be for entities to inform the Commission "as soon as reasonably possible" once the entity suffering the breach understands the dimension of the problem (including whether it presents the problem of the acquisition of information of 500 or more individuals) and is able to take measures to prevent further losses, but in any case no later than the point at which the entity notifies individuals.

2. Methods of Notice

First, Dossia, like many PHRs, is an entirely online service. Maintaining online operations and keeping staff and overhead modest is essential to our ability to offer PHRs at low cost to employers or to individuals directly. It is essential that in the event of a breach, Dossia be able to notify all our users by e-mail, just as we would notify them by e-mail of any other important development affecting their Dossia account.

Dossia appreciates the Commission's recognition that e-mail notification is appropriate. However, Dossia does not support the Commission's requirement that there be separate "express affirmative consent" to receive breach notices by e-mail. Dossia should not be forced to change its operations and incur the additional expense of postal mail if enrollees fail to specifically elect e-mail notice of breaches.

Second, because of Dossia's direct relationship with its users, Dossia expects that it will be able to provide individual notification. However, in those situations where Dossia must provide substitute notice because 10 or more individuals cannot be reached, Dossia believes the FTC's proposed substitute notice is too far-reaching.

---

[8] See footnote 19, page 27.

Certainly Dossia agrees that any posting on its website should be clear and conspicuous. But Dossia believes a six-month posting requirement is unnecessarily and inappropriately long. Dossia disagrees with the Commission that such a requirement would ensure that individuals who intermittently check their accounts will obtain notice without being unduly burdensome for consumers. To the contrary, Dossia believes that the longevity of such a notice may well lead consumers to disregard it – much as many individuals do with respect to their HIPAA privacy notices.

Third, we also urge the Commission to ensure that any "reasonable procedures in place to verify that they are providing the requested information only to the individual and not an unauthorized person" be permitted through an e-mail exchange since, as the Commission anticipates, PHRs generally involve relationships conducted only online.

Finally, Dossia asks the Commission to provide a draft form to be used by entities to provide the immediate and annual required notice to the Commission and request comment on such a form. Dossia believes that it is important to ensure that the requested information can be easily obtained from existing systems and that it will not be unduly burdensome to generate such information.

Preemption of Conflicting State Requirements

We also note that the same important factors leading to regulatory consistency at the federal level also are compelling with respect to preempting state requirements in this area. Today, 44 states plus the District of Columbia have some form of data breach notification requirements. It is difficult for businesses to comply with these requirements.

Consider just one example. The Massachusetts breach notification law states that a breach notice "shall not include the nature of the breach or unauthorized acquisition or use the number of residents of the commonwealth affected by said breach or unauthorized access or use."[9] Other states call for only a general description of a breach.[10] These could be in conflict with the more detailed federal breach notice requirements.

The states moved to enact breach notice laws in the absence of federal legislation. Now, however, Congress has acted with respect to breaches of personal health information generally and vendors of Personal Health Records specifically. Insofar as Dossia or any

---

[9] 2007 Mass. H.B. 4144 (NS) at § 3(b).

[10] *See e.g.*, N.C. Gen. Stat. § 75-65(d) (notice must include description of the "incident in general terms") and Hawaii and New Hampshire (same); *see also, e.g.*, Mich. S.B. 309 (notice must "describe the security breach in general terms").

other entity is covered by and must comply with the requirements of the HITECH Act, these should suffice to meet state requirements as well.[11]

We appreciate this opportunity to provide comments on the FTC's proposed breach notification regulations. We also look forward to working with the FTC (and HHS) as you proceed with your study and report to Congress.

Colin Evans
President
Dossia

[11] Indeed, Dossia notes that in calculating the amount of work necessary to comply with its proposed regulation under the Paperwork Reduction Act, no consideration was given to the time necessary to review applicable state laws and regulations for consistency.