2009

Privacy and Health Information Technology

Deven McGraw
Center for Democracy and Technology

GEORGETOWN UNIVERSITY

O'Neill Institute
for National and Global Health Law

Legal Solutions in Health Reform

Privacy and Health Information Technology

Deven McGraw, JD, LLM, MPH

Legal Solutions in Health Reform is a project funded by
THE ROBERT WOOD JOHNSON FOUNDATION

Prepared for
THE O'NEILL INSTITUTE FOR NATIONAL AND GLOBAL HEALTH LAW
AT GEORGETOWN UNIVERSITY
600 New Jersey Avenue, NW
Washington, DC 20001

O'Neill Institute

for National and Global Health Law

THE LINDA D. AND TIMOTHY J. O'NEILL INSTITUTE FOR NATIONAL AND GLOBAL HEALTH LAW AT GEORGETOWN LAW

The O'Neill Institute for National and Global Health Law at Georgetown University is the premier center for health law, scholarship and policy. Housed at Georgetown University Law Center, in the heart of the nation's capital, the Institute has the mission to provide innovative solutions for the leading health problems in America and globally—from infectious and chronic diseases to health care financing and health systems. The Institute, a joint project of the Law Center and School of Nursing and Health Studies, also draws upon the University's considerable intellectual resources, including the School of Medicine, the Public Policy Institute, and the Kennedy Institute of Ethics.

The essential vision for the O'Neill Institute rests upon the proposition that the law has been, and will remain, a fundamental tool for solving critical health problems in our global, national, and local communities. By contributing to a more powerful and deeper understanding of the multiple ways in which law can be used to improve health, the O'Neill Institute hopes to advance scholarship, research, and teaching that will encourage key decision-makers in the public, private, and civil society sectors to employ the law as a positive tool for enabling more people in the United States and throughout the world to lead healthier lives.

- *Teaching*. Georgetown is educating future generations of students who will become – upon their graduation – policymakers, health professionals, business leaders, scholars, attorneys, physicians, nurses, scientists, diplomats, judges, chief executive officers, and leaders in many other private, public, and nonprofit fields of endeavor. The O'Neill Institute helps to prepare graduates to engage in multidisciplinary conversations about national and global health care law and policy and to rigorously analyze the theoretical, philosophical, political, cultural, economic, scientific, and ethical bases for understanding and addressing health problems.

- *Scholarship*. O'Neill supports world-class research that is applied to urgent health problems, using a complex, comprehensive, interdisciplinary, and transnational approach to go beyond a narrow vision of health law that focuses solely on health care as an industry or as a scientific endeavor.

- *Reflective Problem-Solving.* For select high-priority issues, the O'Neill Institute organizes reflective problem-solving initiatives in which the Institute seeks to bridge the gap between key policymakers in the public, private, and civil society sectors and the intellectual talent and knowledge that resides in academia.

OVERVIEW
LEGAL SOLUTIONS IN HEALTH REFORM

The American public has increasingly identified health care as a key issue of concern. In order to address the multiple problems relating to the access and affordability of health care, President Obama and federal lawmakers across the political spectrum continue to call for major health reform. In any debate on health reform, a predictable set of complex policy, management, economic, and legal issues is likely to be raised. Due to the diverse interests involved, these issues could lead to a series of high-stakes policy debates. Therefore, **it is critical that advocates of reform strategies anticipate such issues in order to decrease the likelihood that legally resolvable questions become barriers to substantive health reform**. In an effort to frame and study legal challenges and solutions in advance of the heat of political debate, the O'Neill Institute for National and Global Health Law at Georgetown University and the Robert Wood Johnson Foundation have crafted the "Legal Solutions in Health Reform" project.

This project aims to identify practical, workable solutions to the kinds of *legal issues* that may arise in any upcoming federal health reform debate. While other academic and research organizations are exploring important policy, management, and economic questions relating to health reform, the O'Neill Institute has focused solely on the critical legal issues relating to federal health reform. The target audience includes elected officials and their staff, attorneys who work in key executive and legislative branch agencies, private industry lawyers, academic institutions, and other key players. This project attempts to pave the road towards improved health care for the nation by providing stakeholders a concise analysis of the complex legal issues relating to health reform, and a clear articulation of the range of solutions available.

LEGAL ISSUES V. POLICY ISSUES

Among the major issues in federal health reform, there are recurring questions that are policy-based and those that are legally-based. Many times questions of policy and of law overlap and cannot be considered in isolation. However, for the purpose of this project, we draw the distinction between law and policy based on the presence of clear legal permission or prohibition.

Under this distinction, policy issues include larger-scale questions such as what basic model of health reform to use, as well as more technical questions such as what threshold to use for poverty level subsidies and cost-sharing for preventive services. In contrast, legal issues are those involving constitutional, statutory, or regulatory questions such as whether the Constitution allows a certain congressional action or whether particular laws run parallel or conflict.

Based on this dividing line of clear permission or prohibition, policy questions can be framed as those beginning with, "*Should we…?"*, and legal questions can be framed as those beginning with, "*Can we…?"* The focus of this paper will be the latter, broken into three particular categories: 1) "Under the Constitution, *can we ever…?*"; 2) "Under current statutes and regulations, *can we now…?";* 3) " Under the current regulatory scheme, *how do we…?"* This final set of questions tends to be mixed questions of policy, law, and good legislative drafting.

PURPOSE AND LAYOUT OF THE PROJECT

This project is an effort to frame and study legal challenges and solutions in advance of the heat of political debate. This effort is undertaken with the optimistic view that all legal problems addressed are either soluble or avoidable. Rather than setting up roadblocks, this project is a constructive activity, attempting to pave the road towards improved health care for the nation. Consequently, it does not attempt to create consensus solutions for the identified problems nor is it an attempt to provide a unified field theory of how to provide health insurance in America. Furthermore, this project does not attempt to choose among the currently competing proposals or make recommendations among them. Instead, it is a comprehensive project written to provide policy makers, attorneys, and other key stakeholders with a concise analysis of the complex legal issues relating to health reform and a clear articulation of the range of solutions available for resolving those questions.

LEGAL ISSUES

Based on surveys of current health policy meetings and agendas, popular and professional press, and current health reform proposals, our team formulated a list of legal issues relating to federal health reform. After much research, discussion, and expert advice and review, our initial list of over 50 legal issues was narrowed to ten. An initial framing paper was drafted which identified these ten legal issues and briefly outlined the main components of each. In May of 2008, a bipartisan consultation session was convened to provide concrete feedback on the choice and framing of the legal issues. The attendees of the consultation session included congressional staff, executive branch officials, advocates, attorneys, employers, and representatives of a wide range of interests affected by health reform. Feedback and analysis from this session further narrowed the ten issues to eight key legal issues which warranted in depth analysis of the current law.

These eight pertinent issues are truly legal in nature and must be addressed in any significant reform proposal to avoid needless debate or pitfalls as policy decisions are made. There are multiple other legal issues that will arise as the discussion evolves and, if a federal policy is adopted, the system changes. In this project, however, we have targeted the issues essential for an immediate discussion of federal health reform.

O'Neill Institute

for National and Global Health Law

LEGAL SOLUTIONS IN HEALTH REFORM PROJECT

JOHN T. MONAHAN, JD
Research Professor
Georgetown Health Policy Institute
Co-Director
Legal Solutions in Health Reform

JACQUELINE R. SCOTT, JD, ML
Adjunct Professor, Senior Fellow
Harrison Institute for Public Law
Georgetown Law

BENJAMIN E. BERKMAN, JD, MPH
Former Deputy Director & Adjunct Professor
O'Neill Institute
Georgetown Law

SHEILA P. BURKE, MPA, RN
Research Professor
Georgetown Public Policy Institute
Distinguished Visitor, O'Neill Institute
Adjunct Lecturer and Senior Faculty Research Fellow, Harvard University
John F. Kennedy School of Government

LISBETH A. ZEGGANE
Former RWJF Project Assistant
O'Neill Institute

TIMOTHY M. WESTMORELAND, JD
Visiting Professor of Law
Georgetown Law
Co-Director
Legal Solutions in Health Reform

SARA P. HOVERTER, JD, LLM
Staff Attorney, Adjunct Professor
Harrison Institute for Public Law
Georgetown Law

JACK EBELER, MPA
Distinguished Visitor, O'Neill Institute
Ebeler Consulting

SANDY H. HAN, JD, LLM
Teaching Fellow
Harrison Institute for Public Law
Georgetown Law

ELENORA E. CONNORS, JD, MPH
Fellow
O'Neill Institute
Georgetown Law

MARIESA M. MARTIN
RWJF Project Assistant
O'Neill Institute

Special thanks to the following individuals who contributed to the editing and production of the Legal Solutions in Health Reform Series, as well as the drafting of the Executive Summaries: Brian Bowen, Astrid Dorélien, Marissa Hornsby, Amy Killelea, Melanie MacLean, Anya Prince, and Luis Rodriguez. Also special thanks to John Kraemer for editing and production assistance.

LEGAL SOLUTIONS IN HEALTH REFORM
LEAD AUTHORS

Executive Authority
Madhu Chugh, JD, MPP
Law Clerk
U.S. Court of Appeals for the D.C. Circuit
Washington, D.C.

Individual Mandates
Mark A. Hall, JD
Fred D. & Elizabeth Turnpage
Professor of Law
Wake Forest University School of Law
Winston-Salem, N.C.

Tax Credits for Health
Fred T. Goldberg, Jr., Esq.
Partner
Skadden, Arps, Slate, Meagher & Flom, LLP
Washington, D.C.

ERISA
Peter D. Jacobson, JD, MPH
Professor of Health Law & Policy
Director, Center for Law, Ethics, and Health
University of Michigan
School of Public Health
Ann Arbor, M.I.

Insurance Exchanges
Timothy S. Jost, JD
Robert L. Willet Family Professorship of Law
Washington & Lee School of Law
Lexington, V.A.

Purchase of Insurance Across State Lines
Stephanie Kanwit, JD
Special Counsel & Healthcare Consultant
America's Health Insurance Plans
Washington, D.C.

Privacy and Security of Information
Deven McGraw, JD, LLM, MPH
Director, Health Privacy Project
Center for Democracy & Technology
Washington, D.C.

Insurance Discrimination Based on Health Status
Sara Rosenbaum, JD
Harold and Jane Hirsh Professor of Health Law & Policy
Chair, Department of Health Policy
The George Washington University School of Public Health and Health Services
Washington, D.C.

ABOUT THE AUTHOR

Deven McGraw, J.D., L.L.M., M.P.H., is the Director of the Health Privacy Project at The Center for Democracy and Technology (CDT). The Project is focused on developing and promoting public policies that ensure individual privacy as personal health information is shared electronically. Ms. McGraw has been active in efforts to establish a nationwide health information network. She served on two workgroups of the American Health Information Community (AHIC): she co-chaired the Confidentiality, Privacy and Security Workgroup and served as a member of the Personalized Health Care Workgroup. Both workgroups provided recommendations to AHIC and the Department of Health and Human Services about policies and practices to facilitate greater use of health information technology. She also serves on the Leadership Committee of the eHealth Initiative.

Prior to joining CDT, Ms. McGraw was the Chief Operating Officer of the National Partnership for Women & Families, providing strategic direction and oversight for all of the organization's core program areas. Ms. McGraw also was an associate in the public policy group at Patton Boggs, LLP and in the health care group at Ropes & Gray. She also served as Deputy Legal Counsel to the Governor of Massachusetts and taught in the Federal Legislation Clinic at the Georgetown University Law Center. McGraw graduated magna cum laude from the University of Maryland. She earned her J.D., magna cum laude, and her LL.M. from Georgetown University Law Center and was Executive Editor of the Georgetown Law Journal. She also has a Master of Public Health from Johns Hopkins School of Hygiene and Public Health.

EXECUTIVE SUMMARY
Prepared by the O'Neill Institute

INTRODUCTION:

The increased use of health information technology (health IT) is a common element of nearly every health reform proposal because it has the potential to decrease costs, improve health outcomes, coordinate care, and improve public health. However, it raises concerns about security and privacy of medical information. This paper examines some of the "gaps" in privacy protections that arise out of the current federal health privacy standard, the Health Insurance Portability and Accountability (HIPAA) Privacy Rule, the main federal law which governs the use and disclosure of health information. Additionally, it puts forth a range of possible solutions, accompanied by arguments for and against each. The solutions provide some options for strengthening the current legal framework of privacy protections in order to build public trust in health IT and facilitate its use for health reform. The American Recovery and Reinvestment Act (ARRA) enacted in February 2009 includes a number of changes to HIPAA and its regulations, and those changes are clearly noted among the list of solutions (and ARRA is indicated below where the Act has a relevant provision).

LAW IN EFFECT PRE-ARRA AND PERCEIVED "GAPS":

The Health Insurance Portability and Accountability Act (HIPAA): The use of health information is currently covered by HIPAA and its implementing regulations. The Department of Health and Human Services (HHS) issued final regulations in 2002, which became effective for most entities covered by HIPAA in 2003. The HIPAA privacy regulations set forth rules governing the access, use, and disclosure of personal health information by most traditional health care entities. The goal of the regulations is to ensure that health information is rapidly accessible to those authorized, but kept confidential and protected from inappropriate use.

- **Who is covered:** The Privacy Rule only applies to entities expressly defined in the HIPAA statute, which places unmentioned, new, and emerging entities outside the direct coverage of the rule.
- **What is covered:** The Privacy Rule regulates the type of health information that can be shared by covered entities and for what purposes. But individuals are concerned that their personal health information will not be protected in the emerging e-health environment. For example, privacy may be at risk due to the lack of federal notification standards for breaches; the possibility that developments in technology may make "de-identified" data (not covered under the Privacy Rule) re-identifiable; and the lack of strong prohibition on the use of personal health information for marketing purposes.
- **State law variation**: The Privacy Rule is only a minimum standard, which gives states the power to enact more stringent protections for health privacy. The resulting variations in state privacy laws may pose an obstacle to health information exchange across state lines and/or to a national health information system.
- **Insufficient comprehension of and compliance with the Privacy Rule and enforcement**: Entities covered by the Privacy Rule and individuals/patients do not adequately comprehend the Privacy Rule's provisions, leading health care entities to either over- or under-interpret the Rule and leaving individuals unaware of their privacy rights. In addition, there has been debate among policymakers and stakeholders over 1) whether the Rule to date has been appropriately enforced; 2) whether or not the current mechanisms are adequate to ensure compliance; and 3) what the limits of the enforcement mechanisms should be.

POTENTIAL SOLUTIONS:

The perceived "gaps" in federal legal protections for health information can be grouped into four categories: 1) who is covered; 2) what is covered; 3) state law variation; and 4) insufficient comprehension of and compliance with privacy protections. The solutions range from amending existing law or regulation to encouraging private action through market or other incentives.

- **Who is covered:** Amend HIPAA to create new categories of covered entities and require the federal agencies to issue new privacy regulations to cover activities of new entities; revise regulations and expand recent guidance on business associate agreements to include all health information exchanges in existence or development (ARRA); require all entities handling health information to adopt policies consistent with fair information practices; and/or keep the law in its current state and encourage adoption of good privacy practices through voluntary business agreements.
- **What is covered:** Enact federal legislation prohibiting the use of personal heath information to determine the terms and conditions of employment or health insurance; establish a federal breach notification law applicable to identifiable health information (ARRA); seek the input of experts and public to examine the de-identification safe harbor exception (ARRA); create more options for the use of health data stripped of some individual identifiers (ARRA) and require data use agreements for all data disclosures; require those obtaining data stripped of patient identifiers to commit to keeping data de-identified except in certain circumstances; strengthen, establish, and increase compliance with HIPAA rules regarding the use of personal information for marketing (ARRA); adopt rules governing marketing uses by non-covered entities such as Internet health sites; issue more guidance on how to comply with the Privacy Rule (ARRA); issue new regulations regarding terms of access to health information exchanges.
- **State law variation:** "Wipe the slate clean" and have Congress could establish a new federal privacy law that preempts existing state laws but allows states to pass new stronger privacy provisions; and/or keep the status quo with the federal standard as a floor.
- **Improving comprehension of and compliance with the Privacy Rule and enforcement:** Revise the Privacy Rule to make it less complex; provide more guidance and better education on the requirements of the rules (ARRA); improve consumer education on HIPAA rights by requiring entities to provide a summary notice; ensure a proper enforcement regime for entities not covered by HIPAA that handle personal health information; amend HIPAA enforcement to clarify enforcement authority and also direct the Secretary to pursue civil actions (ARRA); amend HIPAA to allow the Secretary to directly enforce HIPAA regulations against business associates (ARRA); and/or amend HIPAA to allow a private right of action (ARRA).

CONCLUSION:

Generally, there is consensus that efforts to facilitate widespread adoption and use of health information technology must move forward with appropriate protections for privacy and security. However, achieving consensus on the details of what privacy and security measures need to be put in place continues to be a challenge. The new Administration and Congress are moving forward to increase the use of health IT. Any efforts to reform the nation's health systems and to increase the adoption of health IT will need to address the concerns surrounding the privacy and security of personal health information.

Legal Solutions in Health Reform: Privacy and Health Information Technology

Deven McGraw*

Introduction

In discussions of health reform, the increased use of health information technology (health IT) is a common element of nearly every serious proposal on the table. Health IT includes electronic health records kept by providers, personal health records offered by health insurance plans or owned by consumers, and electronic health information exchanges. Although health reform initiatives being discussed contain little detail regarding health IT, in general they promote health IT to facilitate the electronic sharing of health information to improve individual and population health. During the 2008 Presidential Campaign, the health care proposals of both President Obama and Senator McCain discussed health IT. President Obama's proposal invests $50 billion over the next five years to promote the adoption of health IT with privacy safeguards.[1] Senator McCain's plan also encouraged the adoption of health IT, with an emphasis on coordination.[2]

Proponents hope that the increased use of health IT will improve health outcomes for individual patients by facilitating the delivery of evidence-based care and reducing medical errors. Additionally, proponents hope that increasing information sharing among providers will better coordinate care within and across health care settings. Health IT facilitates the creation of a comprehensive health record that can move with an individual over his or her lifetime, in contrast to the fragmented records that exist today. Further, health IT is promoted as a critical tool for improving population health by allowing for the more efficient gathering of data regarding the effectiveness of certain treatments. Finally, health IT is also expected to help decrease health care costs by reducing the duplication of services and the delivery of unnecessary or inappropriate care.

This paper briefly summarizes current federal health privacy law and examines some "gaps" in privacy protections that have been identified by some policymakers and stakeholders in recent debates on this topic. Additionally, the paper puts forth a range of possible solutions, accompanied by some arguments for and against each idea. The proposals in the paper do not represent the universe of possible solutions to each issue; many of them also are not mutually exclusive. The arguments provided in support for or against a particular idea also do not represent all of the arguments for or against any policy option. The solutions do, however, provide some options for continuing the conversation about how we can best strengthen our legal framework of privacy protections to build public trust in health IT and facilitate its use to reform the health care system.

Note: The initial version of this paper was completed before enactment of the American Recovery and Reinvestment Act in February 2009 ("ARRA").[3] ARRA includes a number of provisions amending the Health Insurance Portability and Accountability Act (HIPAA) and its regulations, the main federal law which governs the use and disclosure of health information. Because much of the details of the privacy and security provisions in ARRA will need to be fleshed out in agency guidance or regulations, and because most of the provisions do not take effect until at least a year after enactment, the author of this paper decided not to completely revise the paper to incorporate the changes in the law. Instead, where there is a provision in

ARRA dealing with an issue identified in this paper, a brief summary of that provision is clearly indicated within the list of solutions.

There is widespread agreement that protecting individuals' health information is necessary in order to build public trust in e-health systems and to help drive the widespread adoption of health IT. But unlike other topics addressed in the Legal Solutions in Health Reform project, current health privacy laws arguably do not pose a legal obstacle to health IT. For example, there are no federal health privacy laws that prohibit or directly inhibit the sharing of information electronically for health purposes and that require specific action to resolve. Instead, the debate centers more around whether current health privacy laws are sufficient to build a foundation of trust in health IT that will support an information sharing environment that will improve health care and our health care system – and if not, what more needs to be done. This makes the path to resolution more difficult, as stakeholders may hold very different opinions about the extent of the problem and the appropriate solutions.

Survey data show that a large majority of the public wants electronic access to their health information – both for themselves and for their health care providers – because they believe such access is likely to increase the quality of their health care. At the same time, people have significant concerns about the privacy of their health information on-line. In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% were very concerned about identity theft or fraud;
- 77% were very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 53% were concerned about insurers gaining access to this information.[4]

Health IT is better equipped than are paper records to protect sensitive personal health information. For example, it is often impossible to tell whether someone has inappropriately accessed a paper record. By contrast, technology - including strong user authentication and tracking mechanisms - can be employed to automatically limit and monitor access to electronic health information. Additionally, electronic health information exchange networks can be designed to facilitate data sharing among health care entities for appropriate purposes without needing to create new, centralized databases of sensitive information that will be attractive targets for marketers and those seeking health data for commercial gain, or that can be vulnerable to security breaches. If a system is breached, sensitive data can be protected, in part, by encryption and other security methods. Technology can never be made 100% tamperproof – but it can be more protective than paper records at preventing inappropriate access to information and helping ensure that when there is abuse, the perpetrators will be detected and punished.

At the same time, absent strong privacy and security safeguards, the computerization of personal health information can magnify the risk to privacy. Tens of thousands of health records can be accessed through a single breach.[5] Recent headlines about breaches of electronic records underscore these concerns. The cumulative effect of reports of data breaches and inappropriate access to medical records deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.

Failing to address public concerns about the privacy of their health information could have significant consequences. Without appropriate protections for privacy and security in the healthcare system, some patients engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[6] According to a recent poll, one in six adults (17%) – representing about 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[7] Persons who report that they are in fair or poor health and racial and ethnic minorities (who report even higher levels of concern about the privacy of their personal medical records) are more likely than average to practice privacy-protective behaviors.[8] Due to the reality of privacy risks associated with the computerization of health information, the movement to e-health could increase the percentage of people who engage in privacy protective behaviors. Ignoring these concerns – or inadequately addressing them – will significantly threaten public trust in these new systems.

In general, stakeholders largely agree that entities that handle electronic personal health information should be subject to a baseline set of privacy standards. This consensus breaks down, however, when the discussion gets to the details. For example:

- Do we extend the privacy rules under the Health Insurance Portability and Accountability Act (HIPAA) to all entities that now handle health information, or create new legal standards for entities not currently covered?

- What protections need to be in place? For example, do we rely on current HIPAA rules or are modifications needed, either to address new challenges or because the rules, in the view of some, were imperfect from the start?

- Are these concerns best addressed through changes in statute or regulations, or is it best to police this nascent marketplace through business best practices (or a combination of both)?

- Should we allow for some state law variation or establish federal standards that preempt the field?

- What should we do to ensure compliance with and appropriate enforcement of privacy protections?

.
A brief list of all proposed solutions in each category (without explanatory text and without the sample arguments for and against) can be found at Appendix A at the end of this paper.

I. Federal Law Prior to Passage of ARRA (as noted above, changes to law enacted in ARRA are set forth below in the "possible solutions" proposed for each issue)

With respect to protecting health information privacy, public policymakers are not faced with a blank slate. Within the traditional healthcare system, uses of health information are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations. When Congress enacted HIPAA to facilitate, among other things, the electronic transmission of health care claims to reduce administrative costs, lawmakers recognized the need to protect the privacy and security of health information when data moves electronically. Congress gave itself two years to enact federal privacy legislation – but ended up tasking the Department of Health and Human Services to promulgate privacy and security regulations to

cover information transactions under the purview of HIPAA. The regulations were finalized in 2002 and effective for most entities covered by HIPAA by 2003. The HIPAA statute sets forth the definition of entities covered by the law and important provisions with respect to HIPAA enforcement; the bulk of the HIPAA privacy and security requirements are in the regulations.

The HIPAA privacy regulations – known collectively as the "Privacy Rule" – are based on fair information practices and set forth rules governing the access, use, and disclosure of personal health information (or "protected health information") [9] by most traditional health care system entities (for example, providers, hospitals, laboratories, pharmacies, and health plans). In summary, the Privacy Rule permits covered entities[10] to access, use, and disclose "protected health information"[11] for purposes of treatment,[12] payment,[13] and health care operations.[14] The Rule also allows access, use, and disclosure for 1) certain lawful public health purposes, as required by law, 2) reporting abuse or domestic violence, 3) health oversight activities, 4) judicial and administrative proceedings, and 5) law enforcement purposes. Covered entities may disclose information to family members, and in facility or office directories, as long as the patient doesn't object. All other purposes not specifically mentioned in the Rule require prior patient authorization to access, use, or disclose information. The Privacy Rule applies to identifiable health information regardless of whether it is in paper or electronic form.

HIPAA provides a federal floor, or minimum standard, of privacy protection. It expressly preserves State laws that provide stronger privacy protections for health information.[15] Such State privacy laws include more stringent requirements regarding access, use and disclosure of particularly sensitive categories of health information, such as mental health records and HIV testing and treatment records. The variation in state laws poses difficulties to a uniform privacy standard.

Other federal laws apply privacy protections to specific types of information, or have limited application in specific contexts. For example, the Genetic Information Nondiscrimination Act of 2008 prohibits employers from using genetic information to make employment decisions and prohibits health insurers from using such information to make coverage and underwriting determinations.[16] The Federal Education Rights and Privacy Act, the regulations governing substance abuse treatment facilities receiving federal funds (commonly known as Part 2), and the Privacy Act of 1974 cover only certain settings of care.[17]

With respect to health information on-line or in consumer-owned personal health records, the Federal Trade Commission can use its "unfair and deceptive trade practices" authority to hold some entities accountable for failure to comply with their privacy policies. Federal law does not require these entities to have a privacy policy, or require that certain elements be included in such a policy if it exists. Some have said that the Electronic Communications Privacy Act (ECPA) protects personal health records (PHRs) because it prohibits the vendors of those services from disclosing the contents of those records without the authorization of the record holder. However, the relevant ECPA provision applies only to services that are offered to the public.[18] PHRs available exclusively to employees of a particular company, for example, likely fall outside of this part of ECPA. Moreover, ECPA applies only if the provider is not authorized to access the contents of a customer's records for purposes of providing any services other than storage or computer processing.[19] This caveat may knock out a lot of PHRs that provide services beyond data storage, or that are advertising-based and analyze individual patient records to target ads.

To keep this paper to a manageable length, it focuses on federal privacy protections that are (or could be) more broadly applicable.

II. Possible Issues to be Resolved

The perceived "gaps" in pre-ARRA federal legal protections for health information can be grouped into the following categories:

- **Who is Covered:** The HIPAA Privacy Rule covers only certain "covered entities" as defined in the HIPAA statute: specifically, providers, plans, and healthcare clearinghouses. Many of the new entities storing, handling or managing personal health information electronically do not qualify as covered entities, and thus are not directly covered by the Privacy Rule. As noted above, other federal health privacy laws apply only in specific contexts or are otherwise limited in their application. As a result, there is no baseline set of federal health privacy protections that apply to all entities that handle personal health information.

- **What is Covered:** The Privacy Rule is based on a model of one-to-one electronic transmission of health information among traditional health care system entities and their business partners who perform health-related functions on their behalf. Since the HIPAA requirements were enacted and promulgated, new opportunities to access and disclose health information have arisen (*e.g.*, electronic health information exchanges) which can enhance access to greater volumes of identifiable health information more effectively and efficiently. The Rule also did not envision the rise of personal health records designed for use by consumers. Some believe that truly building public trust in e-health systems requires strengthening a number of the Privacy Rule's current provisions and/or the promulgation of new or additional legal protections. Others believe the Privacy Rule provides sufficient protections for health information in the new e-health environment, and that policymakers merely need to extend its coverage to apply to entities that did not exist when the Privacy Rule was implemented. Similarly, some have suggested approaching this question by focusing only on what is new in the e-health environment – new actors or new ways to access, use, or disclose information not contemplated when the HIPAA regulations were implemented – in order to avoid getting mired in old debates about the current HIPAA regulations.

- **State Law Variation:** As noted above, HIPAA provides a floor of health privacy protection. State laws that provide more stringent protections for health privacy are expressly preserved and not preempted. Some are concerned that the multiplicity of state privacy laws will create an obstacle to cross-state or nationwide electronic exchange of health information. The obstacles may arise because of the operation of a state law that prohibits information sharing except under certain circumstances (such as with patient consent or authorization), or because health care entities are afraid to disclose information in a way that might violate an applicable state law. Others suggest that any information sharing obstacles are primarily due to a lack of understanding and varying interpretations of state laws, which does not necessarily

justify eliminating stronger state privacy protections and enacting a single federal standard.

- **Improving Understanding of (and Compliance with) Privacy Protections:** Even five years after the Privacy Rule went into effect, there is still a great deal of confusion on the part of some entities covered by the Rule about its provisions. For example, the 34 state teams participating in the Agency for Healthcare Research and Quality (AHRQ)-funded Privacy and Security Solutions for Interoperable Health Information Exchange consistently found a "general lack of understanding about some of the basic tenets" of the Privacy Rule as well as of state laws concerning health information disclosure.[20] The frequent result is a more conservative interpretation of the law – a reluctance to disclose information even in circumstances where it is expressly permitted – which could create unnecessary and sometimes inappropriate barriers to electronic health information exchange.[21] Patients and their families also rarely understand the provisions of the HIPAA privacy notice, which is the vehicle in the Privacy Rule for informing patients about the potential uses of their health information and their rights under the Rule.[22]

A. Who Is Covered

As noted above, HIPAA by statute covers only providers (including health care professionals, hospitals, pharmacies, laboratories), health plans, and healthcare clearinghouses.[23] Thus the HIPAA privacy and security regulations also apply only to these covered entities. Under the Privacy Rule, a covered entity can contract with a "business associate:" an organization that receives personal health information to perform activities or services on behalf of the covered entity, but is not part of their workforce. The HIPAA rules do not apply directly to business associates; instead, business associates must be obligated by contract with the covered entity to comply with the HIPAA regulations. A business associate must enter into a "business associate agreement" with the covered entity in order to access protected health information.[24] This agreement must: 1) spell out the required uses and disclosures of such information by the business associate, 2) include a provision prohibiting the business associate from further using or disclosing the data other than as permitted in the contract or required by law, and 3) contain "satisfactory assurances" that the business associate will "appropriately safeguard the information."[25] The HIPAA rules cannot be enforced by the federal government against business associates, as discussed in more detail below.

HIPAA currently does not cover a number of entities that have emerged as part of the movement to electronic health records. For example:

- State and regional electronic health information exchanges – often called Regional Health Information Organizations (or RHIOs) or Health Information Exchanges (HIEs) – and ePrescribing Gateways, all of which may collect or facilitate the exchange of personal health information, usually among health care system entities, are not HIPAA covered entities.[26] In December 2008 HHS issued guidance clarifying that health information networks that merely exchange data on behalf of covered entities must be business associates and thus must execute business associate agreements.[27] However, such guidance does not cover all of the health information exchanges currently in existence or in development. For example, exchanges that collect and directly access information in a

centralized database are not covered by this guidance, and as a result their status under HIPAA is unclear.

- Personal health records (PHRs) and other consumer-facing health IT tools now being created by Internet companies like Microsoft, Google, and WebMD, as well as by employers (for example, Dossia, the consortium of eight of America's largest employers), are not covered by HIPAA.[28] Because these tools are being designed for primary use by the consumer, individual authorization is typically required in order to move information into or out of a PHR. As a result, the vendors of these products have concluded that a business associate agreement is not required; OCR has issued no guidance on this practice.

- Personal health information is migrating onto the Internet through an array of health information sites, online support groups, and other on-line health tools. Often this information is voluntarily posted or shared by individuals. These potential repositories of sensitive health information are not covered by HIPAA as either covered entities or business associates – and privacy protections are guaranteed primarily through enforcement by the Federal Trade Commission (FTC) of the general prohibition against unfair and deceptive trade practices, such as a failure to follow promises made in a privacy policy.

The gaps in HIPAA coverage of these new entities is of concern to some policymakers and industry stakeholders and may be an obstacle to promoting the use of these new technologies. For example, the public may not trust that their information will be protected when it is exchanged or stored electronically because these non-covered entities are not required to comply with any minimum health information privacy standards. Covered entities may be concerned about an unlevel playing field, where their products and services are required to be compliant with current law and the products and services of their competitors are not.

Possible Solutions

Section 13408 of ARRA clarifies that entities transmitting or processing data on behalf of covered entities, like Regional Health Information Organizations (RHIOs), Health Information Exchanges, or E-Prescribing Gateways, are business associates for purposes of HIPAA. Section 13408 also provides that vendors who contract with a covered entity in order to allow that entity, as part of its electronic health records, to offer patients a personal health record, must also be business associates. Section 13424 requires HHS, working with the FTC, to issue a report within one year of enactment recommending privacy and security protections for information accessed and stored on-line. This study must include a recommendation for which agency should have oversight over uses of health information on the Internet and a timetable for regulation.

- ✓ Amend HIPAA to create new categories of covered entities and require the Office of Civil Rights (OCR) to promulgate new privacy regulations to cover the activities of these new entities.

  Arguments For
  - o Arguably provides the most certainty to the market and a more level playing field (even if the regulations applied to these new entities are tailored to the particular challenges raised by each, as is the case today among the major categories of covered entities). **(steps to accomplish taken in ARRA)**

  Arguments Against
  - o This could be difficult to achieve, as some entities may resist coverage under HIPAA; others may welcome a more certain legal environment.
  - o With respect to PHRs, some have argued that HIPAA may not be the appropriate vehicle for regulating those provided by non-health care entities. For example, The National Committee for Vital and Health Statistics (NCVHS) called for protections at least equal to HIPAA to be extended to all PHRs – but did not recommend extending HIPAA to do so.[29] The Center for Democracy & Technology has argued that HIPAA will not address the particular concerns raised by the handling of personal health information by Internet-based companies and other non-health care entities.[30] Two of the prominent House bills from the 110th Congress – the "Protecting Records, Optimizing Treatment, and Easing Communication Through Health Care Technology Act of 2008" (the PRO (TECH) T Act) (H.R. 6357) and the "Health-e Information Technology Act of 2008" (H.R. 6898) (referred to collectively in this paper as the "House bills") - instead called on HHS and FTC to work together to come up with recommendations (or regulations) for privacy protections for information in PHRs.[31]
  - o This concern could be ameliorated by ensuring that all *health care* entities (including exchanges) that handle personal health information are required to comply with HIPAA (either as covered entities or business associates, depending on their structure and function), and imposing new standards on non-health care entities that provide protections similar to HIPAA but that are targeted to address the particular concerns raised in this environment.

- ✓ Require (or encourage) HHS to issue new regulations or guidance to clarify that entities such as health information exchanges or PHRs that receive protected health information from a covered entity must enter into a business associate agreement and at least be contractually bound to safeguard the information and comply with HIPAA. **(partially addressed in ARRA)**

  Arguments For
  - o Does not require legislative action, thus potentially could be accomplished promptly in 2009.

  Arguments Against
  - o Would likely apply only to those entities that are receiving protected health information from a covered entity and thus would not protect personal health information entered into PHRs or onto Internet health sites directly by individuals. Also, the business associate model currently applies to entities performing tasks *on behalf of* a covered entity (emphasis added). Thus this model may make sense for

health information exchanges (or at least those that are operating for the benefit of their covered entity participants); but it makes less sense for PHRs, which operate for the benefit of the consumer.
- Business associates are contractually obligated to adopt health information safeguards or to comply with HIPAA. However, as discussed in more detail below, federal authorities cannot hold them accountable for failure to comply with HIPAA.

✓ Require any entity that holds or manages protected health information to adopt policies that are consistent with fair information practices, which is the model typically relied on to establish appropriate policies for handling personal information. [32]

Arguments For
- Model is endorsed by NCVHS and the Markle Foundation's Connecting for Health multi-stakeholder initiative.
- Ensures that anyone who handles personal health information is subject to at least a uniform baseline set of standards.
- Eliminates need to continue to revisit this issue as the market evolves and new entities/models for sharing health information are introduced.
- Partial coverage can be achieved by imposing the requirement as a federal funding condition.
- Model is more consistent with data privacy standards adopted by the European Commission, thus helping resolve a potential barrier to global data exchange.

Arguments Against
- Could result in HIPAA requirements for some entities and other, less onerous requirements for other entities.
- Fair information practices (FIPs) provide a good model for moving forward – but FIPs are articulated so broadly that building trust in electronic health information sharing may require more clearly defined rules (and achieving broad support for such rules may be difficult).
- If new framework deviates significantly from current HIPAA rules, there will be costs and disruptions in information flows due to covered entities and their business associates having to adjust to new or even dual standards. Further, the resources already spent coming into compliance with HIPAA will be wasted. (Note that these concerns could be ameliorated by building on the current HIPAA rules or by applying new standards only to entities not currently covered by HIPAA).

✓ Keep the law in its current state and encourage the adoption of good privacy practices through voluntary business agreements and/or certification.

Arguments For
- Requires no further action from Congress or the Administration.
- Less stringent approach arguably allows for more innovative responses to addressing privacy and security issues.

Arguments Against
- Compliance through voluntary business agreements or certification (or other voluntary business commitments) will not achieve a uniform baseline of protections.

Consumers do not always have the option to choose providers, plans or other health services based on privacy and security practices when care is needed and resources are scarce.
- Will be perceived by some stakeholders as a lack of response to the privacy and security concerns raised by e-health; thus, may not accomplish much with respect to building trust in e-health systems.
- Requires covered entities to continue the expense and administrative efforts to comply with the HIPAA privacy requirements and allows other entities working in the same space to be relieved of these corresponding responsibilities and expenses.

B. What Is Covered

Electronic health information exchanges and the rise of consumer-focused health management tools hold great potential for improving the flow of information necessary for good health care and helping individuals take a greater role in improving their own health. But to realize this potential, consumers need to trust that their personal health information will be kept private, confidential, and secure. As information becomes more accessible and moves more freely in an electronic exchange environment, current policies regarding access to, and use and disclosure of, health information may be inadequate and contribute to a lack of public trust in health IT.

A number of the issues discussed below relate to perceived deficiencies in the HIPAA Privacy Rule. Some argue that it makes little sense to try to re-open the compromises that were reached in the current Privacy Rule and instead urge policymakers to focus on how best to address the new challenges raised by the emerging e-health environment. Others argue that perceived deficiencies in the Rule will need to be addressed in order to build trust in e-health, regardless of the source of the problem. The following have been raised as issues that may need to be addressed in order to remove distrust as an obstacle to the widespread adoption of health IT and health information exchange.

1. Addressing Privacy Concerns Through Anti-Discrimination Laws

Some have suggested dealing with privacy concerns by prohibiting the use of personal health information to discriminate against individuals with respect to health insurance and employment - two of the key privacy concerns raised by consumers. This is the approach taken in the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits the use of genetic information to make health insurance coverage determinations and in employment-related decisions. Some believe that passing anti-discrimination legislation based on health information or health status[33] would address the most critical privacy concerns and relieve the pressure to enact standards that "micromanage" an entity's use of health information, which could create obstacles to the information sharing that can improve individual health and the U.S. healthcare system.

Possible Solutions

- ✓ Enact federal legislation prohibiting the use of personal health information in determining the terms and conditions of employment or health insurance coverage.

Arguments For

- As noted above, addresses the most critical consumer fears about use of their health information; could obviate need for specific, detailed provisions on information uses for other purposes.

Arguments Against

- Raises larger public policy issues that in the past have been difficult to resolve and that should be discussed in the broader context of health reform (*e.g.*, to what extent employers can use health status in making employment decisions, particularly where fitness for duty is a work issue; and to what extent should government (particularly the federal government) regulate the business of insurance, which is dependent on the ability to assess and manage health claims risk).
- May be more difficult than enacting specific standards governing use of information in a range of other contexts; even if anti-discrimination legislation could be enacted, it wouldn't necessarily resolve all privacy concerns.

2. Lack of a Federal Breach Notification Standard

Prior to passage of ARRA, there was no federal law requiring that individuals be notified if their personal health information is breached – *i.e.*, inadvertently disclosed to or accessed by the public or persons or entities not authorized to see it. A number of states have enacted laws requiring persons to be notified if their personal data is breached. Only three of these laws explicitly apply to identifiable health information,[34] but some general state breach notification laws may be interpreted to apply to health information.[35] As a result, individuals only had a right to be notified if their personal health information is inappropriately accessed or disclosed if they happened to live in a state with an applicable law, or if their information was breached by an organization that voluntarily provides breach notification as part of its risk mitigation practices. Receiving notice of health data breaches gives individuals an opportunity to prepare or to try to minimize any potential damage (if possible). A breach notification requirement also arguably provides incentives for holders of health data to take the strongest measures possible to protect against breach.

Possible Solutions

Sections 13402 and 13407 of ARRA establish a federal breach notification law that applies to entities covered by HIPAA and vendors of personal health records and other Internet-based health entities.

- ✓ Establish a federal breach notification law that applies to identifiable health information. **(arguably accomplished in ARRA)**

Arguments For

- Establishes a national right of individuals to be notified if health information is breached and establishes national consensus on what constitutes a breach.
- Enactment of a strong federal standard could help facilitate stakeholder agreement for preemption of state health information breach notification laws, which would provide a more consistent policy environment for organizations that operate nationwide.

- Could be done by regulation (modification to the Privacy Rule) with respect to covered entities.

Arguments Against

- Could be difficult to come to consensus on the trigger for breach notification. However, without such a standard, consumers could be inundated with alerts about data breaches that do not involve their information, where there is little chance data recipients could access their personal information, or that the breach would be used to harm them. California, for example, imposes a strict liability standard – requiring notification except in cases where the data is encrypted. Other states follow a harm-based standard – requiring notification only if the individual suffers some type of harm. Consumer advocates argue that defining "harm" with respect to breaches of personal health information requires a standard beyond financial harm, such as discrimination, stigma, or embarrassment. Data holders may find it difficult to determine whether or not a particular breach rises to this standard; consumers may not trust data holders to appropriately make this determination on their behalf.
- If requirement applies only to covered entities, it leaves out many organizations and institutions that hold or manage personal health information, including: HIPAA business associates (who could be required in regulation to notify the covered entity of any breach); PHRs offered by non-HIPAA covered entities; and Internet health sites that collect personal health information. Imposing a requirement to notify individuals of breaches on these entities would require a law of broader application, which may be more difficult to enact.

✓ Status quo (*i.e.*, leave for states to address or to market forces).

Arguments For

- Companies will develop more innovative technologies for protecting information if they compete based on their privacy and security policies and practices, including those dealing with breach notification.
- It is not clear that that this is a new issue raised by the movement to electronic records, which suggests it is not something that needs to be addressed at this time.

Arguments Against

- It is unclear that this is something the market alone will fix. Entities holding health information would likely come to different conclusions as to whether or not it is necessary to notify in the event of a breach.
- Breaches of greater volumes of records are more likely to occur as we store and move information electronically. Failure to address this issue creates an obstacle to building trust in e-health systems.
- Relying on states is unlikely to achieve protection for all patients.
- Continuing to leave this to state law exacerbates the inconsistent policy environment for health care entities that operate nationally or across state lines.

3. Need for Data Stripped of Patient Identifiers for a Range of Health Purposes

The major health reform proposals all require the robust collection of health data for a number of purposes, including: measuring provider performance; determining whether particular treatments

are effective; monitoring health data for safety signals with respect to new drugs and devices; health research; public health surveillance and bioterrorism; and for commercial purposes (for example, determining how often providers are prescribing a particular drug product). The Privacy Rule permits the use or disclosure of identifiable information for some of these purposes, including: quality assessment and improvement activities; public health reporting; and for health care operations such as the credentialing and licensing of health care professionals. However, some of these activities occur now with the use of information stripped of patient identifiers, and some privacy advocates have begun calling for increased use of data stripped of patient identifiers in lieu of using fully identifiable information where it is possible to do so and still accomplish the purpose for which the data was legitimately accessed.

The Privacy Rule includes two ways that covered entities may use or disclose data stripped of patient identifiers: de-identification and the limited data set. Data that qualifies as "de-identified" is not protected by the provisions of the Rule, and therefore there are no limits on how such data can be used and to whom it can be disclosed.

Data can qualify as "de-identified" in one of two ways. Under what is known as the statistical method, an expert must determine that the "risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information."[36] The alternative method (often referred to as the "safe harbor") requires that the covered entity strip out a number of specific data points, including name, address, identifying numbers, and biometric data.[37] In addition, the covered entity releasing the data must have no actual knowledge, or reasonable basis to believe, that the information can be easily re-identified.[38]

A limited data set is information stripped of a number of the same specific data points as required for the de-identification safe harbor.[39] Covered entities may release a limited data set only for purposes of research, public health, and health care operations, and must execute a data use agreement with the entity receiving the data set that sets forth the permitted uses and disclosures of the data and that does not authorize use or disclosure in contravention of the provisions of the Privacy Rule.[40]

Some believe the current de-identification and limited data set provisions raise a number of concerns:

- The de-identification safe harbor standard is now more than five years old, and today there is much greater access to information via public databases (a development that will only increase in the future). It may now be easier to re-identify data,[41] and some have called for an update to the standard, or at least an examination of whether it is as effective as it was when first enacted. Others have questioned whether it remains good public policy to allow data that fits the de-identification standard to remain uncovered by the Privacy Rule.

- Limited data set users must commit to not re-identifying the data, and covered entities may only release de-identified data if it meets the standard, which is supposed to ensure a very low risk of re-identification. But if data is re-identified, either by limited data set recipients or by holders of de-identified data, the ability to hold those persons or entities accountable is very limited. In the case of a limited data set, the data holder is only

contractually obligated to the covered entity not to re-identify; a covered entity can be held responsible for the actions of the data set recipient if 1) the entity knew of a "pattern or practice" that constituted a material breach or a violation of the data use agreement and 2) the covered entity took no action.[42] With fully de-identified data, the information can be shared with non-covered entities and does not require the execution of a contract – thus there are no applicable legal prohibitions against, or penalties for, re-identification, and such prohibitions are not required to be imposed on the data recipient via contract (although nothing in the law prevents data holders from voluntarily imposing such a condition).

- Researchers and others, including people with rare or chronic illnesses, are concerned that the limited data set and de-identification standards – in particular, the provisions that require the elimination of specific data points – make the data unusable for many research and public health purposes. They would prefer some middle ground, where the data is stripped of those identifiers that can be easily used to re-identify (such as name, full address, and identifying numbers) but a sufficient amount of data is retained to accomplish the purposes for which the data is sought.

Possible Solutions

Section 13424 of ARRA requires HHS to study the current HIPAA de-identification provisions. Section 13405 requires the Secretary to establish guidance on the "minimum necessary" standard, which must be followed for access, use, and disclosure of personal health information for most purposes other than treatment. Until such guidance is issued, covered entities and their business associates are directed to use a limited data set to meet the minimum necessary standard if doing so is "practicable."

✓ HHS should seek the input of experts and the public and examine the de-identification safe harbor to determine if it is still robust enough to provide a very low risk of re-identification, and make any appropriate revisions to the Rule. **(arguably accomplished in ARRA)**

Arguments For

- Allows for a public process for re-examining the standard and helps ensure that any changes to the standard are based on the latest science.
- The House bills each had provisions tasking HHS to examine the de-identification standard, indicating some support for such an initiative.

Arguments Against

- Because the current standard requires data holders to have no "reasonable basis" for believing the de-identified data could be used to identify an individual (and no actual knowledge that the information could be re-identified), the standard is already flexible and robust enough.

✓ Create more options for use of health data stripped of some individual identifiers, and require data use agreements for all data disclosures (or at least all that do not meet the threshold of full de-identification). **(steps to accomplish taken in ARRA)**

Arguments For

- Could address concerns raised by some that the current options do not serve many legitimate needs for data stripped of some patient identifiers.
- Could help entities use such "lesser identified" data for activities that today use fully identifiable data (for example, many of the activities covered by health care operations and some research).
- Helps ensure that all data recipients are held accountable.

Arguments Against

- Policymakers will face a difficult task in determining the permitted uses of various new data set options. Could result in an environment that is either less protective or overly stringent compared to the one that exists today.
- Requiring data use agreements for *all* disclosures can be a cumbersome process with little relation to privacy protections.
- Requiring such agreements could obstruct the flow of information for public health reporting, syndromic surveillance, bioterrorism detection, and other important public purposes.
- Data recipients are only held accountable by the terms of their contracts.

✓ At a minimum, require those who obtain data stripped of patient identifiers to commit to not re-identifying the data, except in specific circumstances (for example, notifications about a serious public health threat or drug safety/recall notifications).

Arguments For

- Attacks the key concern with respect to the use of data stripped of patient identifiers without the perceived risks associated with a more comprehensive re-opening of the Rule or the de-identification standard.

Arguments Against

- The arguments above apply here. Most likely, this is possible only through a data use agreement, and currently such agreements are not required when information is de-identified.

4. Prohibitions on Use of Personal Information for Marketing Purposes

Among consumer views on health information privacy, use of their personal information for marketing purposes ranks among the top concerns. For example, in a 2006 survey asking Americans about the benefits of and concerns about online health information, 77% reported being "very concerned" about their information being used for marketing purposes.[43] The HIPAA Privacy Rule governs a covered entity's use of an individual's health information for marketing purposes, but there are no rules regarding use of health information for marketing purposes by entities not covered by the Rule. With respect to information in personal health records, or voluntarily shared on Internet health sites, use for marketing purposes will be governed by whether the HIPAA Privacy Rule requirements apply, the vendor's or site's terms of use or privacy policy, or what individuals may knowingly or inadvertently authorize.

The Privacy Rule prohibits covered entities from using a person's identifiable information for marketing purposes without his or her prior authorization. The definition of what constitutes

"marketing" is a communication about a product or service that encourages the recipient to purchase or use that product or service.[44] The definition includes a number of exceptions that were crafted to allow covered entities to send important health-related communications to their patients and enrollees without having to first obtain individual authorization. For example, covered entities may use personal information to communicate with an individual about his or her treatment; for case management or care coordination, or to recommend alternative therapies, providers, or settings of care; or to describe products or services in a benefits plan or value-added services available only to plan enrollees.[45] Individuals whose personal information is used to make a communication exempt from the marketing rule also do not have the right to object to (or opt out of) their personal information being used for these purposes.[46]

The Privacy Rule prohibits a covered entity from selling (without authorization) protected health information about its patients or enrollees to outside entities so that those entities can directly market their products and services. However, such outside entities could pay the covered entity to use protected health information to make those communications – and as long as those communications fell under one of the exceptions to the marketing definition, authorization would not be required. Some see this as a loophole, enabling outside entities to pay covered entities to send targeted marketing communications that the entities could not send themselves without express individual authorization. Others believe the rule strikes the right balance – ensuring that protected health information remains with the covered entity (or its business associate), and allowing beneficial communications to be sent to patients and enrollees without having to ask first for patient authorization (which under the Privacy Rule must be fairly detailed).

The polling data is clear that individuals feel strongly about the use of their information without their consent for marketing purposes. There does not appear to be consensus, however, on whether the marketing provisions in the Privacy Rule need to be revised in order to build trust in e-health systems. Some claim that direct marketing to individuals helps drive up the cost of care; others point to communications that can help lower costs and ensure individuals get appropriate care (such as communications to facilitate medication adherence, or about lower-cost therapeutic alternatives or free or low-cost prevention services).

Policymakers have not yet begun to address concerns about the use of personal health information in PHRs and on Internet sites for marketing purposes.

Possible Solutions

Section 13406 of ARRA revises the HIPAA marketing rule to require prior authorization when an individual's protected health information will be used to make a communication that is paid for (directly or indirectly) by an outside entity. Exceptions include: communications about drugs or biologics that are currently prescribed for, or administered to, an individual - as long as the payment from the outside entity is reasonable in amount. The provision also makes an exception for remuneration that constitutes payment for treatment of an individual. Other related ARRA provisions include: Section 13406, requiring covered entities to allow individuals to opt-out of receiving fundraising communications; and Section 13405, prohibiting the direct or indirect receipt of remuneration in exchange for an individual's protected health information.

- ✓ Strengthen HIPAA rules requiring prior authorization for use of personal information for marketing by covered entities and establish rules for use of information for marketing purposes by non-covered entities. **(at least partially addressed in ARRA)**

  Arguments For
  - o Attacks a key concern of the public with respect to uses of their health information. Could be structured in a way that permits some targeted communication with patients for legitimate health purposes but without creating loopholes that end up permitting the use of personal information for the purpose of marketing a broad range of health-related products and services.
  - o Could be accomplished by regulatory change with respect to marketing by covered entities and their business associates.

  Arguments Against
  - o Would require legislation for non-covered entities.
  - o Drawing the line between "good marketing" – using individuals' information to send communications that clearly advance their health or health care – and "commercial marketing" – where the communication is arguably related to health but where the benefit to the individual is less clear or is secondary to the commercial interests of the entity sponsoring the communication – can be difficult. There also are stakeholders either firmly committed to preserving the status quo or concerned that any changes could have unintended consequences for patient health or health care business operations.
  - o There could be negative health consequences for individuals (*e.g.*, no or less information about available benefits, treatment alternatives, etc.).

- ✓ Increase compliance with the Privacy Rule's current provisions by issuing additional guidance about the types of communications that are or are not "marketing."

  Arguments For
  - o Does not require amendment to the Rule (although could be done in conjunction with amending the Rule to enhance understanding of the Rule's provisions and improve compliance).
  - o Could result in more communications, which today are allowable under different interpretations of the marketing exemptions, being deemed to be "marketing" and therefore requiring prior authorization.
  - o Would continue to allow essential communications to individuals that directly impact their health, care, and outcomes.

  Arguments Against
  - o Depending on the content of the guidance, could inadvertently bless more marketing uses without patient authorization than occur today.
  - o Because it preserves the perceived inadequacies in the current Rule, unclear how well such an initiative would build consumer trust.

- ✓ Leave Rule as is for current covered entities but set more stringent rules for use of information for marketing purposes by health information exchanges, and adopt rules governing marketing uses by PHRs and Internet health sites.

Arguments For

- Avoids more difficult re-negotiation of the Rule for current actors and instead targets new challenges raised by e-health.
- Challenge of finding a viable business model for electronic exchange networks – and potentially PHRs – makes the information held in or exchanged through these vehicles a potentially attractive target for marketers, strengthening the case for targeting this area for strong regulation.

Arguments Against

- Does not address what some perceive to be deficiencies in the Rule today (for example, the use of protected health information without prior patient authorization by covered entities to send communications that are paid for by an outside company and that encourage the patient to use that company's goods and services).
- Depending on the terms of the specific rule, could potentially cut off a source of operating revenue for these exchanges.

✓ Change Rule from the current "opt-in (but with exceptions)" approach to instead allow individuals to opt-out of receiving all marketing communications, including those that today are exempt from the definition of marketing. **(at least partially addressed in ARRA)**

Arguments For

- Could be easier to implement without the need to determine which communications are "good" (and thus should be permitted without authorization) and which should first require explicit patient permission.
- Assumes patients want to receive these communications but empowers patients to stop them if they object.
- In a variation, could also retain the authorization requirement for communications that qualify under the current marketing definition (thus, permitting opt-out for those communications that are currently exempt from the definition but that consumers could still view as marketing).

Arguments Against

- Places burden on individual to police how their information is and isn't used – clear boundaries on use of information provide more reliable protections for privacy.
- Arguably less protective than current rule, which requires authorization to use information for marketing with some exceptions (unless authorization requirement is retained for those uses that currently qualify as marketing).
- Stifles needed information for individuals and could result in negative health outcomes.

✓ Leave current Rule as is; allow non-HIPAA covered entities to compete on the basis of their policies with respect to use of information for marketing purposes (HIPAA-covered entities could also voluntarily implement more stringent controls on uses of information for marketing purposes, and compete on that basis).

Arguments For

- Does not require changes to current law.

- Could lead to more privacy-protective environment if robust "privacy competition" emerges.

Arguments Against

- Few individuals know the extent to which their information is used to market or make health-related communications to them. Thus, they may be unlikely to inquire or make decisions based on use of their information for these purposes. This may be particularly true in a health care context, where choice of care provider involves a myriad of important variables – and where many individuals do not have choices (or a wide range of choices) with respect to their sources of care.
- Unless the policy is clearly articulated, explanations of uses of information in a privacy policy may not be clear. A clear policy could explicitly state, in part: "we do not use your information to recommend products or services to you under any circumstances".

5. Other Areas where HIPAA Could be Strengthened

As personal health information is accessed and exchanged more easily in the new electronic environment, HIPAA policies regarding access to, and use and disclosure of, health information may be inadequate and contribute to a lack of public trust in health IT and health information exchange. Some of these issues are new ones raised by the new e-health environment, while others were initially raised during the HIPAA regulatory debates and may or may not be exacerbated by the new information sharing models. In the past year policymakers have considered addressing the following:

- Uncertainty regarding how to apply the "minimum necessary" standard. Under the Privacy Rule, access to, and uses and disclosures of, personal health information must be limited to the minimum necessary to accomplish the legitimate purpose for accessing the information, except with respect to treatment.[47] This standard was intended to be flexible in order to accommodate a broad range of circumstances, but the lack of clear boundaries has resulted in a great deal of confusion about how to comply.[48] Some believe further guidance on the minimum necessary standard could help resolve this uncertainty. (**As noted on page 16, ARRA requires the Secretary to issue guidance on the minimum necessary standard and strongly encourages the use of a limited data set.)**

- Perception among some privacy and patient advocates that "health care operations" permits too much sharing of personal health information. Under the Privacy Rule, "health care operations" is specifically defined. However, a number of the descriptions are very broad and permit use and disclosure of personal health information for functions that could be achieved without patient identifiers or could be done only with the consent or authorization of the patient. For example, health care operations include activities such as: conducting quality assessment and improvement activities; reviewing the competence or qualifications of health care professionals; underwriting and premium rating; auditing; and business management and general administrative activities - such as due diligence related to a merger, customer service functions, and fundraising for the benefit of the covered entity (see Appendix B for a complete list). The Privacy Rule also permits covered entities to share health information with another covered entity for the

purpose of the recipient entities' health care operations, as long as both entities have a relationship with the patient.[49]

- The PRO(TECH)T Act of 2008 would have required patient consent (not authorization) for health care operations uses. A number of stakeholders expressed concern that this provision would significantly stifle uses of health care information for important purposes like public health and quality measurement; others noted that because treatment and coverage could be conditioned on patients giving their consent to health care operations uses, it would provide little meaningful privacy protection. The Health-e Technology Act of 2008 took a different approach, tasking HHS to examine the definition of health care operations and determine which functions could be performed with de-identified data and which should require prior authorization.

- Uncertainty regarding which Privacy Rule provisions should apply to health information exchanges. As noted above, the Privacy Rule historically has not applied to health information exchanges (for example, RHIOs, HIEs, and ePrescribing Gateways), except those that may qualify as healthcare clearinghouses. Many of these entities have executed business associate agreements with the covered entities that participate in the exchange. However, it is not clear that all have done so, which has prompted some to call for a requirement that these exchanges either be covered entities or enter into business associate agreements (depending on their structure and function). (**As noted above, ARRA clarifies that some of these entities must enter into business associate agreements.)**

  But securing coverage under HIPAA, either directly or as a business associate, only addresses part of the question. Once covered, policymakers need to determine the data access, use, and disclosure rules that will apply to these new entities. For example, should a person's identifiable health information be used in these exchanges only for treatment of the individual, or can it be accessed to treat another individual? Under the Privacy Rule today, covered entities can use one patient's identifiable information for treating another patient.[50] This permissive use raises privacy concerns, particularly when data on any patient can be accessed across multiple institutions and providers participating in a network. Should exchanges be accessible for payment purposes, or to accomplish health care operations? Should exchanges exist only to facilitate the health care activities of the covered entities participating in the exchange, or should the exchange itself be permitted to use data for its own purposes? What if some of the entities providing support for and participating in the exchange are not themselves covered by HIPAA? In the absence of clear rules, health exchanges are working out the rules of the road on their own, often with multi-stakeholder involvement. There has been no objective study of the results to date.

- Confusion regarding whether quality improvement uses of identifiable health information is a health care operation (not requiring patient consent) or research, which requires authorization except in certain circumstances. As noted multiple times throughout this paper, health reform proposals are looking to health IT as the linchpin for providing the data that will help improve quality of care. The Privacy Rule permits the use of identifiable health information without patient consent for "quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines" – as long as "obtaining generalizable knowledge is not the primary purpose

of any studies resulting from those activities."[51] The Privacy Rule also permits the use of identifiable information without patient consent for population-based activities relating to improving health or reducing health care costs, and protocol development.[52] Separate provisions of the Privacy Rule permit covered entities to use and disclose identifiable information for research purposes; such research requires specific authorization from the patient unless an IRB or Privacy Board waives the requirement based on the low risk to patient privacy.[53] (As noted above, use of de-identified data or a limited data set for research purposes is also permitted and in most cases will not require prior patient authorization.) Confusion about which provision applies to what types of quality improvement activities could hinder efforts to implement more robust measurement and other quality improvement efforts. (**Some have expressed concerns about the possible negative impact of ARRA's prohibition (13405) on the receipt of remuneration for protected health information on uses of data for research and public health.)**

- Inability to meaningfully restrict access to and disclosure of health information. Under the Privacy Rule, individuals have a right to request a restriction on the use and disclosure of their health information – but covered entities are neither required to comply with the request, nor provide a reason for noncompliance.[54] If a covered entity grants the request, however, it must comply. Some have advocated for granting a stronger right to restrict access to information, particularly with respect to information that is exchanged electronically through the "National Health Information Network" (NHIN). For example, NCVHS has recommended allowing people to choose whether or not their information is included in the NHIN, and to be able to restrict network access to data in certain sensitive categories.[55] In its recommendation regarding the right to restrict access to sensitive information, NCVHS acknowledged that few individuals would likely make such a request; but noted that individuals would strongly value the right and ability to do so.[56] (**Section 13405 of ARRA gives individuals a right to request a restriction on disclosures to health plans for payment and health care operations when they pay for their care out-of-pocket in full).**

  Technology may improve the ability for health data holders to segregate sensitive data and comply with a patient request to restrict data access. However, if compliance with such a restriction is mandatory, providers, plans and other health data holders will likely seek to be held harmless for inadvertent access and disclosure of information in contravention of a patient's requested restriction, as long as the holders used reasonable efforts to comply. NCVHS also recognized that providers should be notified if a patient has decided to sequester or restrict access to information in a sensitive category, but they left for further discussion how this notification would take place.[57] Further, a requirement that applies only to those with electronic records risks creating disincentives for providers and others to move from paper to electronic systems.

- Uncertainty over patients' rights to access their records electronically, or receive an electronic copy. The effort to engage more individuals in their health care through the use of consumer-facing electronic tools such as PHRs will not be successful if individuals cannot easily and promptly obtain electronic access to, or electronic copies of, their health records. Under the Privacy Rule, patients have the right to access, and obtain a copy of, their health information in the form or format requested, "if it is readily producible in that form or format."[58] Some believe that this language already obligates providers and plans with electronic health records to provide an electronic copy of the

record. Anecdotal reports, however, suggest that providers are not clear on their obligations and that patients have had difficulty obtaining copies of their health records in electronic format, in part because not all electronic health record applications facilitate the easy production of electronic copies. In general, difficulty in obtaining a copy of one's record, even in paper format, is the one of the top five HIPAA complaints investigated by OCR.[59] Also, some believe that the timeframe for responding to a records request – which is at least 30 days under the current Rule[60] – should be shortened when those records are kept electronically, and that the cost to consumers of obtaining an electronic copy should be free or set at a level more commensurate with the costs of making electronic an electronic copy available. Under the current Rule, such costs are required to be "reasonable" and "cost-based";[61] however, most states set limits on copying charges for medical records, which range from free (Kentucky) to $37.00 for up to the first 10 pages of a hospital record (Texas).[62] **(Section 13405 of ARRA requires covered entities using "electronic health records" (a defined term in ARRA) to provide individuals with an electronic copy. Any fee charged for this electronic copy cannot exceed the entity's labor costs in responding to the request. Individuals can have their electronic copy transmitted to another person or entity, as long as their choice is "clear, conspicuous, and specific".)**

- Controversy over the appropriate role for patient consent or authorization. The Privacy Rule permits the gathering and sharing of information for a range of purposes without the need to first obtain the patient's consent. For uses and disclosures not specifically permitted under the Privacy Rule, a patient's specific written authorization is required. An earlier version of the Rule would have required patient consent for treatment, payment, and health care operations; but providers and plans could have conditioned treatment or coverage on obtaining patient consent for these routine uses of their information.[63] However, this version was harshly criticized by the health care industry, who argued that the requirements would hinder the delivery of treatment, the processing of payments, and other routine activities by requiring consent to be obtained over and over again.[64] In response, HHS amended this version in 2002 before it went into effect and replaced it with the structure that is in place today: permissive use of information for certain routine health purposes: authorization required for uses and disclosures not specifically enumerated in the Rule; and plans and providers may not condition providing coverage or treatment on the patient's execution of such an authorization.[65] A number of privacy advocates harshly criticized the amendment, and some continue to call for restoration of the earlier version requiring consent for nearly all uses and disclosures of health information.[66] Others note that such consent could not possibly be voluntary, and that overreliance on consent unfairly shifts the burden for protecting privacy to individuals and not to the organizations holding the data.[67] Some entities would not likely support such a proposal, as requiring individual consent for routine health care functions could stifle necessary payment and other important processes.

  Also relevant is whether there should be an enhanced role for patient choice with respect to whether or not health information is included in an electronic exchange network. Exchange networks across the country are considering, and some have begun to implement, consent policies that require people to opt-in to, or allow them to opt-out of, sharing their health information through an exchange network either in whole or in part (such as by provider or by type of information).[68] In general, those networks must

balance the extent to which providing consumers with meaningful choice about having their personal information exchanged in a local, state, or national network increases patient trust and values individual autonomy against the consequences both for individuals and for the system of having potentially incomplete data available for treatment decisions and public health. As noted above, NCVHS has recommended that individuals at least have the right to opt-out of information sharing through the NHIN.[69] Additionally, the Markle Foundation's Common Framework released in 2006 - Resources for Implementing Private and Secure Health Information Exchanges, recommends giving patients control by allowing them to create a second or third identity for records they want to keep out of networked electronic records exchanges.[70] Although a number of sources have begun informally tracking the policies of various exchanges throughout the country, there has been no systematic study of the impact of the various policy models being adopted.

Possible Solutions

- ✓ HHS could issue more guidance on how to comply with the Privacy Rule. (**As noted on page 16, ARRA directs the Secretary to issue guidance on the minimum necessary standard.)**

  Arguments For
  - o A common sense and prompt way to address a number of the above issues, including: confusion regarding the minimum necessary rule; which quality measurement/improvement activities are permitted without consent as health care operations and which constitute research and require authorization absent a waiver; and the obligation of covered entities to provide individuals with electronic copies of their health records.
  - o Could be combined with a new system whereby stakeholders, without penalty, can ask the Office of Civil Rights (OCR) to publicly opine on whether certain proposed health information uses or disclosures are in compliance with the Rule.

  Arguments Against
  - o OCR is already under-resourced, and without a resource increase may not be able to issue guidance promptly and on as broad a range of topics as desirable. Also probably not possible without more resources to institute any new program to publicly issue specific responses to stakeholder questions.
  - o Guidance alone may not be sufficient to address all of the concerns raised above.

- ✓ HHS could examine the health care operations definition and issue new regulations that limit the use of identifiable data without consent. The regulations could require more of the current health care operations to be done with data stripped of some patient identifiers, or could potentially require authorization for some uses that today are permitted without consent. Another possible option is for HHS to issue guidance on the "minimum necessary" standard that encompasses both the extent of data accessed, as well as the extent of "identifiability" of the data, for health care operations purposes. **(partially accomplished in ARRA)**

Arguments For

- Addresses directly one of the biggest concerns that privacy advocates have with the Privacy Rule.
- Outcome could enhance privacy while still allowing the use of data for a range of operational purposes.

Arguments Against

- Health care industry has five years of experience working with HIPAA and will be concerned about not being permitted to use identifiable data for the same broad range of purposes as is permitted today. A possible compromise could be to allow use of identifiable data only for an entity's own health care operations, whether performed by the entity itself or a business associate on its behalf. However, this compromise may not be feasible in a more interconnected health system.
- Because of the significant interests involved, could be difficult to achieve, even in a regulatory context.
- Requiring the use of data stripped of patient identifiers for routine operations could increase health care costs. Additionally, as many health care operations are closely linked to treatment and payment functions, delays may result in information sharing for these purposes as well as for health care operations that help facilitate quality improvement efforts.
- Could result in broad requirements that negatively impact essential health care operations such as quality improvement programs.

✓ HHS could issue new regulations regarding the terms of access to health information exchanges, including defining minimum standards for consumer choice.

Arguments For

- For states currently establishing exchanges, a clear set of baseline rules could clarify the difficulty of trying to achieve a mutual agreement among stakeholders.
- Public trust will be enhanced if these entities are subject to enforceable rules about how they can and cannot use health information.

Arguments Against

- It is too early to establish rules to govern the behavior of these exchanges. Premature regulation may stifle local variation and innovation. (Note that, in the alternative, exchanges could at least be required to adopt policies that are consistent with a health fair information practices models such as the Markle Common Framework).
- Viable business models for long-term operation of these exchanges have yet to be established and regulating too stringently or early in this space could jeopardize their implementation.

✓ Filling gaps in HIPAA and establishing privacy protections that go beyond the HIPAA floor could occur through voluntary adherence to best practices or certification.

Arguments For

- Such an approach is consistent with the HIPAA model, which provides a baseline floor of standards and allows for states to adopt more stringent laws and for the private sector to voluntarily promote and adopt more stringent privacy protections.

- Likely easier to accomplish than regulatory or legislative change.
- May be more cost-effective than imposing through a top-down regulatory approach.

Arguments Against

- Patients care about their health information privacy, but often don't make health care decisions based on an institution's privacy policies, as noted above. There will be few (if any) market incentives for enhancing privacy, thus there is a strong role for public policy to play.
- Voluntary adoption of best practices and certification is less likely to achieve broad-based adoption of stronger privacy protection.
- Certification, which typically occurs only in time intervals, may be inappropriate for ensuring adequate protections for privacy. For example, a health IT product may be certified to include certain functionalities that are privacy-enhancing, such as role-based access and audit trails. But if these functions are not being consistently used, or if the entity is not monitoring compliance (or being actively monitored for compliance), certification does little to enhance privacy protection.

C. State Law Variation

As noted above, because HIPAA was structured to provide a floor of protections, state laws providing more stringent protections for health information are expressly preserved. Movement towards an interconnected national health information network raises concerns that the multiplicity of state privacy laws will create an obstacle to the nationwide electronic exchange of health information or the exchange of information regionally across state lines. Others have noted the difficulty in determining a particular state's health privacy laws, as they are often a combination of statute, regulation and guidance, customary practice, and common law.

Possible Solutions

- ✓ Establish a federal health privacy law that preempts all state health privacy laws. A possible alternative is to set a single federal standard that preempts existing state law (*i.e.*, "wipes the slate clean"), but allow states to pass new laws establishing stronger privacy provisions (perhaps within a certain window of time).

Arguments For

- Should eliminate confusion and create a more consistent policy environment for privacy and nationwide electronic health information exchange.
- Makes more sense in a health care arena increasingly dominated by multi-state players.
- The alternative approach preserves the ability for states to re-enact those privacy provisions they deem to be most important while making it easier for cross-state actors to understand and comply with relevant laws (because there will likely be fewer of them).

Arguments Against

- Congress intended the HIPAA Privacy Rule to provide a floor of protections – not a ceiling. Thus, if the single national standard is the set of current HIPAA rules, some

stakeholders will fight any attempts to decrease privacy protections for individuals living in states with laws that are currently stronger than HIPAA.
  - The more stringent state laws typically cover more sensitive health information, such as mental health, sexually transmitted diseases, or HIV/AIDS. Efforts to eliminate these protections will be opposed by their constituencies and could erode public trust.
  - Another alternative is to create a national standard that is greater than HIPAA (perhaps using the states with the most expansive privacy protections as model) – but this may be opposed by industry stakeholders, particularly those whose business operations are primarily in states with less stringent privacy laws.
  - Many of the state protections for health data were enacted as part of state public health reporting statutes – so eliminating the protections could inadvertently jeopardize the reporting provisions.

- ✓ Status quo - federal standards are a floor, with states able to adopt more protective measures. Arguments for and against this option are the reverse of those for the above option.

D. Improving Understanding of and Compliance with HIPAA Protections

As noted above in the introduction, confusion about the Privacy Rule persists, which often results in overly conservative interpretations of the Rule and a failure to share health information even for legitimate purposes. Some attribute this confusion to a lack of education about the substance of the Rule; others believe the Rule is too complex to be effective. In addition, privacy advocates express concerns about what they perceive to be a lack of aggressive enforcement of HIPAA. Others are concerned about oversight and enforcement over entities handling personal health information that are not covered by HIPAA. This section of the paper discusses these concerns in more detail.

1. Complexity of the Rule/Lack of Understanding

Possible Solutions

Section 13403 of ARRA requires HHS to develop and maintain a "multi-faceted national education initiative" to educate individuals on the uses of their health information and their privacy rights.

- ✓ Revise the Privacy Rule to make it less complex. For example, rely more on broadly worded fair information practices and principles and address detailed circumstances through guidance, model policies, etc.

  Arguments For
  - Increases the likelihood that patients and covered entities will understand their rights and obligations.
  - Provides more opportunities for innovative approaches to protecting privacy.

  Arguments Against
  - Industry has had five years to become accustomed to current law. Notwithstanding that some confusion persists, isn't it more disruptive to start over?

- Arguably will not result in a consistent set of baseline rules, and consumers will have to read and understand an entity's policies in order to get a clear picture of how well their health information is protected.
- Alternative is to task HHS with identifying those areas of the Rule that have been the largest sources of confusion and target those for simplification.

✓ Provide more guidance and better education on the requirements of the Rule to entities covered by it.

Arguments For

- More guidance and extensive education on the requirements of the Rules could help clear up any remaining areas of confusion.

Arguments Against

- There may not be resources at OCR to support an effective education program. Is OCR the ideal entity to conduct this education, or are there better alternatives (such as an OCR partnership with health industry trade associations)?
- Further, who would set the standards for such programs and is it possible to generate any measurable outcomes from them?

✓ Improve consumer education on HIPAA rights by requiring entities to provide a one-page summary privacy notice, written in plain English at average reading levels. This could be provided in addition to the more detailed notice; HHS could create models. **(partially accomplished in ARRA)**

Arguments For

- Ensures consumers are provided with a more digestible summary of the most important aspects of the Rule.
- The summary would be provided in addition to the more detailed notice, which would still be provided for patients who want to read more details.
- Is consistent with the "layered notice" approach recommended by privacy advocates.
- If models are developed and disseminated by HHS, notices will be more consistent. This also helps promote greater understanding of the law.

Arguments Against

- HHS has insufficient resources to accomplish this.
- It is already burdensome for covered entities to provide, and for patients to read, the extensive HIPAA privacy notice that is already required under the law – why should the response be to provide consumers with yet another summary of their rights?
- Consumers may not welcome yet another notice about their privacy rights.

2. Compliance with the Rule and Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for failure to comply with the statute, and these penalties applied to the subsequent privacy and security rules implemented years later. But whether the HIPAA rules are being adequately enforced is the subject of some debate among policymakers and stakeholders.

OCR has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[71] The Justice Department (DOJ) has levied some penalties under the criminal provisions of the statute, but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limits the application of the criminal provisions to covered entities and not to individuals working within or on behalf of those covered entities (except in cases where an individual's criminal behavior was actually sanctioned by the covered entity). [72] Although DOJ has prosecuted individuals for criminal HIPAA violations in at least two instances subsequent to the OLC opinion, some have argued that its release has had a chilling effect on HIPAA criminal enforcement.[73]

Congress tasked HHS and DOJ with enforcing HIPAA: HHS for civil enforcement and DOJ for criminal enforcement. Within HHS, OCR enforces the Privacy Rule, and the Centers for Medicare and Medicaid Services (CMS) enforces the Security Rule. State authorities may be able to enforce HIPAA if their state statutes authorize them to enforce federal consumer protection laws. Otherwise, state authorities can only enforce state health privacy laws.

Some privacy advocates believe that the failure of HHS to aggressively pursue civil monetary penalties sends a message to entities that they need not devote significant resources to compliance with the rules. They also argue that, without strong enforcement, even the strongest privacy and security protections are but an empty promise for patients. Privacy advocates also are concerned about HIPAA's failure to include a private right of action, which leaves consumers dependent on the federal government and without a way to be made whole for any harm due to HIPAA noncompliance.

Covered entities repeatedly express concern about protecting patient privacy and cite the potential irreversible damage to their reputations if patients lose confidence in their ability to protect personal health information. The covered entities believe this provides a powerful incentive for them to comply with the law. They argue that strengthening HIPAA's enforcement provisions would have the unintended consequence of stifling appropriate health information sharing, because entities could over interpret the Rule in an effort to *ensure* that they are not using or disclosing information in violation of the Rule or in contravention of a patient's right. They are worried that providing patients with a private right of action would have the same consequence and is more likely to profit attorneys than to provide a fair way of promptly compensating patients for any harm that results from failure of a covered entity to comply with HIPAA. In addition, some believe that an enforcement approach that seeks voluntary compliance from covered entities is a more effective method for actually achieving compliance with the requirements.

As discussed above in this paper, privacy advocates have also been concerned about the federal government's lack of authority before the passage of ARRA to hold business associates accountable for failure to comply with HIPAA. Instead, business associates could only be held accountable to the covered entities with which they contract for complying with the contract terms and any applicable HIPAA rules. OCR could only hold covered entities responsible for the actions of their business associates if an entity knew of a "pattern of activity or practice of the business associated that constituted a material breach or violation" of its contract and the entity did nothing to cure the breach or terminate the contract.[74] Of interest, if the covered entity decided that terminating the contract was "not feasible," the entity was required to report the problem to the Secretary. [75] However, HIPAA did not give the Secretary any further authority to

enforce the statute and regulations against the business associate or to hold the covered entity responsible for the violation. Entities serving in the role as business associates argue that contractual liability to the covered entity is sufficient to ensure enforcement of applicable HIPAA rules, as the business associate's business and public reputation is at stake if there is a failure to comply.

Some believe the enforcement provisions of the HIPAA statute are poorly worded and partly to blame for the current enforcement environment, while others attribute the Bush Administration's discretion with respect to enforcement priorities and a lack of sufficient enforcement resources as more significant factors. On the other hand, some industry stakeholders believe that the enforcement provisions in the statute and regulations provide sufficient and clear legal authority for enforcement of the rules, and that the combination of the law and non-legal penalties for failure to comply with HIPAA provides sufficient protection for consumers.

For entities not covered by HIPAA, enforcement depends on the particular health privacy law that applies. For example, the FTC can use its unfair and deceptive trade practices authority to penalize those companies that fail to abide by their privacy policies with respect to the personal health information they collect, manage, or store. Similarly, for those personal health record vendors subject to the Electronic Communications Protection Act, the Justice Department can impose criminal fines and penalties against entities that release personal health information without the individual record holder's authorization. Such entities may also be subject to state law claims.

Possible Solutions

ARRA contains a number of provisions addressing the enforcement issues raised above:

- **Section 13401 makes business associates directly accountable to authorities for complying with applicable HIPAA regulations.**
- **Section 13409 clarifies that HIPAA criminal penalties can be enforced against individuals.**
- **Section 13410 clarifies that HHS can pursue a HIPAA violation civilly when criminal penalties could apply but DOJ declines to prosecute.**
- **Section 13410 also requires HHS to impose civil monetary penalties in cases of willful neglect of HIPAA rules (and requires the Secretary to formally investigate any complaint where the facts indicate a possible violation due to willful neglect).**
- **Section 13410 increases the civil monetary penalties for HIPAA violations.**
- **Section 13410 authorizes State Attorneys General to enforce HIPAA.**
- **Section 13411 requires the Secretary to conduct periodic audits for compliance with HIPAA regulations.**
- **Section 13410 further requires that civil penalties or monetary settlements for HIPAA violations be transferred to HHS to be used for enforcement purposes. In addition, GAO is required to propose a methodology for providing individuals harmed by HIPAA violations with a percentage of any penalties or monetary settlements collected; the Secretary is required to implement such a methodology within three years of ARRA enactment.**
- **Section 13424 requires HHS to submit an annual report to Congress on enforcement.**

- ✓ Ensure that there is an enforcement regime to address entities not covered by HIPAA that are handling personal health information. **(at least partially addressed in ARRA)**

  Arguments For
  - o Enforcement is a critical part of fair information practices. Ensuring that non-HIPAA entities are subject to enforcement of either currently applicable standards or any new standards adopted by Congress and/or the new Administration should be a focus in 2009.

  Arguments Against
  - o Few will argue that some enforcement structure is needed to build public trust in these new health information exchange tools. It may be harder to agree on the details: what the standards are, who enforces, whether the penalty structure is appropriate, etc.

- ✓ Amend the HIPAA statutory enforcement provisions to clarify current enforcement authority. The amendments could require the Secretary to formally investigate and impose civil monetary penalties in cases of willful neglect of the HIPAA rules. Or, the provision could clearly state that the Secretary can pursue civil actions in cases where a criminal violation may have occurred but the Justice Department decides not to pursue the case. Finally, an amendment could correct the Office of Legal Counsel's interpretation of HIPAA with respect to the ability to pursue individuals who violate HIPAA's criminal provisions. **(addressed in ARRA)**

  Arguments For
  - o Arguably this is just a clarification of current enforcement authority, so it may not be as controversial (note that provisions accomplishing the above were part of the Health-e Information Technology Act of 2008).

  Arguments Against
  - o There is already sufficient statutory and regulatory authority to enforce HIPAA.
  - o Covered entities may oppose any effort to clarify statutory enforcement authority, viewing it as opening the door to more aggressive enforcement.

- ✓ Amend HIPAA to allow the Secretary of HHS to directly enforce the HIPAA regulations against business associates. **(addressed in ARRA)**

  Arguments For
  - o Closes an enforcement loophole and allows the federal government to directly hold business associates accountable for complying with HIPAA (provisions to accomplish this were in the House bills).
  - o Brings federal health privacy law closer to a data stewardship model (*i.e.*, all entities that handle personal health information have to comply with baseline standards and can be held legally accountable).

Arguments Against

- Will be vigorously opposed by entities who frequently act as business associates to covered entities. Could cause these entities to be unwilling to contract with health care entities out of fear of increased penalties. If these entities cease providing services, the cost of health care products and services could be affected.
- As an alternative, policymakers could make covered entities responsible for the actions of their business associates, which will generate vigorous opposition from covered entities who do not want to be legally responsible for behavior not in their control.

✓ Amend HIPAA to provide a private right of action for individuals to seek redress for HIPAA violations. **(at least partially addressed in ARRA)**

Arguments For

- Patients will not have to depend on the government's taking action when their privacy rights have been violated.
- Provides patients with a way to directly seek redress for privacy violations.

Arguments Against

- Will generate aggressive opposition, including from those promoting general tort reform. A possible alternative is to re-direct some or all of the civil monetary and criminal penalties collected to individuals whose privacy is violated. Provisions to eventually establish a method for distributing a percentage of civil monetary penalties to individuals harmed by HIPAA violations were included in the Health-e Information Technology Act of 2008.)
- Not clear that allowing individuals to sue to seek redress for privacy violations is the most effective or efficient way to improve enforcement of privacy protections or get individuals compensation for harm due to a HIPAA violation.
- Individuals are likely to be frustrated with such a cumbersome process. Litigation is time-consuming and expensive. Often, individuals are concerned with exercising their privacy rights under HIPAA (*e.g.*, access, amendment) and litigation is neither an efficient nor cost-effective way to provide immediate results or access.
- Increased costs from litigation expenses can affect overall health care costs for consumers.

✓ Expressly authorize state authorities to also enforce the federal HIPAA rules. **(addressed in ARRA)**

Arguments For

- There is precedent for doing this (see CAN-SPAM, which authorizes state attorneys general to enforce federal anti-spam provisions[76]).
- Devotes more resources to enforcement without a change to the current provisions.

Arguments Against

- Requires federal legislation to clearly authorize authorities in all states to enforce HIPAA.
- Likely controversial, as covered entities may be concerned about overly zealous state authorities and the possibility that legitimate data sharing will be thwarted because entities will be more cautious. Provisions were included in the as-introduced version

of Health-e Information Technology Act of 2008, but attempts to add such a provision to the PRO(TECH)T Act were unsuccessful because the provision did not have the support of all of the bill's primary co-sponsors.
- Potentially opens up the Privacy Rule to 50 different state interpretations.
- Presents an opportunity for duplicate fines for the same acts/offenses.
- Unclear whether this would result in better enforcement, as state authorities cannot be compelled to enforce federal law. As a result, only those state authorities with a strong desire to enforce HIPAA will likely take advantage of the provision.

✓ Status quo with respect to HIPAA enforcement provisions.

Arguments For
- There is no objective evidence that the current enforcement provisions are flawed. DOJ has pursued a handful of criminal violations, notwithstanding the OLC memo.
- The new Administration should and will set its own enforcement policies with respect to criminal and civil HIPAA violations.
- Covered entities will vigorously enforce the terms of their business associate contracts because it is in their best interests to do so, and business associates will use their best efforts to comply because it makes good business sense to do so.

Arguments Against
- Such an approach ignores the flaws in the statute, and the potential that the Obama Administration will have the same perceived difficulty as the Bush Administration in navigating them.
- Such an approach fails to address the frustration felt by consumers about the perceived lack of enforcement of the law.
- Such an approach leaves business associates with a free pass, creating an unlevel playing field.

Conclusion

Many believe more efficient sharing of accurate health information is a critical factor in improving health care quality for individual patients and for the nation as a whole. Health information technology provides the necessary infrastructure for creating the information-rich health care system we seek – but building the infrastructure is not enough. Consumers, providers, health plans, and other health system stakeholders will be reluctant to put information in the system if they don't trust that it will be protected. Privacy and security protections are essential to building this foundation of trust and allowing us to reap the benefits that health IT can provide.

For the most part, there is consensus that efforts to facilitate widespread adoption and use of health information technology must move forward with appropriate protections for privacy and security. However, achieving consensus on the details of what privacy and security measures need to be put in place continues to be a challenge. **The enactment of ARRA represents a new generation of health privacy – but implementation challenges remain to be addressed.**

The new Administration and new Congress present us with new opportunities to break the privacy "gridlock." Notwithstanding other critical national issues that need urgent attention, we

have never had a better opportunity to pursue reform of our health care system, facilitated by interoperable health IT with protections for privacy and security. Consistent with the goal of the Legal Solutions in Health Reform Project, this paper presents a range of possible solutions to privacy concerns that have been raised by some policymakers and stakeholders, along a few of the likely arguments for and against each. Hopefully, it will be a catalyst for continuing to make progress on this difficult issue.

APPENDIX A – List of Possible Solutions by Issue Category (issues addressed at least in part by ARRA are so designated)

Who is Covered - Do we extend the privacy rules under the Health Insurance Portability and Accountability Act (HIPAA) to all entities that now handle health information, or create new legal standards for entities not currently covered?

- ✓ Amend HIPAA to create new categories of covered entities and require OCR to promulgate new privacy regulations to cover the activities of these new entities.

- ✓ Clarify business associate agreements. Require (or encourage) HHS to issue new regulations or strengthen current guidance to ensure that entities receiving protected health information from a covered entity – such as exchanges or PHRs that offered by that entity– must enter into a business associate agreement or at least be contractually bound to safeguard the information and comply with HIPAA. (ARRA)

- ✓ Require any entity that holds or manages protected health information to adopt policies consistent with fair information practices, which is the model typically relied on to establish appropriate policies for handling personal information.

- ✓ Keep the law in its current state but encourage the adoption of good privacy practices through voluntary business agreements and/or certification.

What is Covered - What protections need to be in place? For example, do we rely on current HIPAA rules or are modifications needed either to address new challenges or because, in the view of some, the rules were insufficient from the start? Are these concerns best addressed through changes in statute or regulations, or is it best to police this nascent marketplace through business best practices (or a combination of both)?

Addressing Privacy Concerns Through Anti-Discrimination Laws

- ✓ Enact federal legislation prohibiting the use of personal health information in determining the terms and conditions of employment or health insurance coverage.

Lack of a Federal Breach Notification Standard

- ✓ Establish a federal breach notification law that applies to identifiable health information. (ARRA)
- ✓ Status quo (*i.e.*, leave for states address or to market forces).

Need for Data Stripped of Patient Identifiers for a Range of Health Purposes

- ✓ HHS could seek the input of experts and the public and examine the de-identification safe harbor. This could help determine if it is still robust enough to provide a very low risk of re-identification. If not, HHS could make any appropriate revisions to the Rule. (ARRA)
- ✓ Create more options for use of health data stripped of some individual identifiers, and require data use agreements for all data disclosures (or at least all that do not meet the threshold of full de-identification). (ARRA)
- ✓ At a minimum, require those who obtain data stripped of patient identifiers to commit to not re-identifying the data, except in specific circumstances (for example, such as notifications about a serious public health threat or drug safety/recall notifications)

Prohibitions on Use of Personal Information for Marketing Purposes

- ✓ Strengthen HIPAA rules for use of personal information for marketing by covered entities by requiring prior authorization in more circumstances. (ARRA) Establish rules for use of information for marketing purposes by non-covered entities.
- ✓ Increase compliance with the Privacy Rule's current provisions rule by issuing additional guidance about the types of communications that are or are not "marketing."
- ✓ Leave Rule as is for current covered entities but set more stringent rules for use of information for marketing purposes by health information exchanges, and adopt rules governing marketing uses by PHRs and Internet health sites.
- ✓ Change Rule to allow individuals to opt-out of receiving any marketing communications, including those that today are exempt from the definition of marketing. (ARRA with respect to fundraising by a covered entity)
- ✓ Leave current Rule as is and allow non-HIPAA covered entities to compete on the basis of their policies with respect to use of information for marketing purposes (HIPAA-covered entities could also voluntarily implement more stringent controls on uses of information for marketing purposes, and compete on that basis).

Other Areas Where HIPAA Could be Strengthened

- ✓ HHS could issue more guidance on how to comply with the Privacy Rule. (ARRA)
- ✓ HHS could examine the health care operations definition and issue new regulations that limit the use of identifiable data without consent, which require more of the current health care operations to be done with data stripped of some patient identifiers, and to potentially require authorization for some uses that today are permitted without consent. HHS could also issue guidance on the "minimum necessary" standard that encompasses both the extent of data accessed and the extent of "identifiability" of the data, for health care operations purposes. (ARRA)
- ✓ HHS should issue new regulations regarding the terms of access to health information exchanges, including defining minimum standards for consumer choice.
- ✓ Filling gaps in HIPAA and establishing privacy protections that go beyond the HIPAA floor through voluntary adherence to best practices or certification.

State Law Variation - Should we allow for some state law variation or establish federal standards that preempt the field?

- ✓ Establish a federal health privacy law that preempts all state health privacy laws.
- ✓ Status quo - federal standards are a floor, with states able to adopt more protective measures.

Improving Understanding of (and Compliance with) Privacy Protections: How do we ensure compliance and appropriate enforcement of privacy protections?

Complexity of the Rule/Lack of Understanding

- ✓ Revise the Privacy Rule to make it less complex. For example, the rule could rely on more on broadly worded fair information practices and principles and addressing detailed circumstances through guidance, model policies, etc.)

- ✓ Provide more guidance and better education on the requirements of the Rule to entities covered by it. (ARRA)
- ✓ Better educate consumers on their HIPAA rights by requiring entities to provide a one-page summary privacy notice, written in plain English at average reading levels. This could be provided in addition to the more detailed notice; HHS could come up with models.

Compliance with the Rule and Enforcement

- ✓ Ensure that there is an enforcement regime to address entities not covered by HIPAA that are handling personal health information. (ARRA)
- ✓ Amend the HIPAA statutory enforcement provisions to clarify current enforcement authority. For example, require the Secretary to formally investigate, and impose civil monetary penalties, in cases of willful neglect of the HIPAA rules; make it clear that the Secretary can pursue civil actions in cases where a criminal violation may have occurred but the Justice Department decides not to pursue the case; and correct the Office of Legal Counsel's interpretation of HIPAA with respect to the ability to pursue individuals who violate HIPAA's criminal provisions). (ARRA)
- ✓ Amend HIPAA to allow the Secretary of HHS to directly enforce the HIPAA regulations against business associates.(ARRA)
- ✓ Amend HIPAA to provide a private right of action for individuals to seek redress for HIPAA violations. (ARRA)
- ✓ Expressly authorize state authorities to also enforce the federal HIPAA rules. (ARRA)
- ✓ Status quo with respect to HIPAA enforcement provisions.

APPENDIX B – Health Care Operations (defined at 45 CFR 164.501)

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

* Deven McGraw, JD, LLM, MPH, is the Director of the Health Privacy Project at the Center for Democracy & Technology.

[1] Obama-Biden 2008, "Barack Obama and Joe Biden's Plan to Lower Health Care Costs and Ensure Affordable, Accessible Health Coverage for All," *available at* http://www.barackobama.com/pdf/issues/HealthCareFullPlan.pdf (last visited Dec. 29, 2008).

[2] Health08.org, Kaiser Family Foundation, 2008 Presidential Candidates: Health Care Issues Side-by-Side, *available at* http://www.health08.org/healthissues_sidebyside.cfm (last visited February 4, 2009).

[3] Public Law No. 111-5, The American Recovery and Reinvestment Act of 2009.

[4] Connecting for Health, Markle Foundation, "Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care," survey conducted by Lake Research Partners and American Viewpoint in November 2006 for the Markle Foundation's conference, *Connecting Americans to Their Health Care: Empowered Consumers, Personal Health Records and Emerging Technologies, available at* http://www.markle.org/downloadable_assets/research_doc_120706.pdf (last visited Dec. 29, 2008).

[5] There is a difference between "privacy" and "security." Although there are no universally accepted definitions of those terms, in general privacy refers to policies and practices that govern the access, use, and disclosure of personal health information, and security refers to the technological tools that are used to implement those policies.

[6] See J. Goldman, "Protecting Privacy to Improve Health Care," *Health Affairs*, 10, no. 6 (1998): 47-60, at 49; J. Goldman and Z. Hudson, California Healthcare Foundation, *Promoting Health/Protecting Privacy: A Primer* (January 1999), *available at* http://www.chcf.org/topics/view.cfm?itemID=12502 (last visited February 3, 2009).

[7] Harris Interactive, "Many U.S. Adults are Satisfied with Use of Their Personal Health Information," The Harris Poll #27 (March 26, 2007), *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=743 (last visited Dec. 29, 2008).

[8] L.S. Bishop et. al, California Healthcare Foundation, *National Consumer Health Privacy Survey 2005*, (November 2005), *available at* http://www.chcf.org/topics/view.cfm?itemID=115694 (last visited Dec. 29, 2008).

[9] This paper uses the term "personal health information" to refer generally to an individual's identifiable health information, and uses the term "protected health information" to refer to information expressly protected by HIPAA.

[10] Covered entities are health plans, health care clearinghouses, and most health care providers who submit health care claims electronically (specifically, those who transmit health information in electronic form for those transactions for which the Secretary has adopted standards (i.e., transaction code sets). See 45 C.F.R. § 160.102(a) (2007).

[11] Protected health information is individually identifiable health information that includes demographic information and "that 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; and that identifies the individual or "there is a reasonable basis to believe the information can be used to identify the individual." See 45 C.F.R. § 160.201 (2007) for the precise definition.

[12] Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. See 45 C.F.R. § 164.501 (2007).

[13] Payment includes activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and to furnish or obtain reimbursement for health care delivered to a patient. See 45 C.F.R. § 164.501 (2007).

[14] Health care operations include: conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and business management and general administrative activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. See Appendix A and 45 C.F.R. § 164.501 (2007).

[15] Social Security Act § 1178, 42. U.S.C. § 1320d-7 (2009); 45 C.F.R. § 160.203 (2007).

[16] K. Pollitz, Georgetown University Health Policy Institute, the Genetics and Public Policy Center at Johns Hopkins University, Summaries of the Genetic Information Nondiscrimination Act of 2008 (GINA). Public Law 110-28, Title 1: Health Insurance *available at* http://www.dnapolicy.org/resources/GINATitle1summary.pdf; Public law 110-233, Title II: Employment *available at* http://www.dnapolicy.org/resources/GINATitleIIsummary.pdf (last visited February 3, 2009).

[17] FERPA applies to health and other records in educational settings; part 2 applies to federally funded substance abuse treatment facilities; and the Privacy Act applies to federal facilities.

[18] See 18 U.S.C. §§ 2702 (a)(1)-(3) (2007).

[19] See 18 U.S.C. § 2701 (c)(1) (2007); see also 18 U.S.C. § 2702 (a)(2)(B) (2007).

[20] See L. L. Dimitropoulos, Agency for Healthcare Research and Quality, *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variations and Analysis of Solutions Report,* (July 2007): 3-8 – 3-9, *available at* http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_661882_0_0_18/AVAS.pdf, [hereinafter cited as "Privacy and Security Solutions". For an "Overzealous" interpretation of HIPAA, see J. Gross, "Keeping Patients' Details Private, Even from Kin," *New York Times*, July 3, 2007, *available at* http://www.nytimes.com/2007/07/03/health/policy/03hipaa.html?_r=1; see also S. H. Houser et al., "Assessing the Effects of the HIPAA Privacy Rule on the Release of Patient Information by Healthcare Facilities," *Perspectives in Health Information Management*, 4, no. 1 (spring 2007), *available at* http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2082070&tool=pmcentrez [hereinafter cited as "HIPAA Privacy Rule"] (which recommended additional clarification of HIPAA regulations, standardized instructions, and extensive training of healthcare workers).

[21] See HIPAA Privacy Rule, *supra* note 20.

[22] See M. K. Paasche-Orlow, et. al, "Notices of Privacy Practices: A Survey of the Health Insurance Portability and Accountability Act of 1996 Documents Presented to Patients at U.S. Hospitals," *Medical Care*, 43, No.6 (June 2005): 558-564; M. Hochhauser, "Why Patients Won't Understand Their HIPAA Privacy Notices" *Privacy Rights Clearinghouse*, (Apr. 10, 2003), *available at* http://www.privacyrights.org/ar/HIPAA-Readability.htm; M. C. Pollio, "The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding," *New York University Annual Survey of American Law*, 60 (2005): 579-620, at 593.

[23] A health care clearinghouse is "a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements", Social Security Act § 1171(2), 42. U.S.C. § 1320d (2009).

[24] 45 C.F.R. § 165.504(e)(2) (2007).

[25] *Id.*

[26] Those who meet the definition of a health care clearinghouse would be covered by HIPAA.

[27] See The HIPAA Privacy Rule and Health IT, Health Information Techonolgy, Deparment of Health and Human Services, *available at* http://www.hhs.gov/healthit/privacy/hipaa.html (last visited February 3, 2009).

[28] Personal health records offered by covered entities would be covered by the Privacy Rule.

[29] National Committee on Vital and Health Statistics (NCVHS) Reports and Recommendations, *Letter to the Secretary of the U.S. Department of Health and Human Services: Personal Health Record (PHR) Systems*, (September 9, 2005), *available at* http://ncvhs.hhs.gov/050909lt.htm (last visited February 4, 2009).

[30] See Center for Democracy and Technology, "Comprehensive Privacy and Security: Critical for Health Information Technology," (May 2008), *available at* http://www.cdt.org/healthprivacy/20080514HPframe.pdf (last visited February 3, 2009); see also *Promoting the Adoption and Use of Health Information Technology*: *Hearing Before the Sucomm. On Health of the H. Comm. on Ways and Means*, 110th Cong. (2008) (statement of Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology), *available at* http://cdt.org/testimony/20080724mcgraw.pdf.

[31] With respect to the leading bill in the Senate, the Wired for Health Care Quality Act (S.1693), the version marked up by the Health, Education, Labor and Pensions (HELP) Committee included a provision that would have subjected PHRs to coverage under HIPAA; however, a proposed amendment from Senator Leahy that was under serious consideration by bill sponsors would have stripped out this provision and replaced it a provision similar to those in the House bills.

[32] For an articulation of fair information practices as applied to a health information exchange environment, see The Markle Foundation, "Connecting Professionals: Private and Secure Information Exchange," 2006, *available at* http://www.connectingforhealth.org/commonframework/index.html (last visited Dec. 29, 2008). See also the Organization for Economic Cooperation and Development (OECD) Data Protection Principles, 1980, extract from *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/OECDPs.html.

[33] HIPAA nondiscrimination provisions (Title I) prohibit individuals in group health plans from being denied eligibility for benefits or charged more for coverage because of any "health factor," which includes health status and medical history or condition. These provisions do not apply to insurance purchased in the individual market. For a summary of these provisions, see Employee Benefits Security Administration, U.S. Department of Labor, "FAQs: About the HIPAA Nondiscrimination Requirements," *available at* http://www.dol.gov/ebsa/faqs/faq_hipaa_ND.html (last visited Dec. 29, 2008).
[34] The three states are Arkansas, California and Delaware. For more information, see D. Gage, "California data-breach law now covers medical information," *San Francisco Gate*, January 4, 2008, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U9000.DTL (last visited Dec. 29, 2008).
[35] A comprehensive analysis of state breach notification laws is beyond the scope of this paper.
[36] 45 C.F.R. § 164.514(b)(1) (2007).
[37] 45 C.F.R. § 164.514(b)(2) (2007).
[38] 45 C.F.R. § 164.514(a)(b)(2)(ii) (2007).
[39] 45 C.F.R. § 164.514(e) (2007).
[40] 45 C.F.R. § 164.514(e)(3)-(4) (2007).
[41] L. Sweeney, *The Identifiability of Data* (forthcoming book publication); see Salvador Ocha et al., Massachusetts Institute of Technology, "Reidentification of Individuals in Chicago's Homicide Database, A Technical and Legal Study," (November 2008), *available at* http://web.mit.edu/sem083/www/assignments/reidentification.html.
[42] 45 C.F.R. § 164.514(e)(4)(iii)(A) (2007).
[43] *Supra* note 4.
[44] 45 C.F.R. § 164.501 (2007).
[45] *Id.*
[46] The Privacy Rule gives individuals a right to request a restriction on uses or disclosures of protected health information for treatment, payment and health care operations (and on disclosures to family or friends who are assisting in the individual's care); but the covered entity does not have to comply with the request. See 45 C.F.R. § 164.522(a) (2007).
[47] 45 C.F.R. § 164.514(d) (2007).
[48] See Privacy and Security Solutions, *supra* note 20, at 3-5, 3-7.
[49] 45 C.F.R. § 164.506(c)(4) (2007).
[50] For an explanation of the definition of "treatment", see the Preamble to the Final HIPAA Privacy Rule, *available at* http://aspe.hhs.gov/ADMNSIMP/final/PvcPre02.htm; see also OCR's clarification of the definition of "treatment" in its FAQs, *available at* http://www.hhs.gov/hipaafaq/providers/treatment/481.html.
[51] See section (1) in the definition of health care operations, 45 C.F.R. § 164.501 (2007).
[52] *Id*.
[53] 45 C.F.R. § 164.512(i) (2007).
[54] 45 C.F.R. § 164.522(a) (2007).
[55] National Committee on Vital and Health Statistics (NCVHS) Reports and Recommendations, *Letter to the Secretary of the U.S. Department of Health and Human Services: Privacy and Confidentiality in the a Nationwide Health Information Network (NHIN)*, (June 22, 2006), recommending that individuals have a choice regarding whether or not their information is included in the NHIN; See also NCVHS Reports and Recommendations, *Report to the Secretary of the U.S. Department of Health and Human Services: Individual control of sensitive health information accessible via the NHIN for purposes of treatment* (February 20, 2008), recommending individuals be allowed to sequester information in certain sensitive categories.
[56] NCVHS Report to the Secretary, February 20, 2008, *supra* note 56.
[57] *Id.*
[58] 45 C.F.R. § 164.524(c)(2) (2007). Such access right is to information maintained in a designated record set, and exempts psychotherapy notes and a few other categories of information; see also 45 C.F.R. 164.524(a)(1) (2007).
[59] U.S. Department of Health and Human Services, Health Information Privacy, Compliance and Enforcement, Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/top5issues.html
[60] 45 C.F.R § 164.524(b)(2) (2007).
[61] 45 C.F.R. § 164.524(c)(4) (2007).
[62] See Georgetown University Health Policy Institute, Health Policy Institute, Center on Medical Record Rights and Privacy, *available at* http://hpi.georgetown.edu/privacy/records.html for more information.
[63] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R pt. 160, 164).

[64] U.S. Department of Health and Human Services, HIPAA Frequently Asked Questions: About the Privacy Rule, "Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?" November 9, 2006, *available at* www.hhs.gov/hipaafaq/about/193.html (last visited February 3, 2009).
[65] 45 C.F.R. § 164.508(b)(4) (2007).
[66] See, e.g., *Discussion Draft of Health Information Technology and Privacy Legislation*: *Hearing Before Subcomm. on Health of the H. Comm. on Energy and Commerce*, 110th Cong. (2008) (written testimony of Dr. Deborah Peel, Founder & Chair, Patient Privacy Rights) *available at* http://www.patientprivacyrights.org/site/DocServer/Peel_written_testimony_06.04.08.pdf?docID=4021; See also *Privacy and Health Information: Hearing Before Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics, U.S. Department of Health and Human Services* (Feb. 23, 2005) (testimony of Sue A. Blevins, Founder and President, Institute for Health Freedom), *available at* http://www.ncvhs.hhs.gov/050224p6.htm.
[67] See, e.g., Center for Democracy & Technology, Rethinking the Role of Consent in Protecting Health Information Privacy (January 2009), *available at* http://www.cdt.org/healthprivacy/20090126Consent.pdf.
[68] See *id.* at 14-19 for examples of approaches to consent taken by some state electronic exchange networks; For state profiles, see generally State-level Health Information Exchange Consensus Project, Profiles of Sate-level HIE Efforts, *available at* http://www.slhie.org/efforts.asp.
[69] NCVHS Letter to the Secretary, June 22, 2006, *supra* note 56.
[70] The Markle Foundation, Connecting for Health, The Common Framework: Networked Health Information, *available at* http://www.connectingforhealth.org/commonframework/#guide.
[71] R. Alonso-Zaldivar, "Effectiveness of medical privacy law is questioned," *Los Angeles Times*, April 9, 2008, *available at* http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story. In July 2008, HHS announced that Seattle-based Providence Health & Services agreed to pay $100,000 as part of a settlement of multiple violations of the HIPAA regulations. But the press release from HHS made clear that this amount was not a civil monetary penalty; See also U.S. Department of Health and Human Services, News Release, "HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information," July 17, 2008, *available at* http://www.hhs.gov/news/press/2008pres/07/20080717a.html (last visited February 3, 2009).
[72] For more information on the OLC memo and consequences, see P. Swire, "Justice Department Opinion Undermines Protection of Medical Privacy," *Center for American Progress*, June 7, 2005, *available at* http://www.americanprogress.org/issues/2005/06/b743281.html (last visited February 3, 2009).
[73] *Id.*
[74] 45 C.F.R. § 164.504(e)(1)(ii) (2007).
[75] 45 C.F.R. § 164.504(e)(1)(ii)(A)-(B) (2007).
[76] See 15 U.S.C. § 7706(f) (Supp. 2004).