

Written Testimony of

**Colin Evans
President CEO, Dossia**

Before the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality, and Security

May 20, 2009

Chairs and Members of the Subcommittee, my name is Colin Evans, and I am the President and CEO of Dossia Foundation, a non-profit organization set up by a consortium of large U.S. employers for the purpose of creating a national system to deliver lifelong, personal, private, and portable health records for their employees. We commend the Subcommittee for holding this hearing today. We are committed to working collaboratively with you, others in the Department of Health and Human Services, the Federal Trade Commission, and other stakeholders to explore ways to protect the privacy and security of health data while also empowering individuals with practical access to their own personal health information.

My testimony today begins by describing the current state of our nation's healthcare system, then moves to discussing what we believe to be the future of healthcare—an environment in which patients have control of their information and move from simply being patients to being fully informed consumers. The testimony then discusses how the principles of privacy, control, and security should be incorporated into the innovative IT healthcare solutions that will form the foundation of this future.

I. Current State Of Healthcare in the United States

The current U.S. healthcare system is dysfunctional. Healthcare costs currently fall on U.S. industry through direct payment for their employees' healthcare, through taxes to pay for everyone else's healthcare, and through the costs of uncompensated care for the uninsured. As costs have risen dramatically, fewer employers can afford to provide healthcare, and fewer employees can afford to take the healthcare offered, resulting in the swelling ranks of the uninsured. In a global economy, healthcare inefficiency is penalizing the United States by draining resources away from U.S. innovation, investment, and jobs.

The healthcare sector in our country consumes 16 percent of U.S. Gross Domestic Product (GDP). The average for countries who are members of the Organization for Economic Cooperation and Development, however, is nine percent and no other developed nation spends more than 11 percent of their GDP on healthcare. The higher amount of spending in the U.S. is not delivering a higher quality of care. In fact, the opposite is true. The Commonwealth Fund scorecard gives the U.S. system a failing grade compared with other developed economies, measuring significant shortfalls in efficiency, access, and quality of care.

A. National Healthcare Spending Increases ¹

In 2008, health care spending in the United States reached \$2.4 trillion, and was projected to reach \$3.1 trillion in 2012. Health care spending is projected to reach \$4.3 trillion by 2016. The annual premium that a health insurer charges an employer for a health plan covering a family of four averaged \$12,700 in 2008. Workers contributed nearly \$3,400, or 12 percent more than they did in 2007. The annual premiums for family coverage significantly eclipsed the gross earnings for a full-time, minimum-wage worker (\$10,712).

Workers are now paying \$1,600 more in premiums annually for family coverage than they did in 1999 and, since 1999, employment-based health insurance premiums have increased 120 percent, compared to cumulative inflation of 44 percent and cumulative wage growth of 29 percent during the same period. Further, premiums for employer-sponsored health insurance in the United States have been rising four times faster on average than workers' earnings.

B. U.S. Healthcare Costs Exceed Those of Other Developed Countries ²

The United States spends more money on health care than any other country in the OECD. The OECD consists of 30 democracies, most of which are considered the most economically advanced countries in the world. According to OECD data, the United States spent \$6,102 per capita on health care in 2004 — more than double the OECD average and 19.9% more than Luxembourg, the second-highest spending country. In 2004, 15.3% of the U.S. economy was devoted to health care, compared with 8.9% in the average OECD country and 11.6% in second-placed Switzerland.

C. U.S. Healthcare Quality Is Lower Than Other Developed Countries ³

Previously, it was taken as an article of faith among most Americans that the U.S. health care system was simply the best in the world. Yet growing evidence indicates the system falls short given the high level of resources committed to health care. The quality of care in our country is highly variable and is delivered by a system that is too often poorly coordinated, which drives up costs and puts patients at risk. These rising costs strain family, business, and public budgets. These factors, along with deteriorating access and variable quality, makes improving healthcare performance a matter of national urgency.

II. Future of U.S. Healthcare: A Patient-Driven System

We applaud the Administration's vision to reform health care through advancements in health information technology, but we believe it is of critical importance that the American consumer is at the center of any effort. Dossia believes that, along with equipping doctors, the Administration's highest priority should be to invest in connecting consumers with their personal health information directly – to make every citizen a true stakeholder in our shared responsibility and mutual interest to manage the health and wellness of the nation.⁴

¹ See www.nchc.org/facts/cost.shtml - The National Coalition on Health Care

² See assets.opencrs.com/rpts/RL34175_20070917.pdf - U.S. Health Care Spending: Comparison with OECD – Congressional Research Service – 9/07

³ See www.commonwealthfund.org/publications/publications_show.htm?doc_id=401577 - Why Not the Best? Results from a National Scorecard on U.S. Health System Performance - September 2006.

⁴ The benefits of this high-tech, patient-driven 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

A. The Need for Empowering Consumers with Information

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 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 make healthier choices and lend their voice to reform of our dysfunctional health care system.

Our approach is entirely focused on connecting the health care consumer to their data for several key reasons:

- Better information about patients will produce better health outcomes. It's not enough that information exists "somewhere"; it needs to be available at the right time.
- Patient control and ownership of their health data will facilitate competition. Informed patients will ask better questions and demand better answers from all their healthcare providers. This is critical to cost and quality transparency.
- Better informed patients make better decisions about their care, and make more efficient use of scarce health care resources – most health care consumers today do not have access to vital information that would aid their decision-making.
- Real change can only come about when every American health care consumer has the power and ability to participate as a true stakeholder in their own health - hiding information from patients will only make our current problems worse.
- Personal health record systems represent a quicker, simpler, and cheaper path to a health record for every American as an interim step towards a comprehensive connected Health IT network.

B. Personal Health Records: An essential part of the complete solution

First we have to address a key myth: there is no such thing as an Electronic Medical Record for any American. Health and medical information on any individual is fragmented and scattered across systems, across institutions, and across time. Most of the information is on paper and effectively inaccessible. Any one person's medical picture is like a mosaic in Pompeii; each piece is critical to the total image but most are lost to history. The result of this fragmentation is

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.

care that is unsafe and uncoordinated. Asking the thousands of healthcare participants to collaborate to put all of this into a shared clinical EMR system via a nationally agreed network is impossible economically, politically, and commercially; there are just too many conflicting opinions, technologies, and interests to reconcile.

Second, personal medical data is now being created and managed in more and more places; a vastly increasing number of pieces in the mosaic from personal health devices, exercise equipment, remote patient monitors, connected biometrics, retail genomics, internet searches and purchases. All of this is digital and all of it is getting closer to the individual user/patient/consumer.

In reality, a personally controlled health record is the only feasible way to quickly assemble a coherent picture of an individual – HIPAA makes it clear that everyone is entitled to a copy of their data and ARRA took this a step further by entitling everyone to an electronic copy of their information sent to a place of their choice. This legislative foresight, finally granting everyone the right to meaningful access to their own information, creates the conditions for rapid and effective change in healthcare.

Personal health records (PHRs) empower individuals to take control of their health and reduce medical costs by initiating, maintaining and controlling access to a complete and accurate summary of the health and medical history of an individual. Potential savings from healthcare literacy through interoperable online PHRs are projected to be as much as \$21 billion annually on a national level (with an 80% usage rate) in a November 2008 report issued by the Center for Information Technology Leadership. The ability to inventory test results, as well as to access medication lists and renewal schedules, are examples of the efficiencies and improved quality of care that can be achieved through the individual access to lifelong, portable, private, and secure health records.

As we consider ways to deliver much needed improvements in healthcare quality and effectiveness, we should regard the PHR as a crucial patient-doctor communication tool. Chronic care accounts for 80% of US healthcare spending but most of chronic care management activity takes place outside the clinical setting. Improvements will come, therefore, not just from increased doctor performance but increased patient performance that can be driven by engaging, connected and personal health systems.

Finally, as we consider the broader questions for health reform, remember that PHRs have a chance of much faster proliferation than EHRs and can offer a disruptive care infrastructure that can help generate new care models and new markets for personal health solutions that improve quality and access while reducing costs. True health reform requires a rethinking of the care model and business model for health provisioning and PHRs are a key part of that rethinking. By putting data into the hands of consumers (both for self-care and family caregiving), by creating new forums for conversation between patients and clinicians, by facilitating better care coordination between the fragmented locations and specialties of care that exist today, and by offering a platform for behavior change and early detection that is where real costs and suffering will be reduced

C. The Dossia Model

Dossia is a non-profit organization initiated by a consortium of large U.S. employers for the purpose of creating a national system to deliver PHRs for their employees. Founding

members include large U.S. companies representing over five million employees, including Abraxis Bioscience, Applied Materials, AT&T, BP America, Inc., Cardinal Health, Intel, Pitney Bowes, sanofi-aventis and Walmart.

Rather than taking steps as individual companies, we are collaborating to provide employees with access to – and control over – their personal health information through private, portable, and secure lifelong digital health records. Through Dossia, the founding member companies are able to leverage their combined influence to break down barriers to health information, which will help drive consumer-initiated change. Dossia is part of a comprehensive health outreach to the founders' employees via other wellness programs, thus aligning with larger public health goals and programs.

At the employee's request, Dossia gathers health data from both institutional sources – insurance claims, laboratory, pharmacy, hospital, physician – and personal sources – health devices, self entered information, personal biometrics - and facilitates the transfer of electronic copies into the employee's personally controlled health record. 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.

Dossia, although sponsored and funded by employers, is a non-tethered PHR. We strongly believe that this model is critical to the creation of both value and trust for 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 US healthcare sector and the mobile nature of employees – changing jobs, health plans, doctors, pharmacies.

Dossia also has a commitment to open source solutions. The system has been developed in collaboration with researchers at Children's Hospital Boston and Harvard Medical School and the core software will be made available for other public health and research efforts. This openness is also critical to the privacy and trust features of Dossia by allowing inspection of the core code and architecture.

Most importantly, as described below, the PHR is personally controlled, private and secure. Dossia is completely opt-in, and is designed to be a flexible tool that allows patients to input or capture – and share with whom they choose – as much or as little information as they alone determine.

Dossia is working with a number of Personal Health Application and service solutions; independent entities that, with patient permission, can provide a plethora of individualized tools and services such as chronic care management, medication adherence, personal wellness coaching, patient monitoring, or medical information sharing, health communities; the list is potentially endless. Dossia enables these solutions with meaningful data under complete patient control.

The Dossia PHR enables employees to better understand their health. It empowers them to be active partners in managing their healthcare and to make better choices for themselves and their families, and will help improve the quality of care received. Dossia will help make the healthcare system more efficient and effective – reducing medical errors, eliminating waste and reducing costs to healthcare providers and employers that provide health benefits to employees.

D. Electronic Access to a Patient's Information

Under HIPAA, patients have a legal right to a copy of their medical records. In practice, however, this right has often been difficult, sometimes impossible, to exercise. Many clinicians or hospitals require patients to “come to the basement” for their records, refusing to mail or fax records to patients. Charges for copying are sometimes onerous and excessive, delays are common, and the whole process assumes a paper records paradigm..

Congress rightly decided to expand patient access rights in the American Recovery and Reinvestment Act (ARRA) in order to make access more meaningful and practical. Congress directed providers that use electronic health records to give patients electronic copies of medical records. If patients request to have their electronic records sent to a designated entity or person, providers must comply, provided the patients' choice is clear, conspicuous, and specific. While many implementation details must be worked out over time before electronic transmission to patients and their designees is easy and ubiquitous, Congress understood that this expanded right would greatly enhance patients' ability to view and manage their medical records and thus better manage their health. We urge policymakers to take a full and robust view of this access right, which will accelerate adoption of PHRs and the drive to the patient-driven model of the healthcare system.

III. Privacy, Security, and Trust are Key to the Patient-Driven System

Safeguarding sensitive information is crucial to developing a patient-driven healthcare system. Consumers and health care providers will only share and use data if they can trust that its privacy and security will be protected. The challenging issue is deciding what the substantive privacy protections for PHRs and PHAs should look like.

A. Core Privacy Principles

There is widespread consensus that because electronic health data repositories are rapidly growing outside the HIPAA regulatory environment, sensitive data must be adequately protected. Unquestionably, consumers could be severely harmed if their medical data becomes commoditized or is subject to inadequate security. Dossia is in firm agreement with this view. We will comment here on what principles we believe should govern the regulatory environment for PHR/PHA health data held outside the traditional scope of HIPAA. (Consumer medical information could be considered more broadly, but for purposes of discussion here it is used to mean data held in PHRs and PHAs.) The next section will touch on the steps Dossia itself has taken to directly protect the data it holds.

One of the fundamental questions in considering regulation of consumer health information is what legal framework is appropriate. Specifically, a threshold question is whether the framework should be an “extension” of HIPAA or the application of consumer protection law, perhaps customized to the PHR/PHA environment. We would like to briefly point out some problems with a simple “extension” of HIPAA, and encourage policymakers to instead consider the merits of a thoughtful, consumer protection-oriented approach like that of the Markle Foundation.

HIPAA is based on the fundamental legal principle that medical records held by health care entities are business records of those entities. HIPAA did not change the ownership of the records themselves. Instead, understanding that health care records are sensitive and important

and that the absence of controls would produce harm to patients, HIPAA created certain obligations and limitations regarding medical records on the part of health care entities, and it created certain rights regarding those records on the part of patients. These obligations, limitations, and rights drive the complexity of HIPAA, for HIPAA was intended to intricately balance the needs of health care entities, the interests of patients, and societal interests like public health, quality, and research. HIPAA appropriately allows for certain transfers of medical data within the established health care environment where needed for treatment, payment, or operations regarding a patient.

Consumers' data held in PHRs and PHAs should be viewed in stark contrast to this fundamental legal underpinning of HIPAA, *i.e.*, that medical records are business records owned by others. Instead, PHR/PHA data should be viewed more like the contents of one's own home file cabinet – electronic and more useful, to be sure, but still a consumer's own property and subject to the consumer's near-complete control. Other than necessary narrow exceptions discussed below, consumers should have granular and full control over who gets to see the contents of their PHR/PHAs, the scope of data they can see, and whether the data disclosed is identifiable or not, and they should be able to change these choices at any time. This guiding principle for consumer data is different from the logic and foundation of the HIPAA structure, and we are concerned that any attempt to simply “extend” HIPAA to PHR/PHAs would not only be a square peg/round hole problem, but also would inadequately protect consumers. Put simply, consumers should have more control over their PHR/PHA data than they have over records held inside the health care entity/HIPAA environment.

The Markle Foundation's Connecting for Health Common Framework for Networked Personal Health Information⁵ provides a robust and thoughtful foundation suitable to the governance of consumers' PHR/PHA data. We believe the Markle principles, developed through consensus of numerous health care and advocacy stakeholders, should inform any new legal framework and, until new laws or regulations are adopted, should serve as the basis for the design of trustworthy PHR/PHAs. The principles, which are explained well on the Markle website, are:

- openness and transparency
- purpose specification
- collection limitation and data minimization
- use limitation
- individual participation and control
- data quality and integrity
- security safeguards and controls
- accountability and oversight
- remedies

We urge policymakers to address substantive governance of PHR/PHA privacy and security concerns in a manner that will foster consumer trust, advance innovation, and encourage consumers to use newly available technologies to better manage their health. We are concerned that regulatory mechanisms like HIPAA that were designed for a fundamentally different environment could lead to confusion and compliance burdens, as well as inadequate protection for individuals. Furthermore, because the PHR/PHA environment is new and rapidly evolving,

⁵ See www.connectingforhealth.org. See also <http://www.cdt.org/healthprivacy/> which offers many resources on health privacy as well as testimony given before the House Health Committee, discussing, among other things, the fair information principles.

we are concerned that technology and process mandates that are too prescriptive may chill innovation, just at a time that consumers urgently need innovative solutions to help them finally have meaningful access to their own health information.

B. Dossia's Commitment to Strong Privacy Protections

Because of the key link between privacy and consumer trust, Dossia, in consultation with internal and external privacy staff and advocates, made specific public promises about our privacy practices in our Privacy Statement, understanding that these promises would be backed up by federal and state consumer protection law. Some of the issues we analyzed may be of interest to the Committee:

Consent. Consumer control over health information is central to Dossia's vision. Accordingly, we bound ourselves to not permitting disclosure of PHR data unless the participant explicitly and specifically consents (subject to narrow, defined exceptions.) We believe that meaningful consent over disclosures should not be buried in blanket agreements but rather should be unambiguously presented in the User Interface at the point of choice. (The consent issue also highlights one of the square peg/round hole problems of simply "extending" HIPAA to PHRs/PHAs. If disclosing information from a PHR required a lengthy HIPAA authorization with numerous mandatory elements, which would have to be placed behind a hyperlink, consumers would be more confused than if offered a clear, simple, consumer-friendly explanation, question, and check-box, suited to the online environment.)

Exceptions to Consent. How broadly or narrowly to define exceptions to the general principle of complete consumer control over data is a crucial design question for PHRs/PHAs, as well as a crucial policy question for lawmakers. After extensive discussions, including with a panel of clinician advisors, Dossia chose to permit nonconsensual disclosures only: (a) to outside vendors for operational purposes, subject to strict contractual controls, (b) where required by law, including subpoenas, or (c) in extraordinary circumstances, where Dossia reasonably believes disclosure is needed in response to an imminent physical threat to individuals, to defend or assert legal rights, or in response to an immediate health risk authenticated by medical personnel. In defining the scope of these exceptions, Dossia was guided by principles embedded in HIPAA. In fact, we voluntarily undertook an obligation that HIPAA imposes as a mandate on Covered Entities, which is to make reasonable efforts to notify patients or seek a protective court order before complying with a legal requirement to disclose data.

Changes and updates to the Privacy Statement. Some commentators maintain that promises made in privacy statements, in contrast to mandates written in law, are illusory, because companies retain the ability to change their privacy statements at will and without notice. These commentators may be unaware of the growing trend in privacy litigation to prevent companies from unilaterally changing privacy policies to the material detriment of users. That said, Dossia was concerned that users might feel unwilling to trust their data to Dossia's safekeeping if we had full, unilateral power to change our Privacy Statement at will. Knowing that most changes to our Privacy Statement were likely to be merely editorial or reflect operational updates, we did not want to create an obligation to re-consent users for every modification, which could lead to user irritation, attrition, or possibly even users' accounts being closed against their wishes and their data becoming unavailable simply because they failed to respond to a re-consent request. To balance these concerns, our decision was to oblige ourselves to give users' 30 days advance notice (on the Dossia site and via email) before we make material changes to our Privacy Statement. This notice period gives Dossia the flexibility to keep our privacy representations up-

to-date, while giving users time to close their accounts and save their data elsewhere if they do not approve of any changes we might make in the future.

Disclosure of De-identified or Aggregate Data. As the Committee knows, de-identified and aggregate health data has numerous important societal benefits, including research advancements, health care quality, development of best practices, and public health. We are not commenting on the HIPAA provisions regarding de-identified data held by health care entities. But for PHRs, we chose to draw the line more tightly. Because of Dossia's commitment to personal control, we committed ourselves that, subject to the narrow exceptions explained above, we would not release users' data without explicit and specific consent, even if that data was in a de-identified or aggregate format. This position does not reflect a lack of support for data uses such as research or public health; to the contrary, we fully intend to integrate mechanisms whereby users can have their data disclosed for such purposes. But whether the data is de-identified or identifiable, in the Dossia system the users must affirmatively elect to have their data disclosed, even for socially important purposes.

The subject of appropriate controls and safeguards for PHRs and PHAs is complex, both from the standpoint of policymakers and those designing applications. What is clear, though, is that the controls and laws must be thoughtfully designed, customized to the PHR/PHA environment, conducive to innovation, and protective of the sensitive medical information that consumers are trusting to these novel information systems.

Dossia will be submitting formal comments to the Federal Trade Commission proposed rules and the HHS guidance documents. We welcome others' insights on our own operations, and we look forward to continuing to engage in public policy discussions regarding the appropriate substantive regulatory framework for PHRs and PHAs.

IV. Conclusion

In conclusion, we would like to emphasize the following points:

- The U.S. healthcare system is inefficient, ineffective, and unaccountable and previous fixes have not resulted in disruption or systemic change.
- Health care literacy is a critical component of driving health care costs down and improving the quality of care for everyone.
- People can only act on what they know. Giving individuals access to their own personal and private health data will help them be better health care consumers.
- Building trust and providing thoughtful and robust privacy and security functions into IT healthcare systems will drive adoption of the patient-driven model.

Dossia believes that we can change healthcare in the United States by enabling people to help themselves. We look forward to working with you and others in the healthcare ecosystem to move toward the patient-driven healthcare model. Thank you for giving us the opportunity to testify today.