Patient-Centric Privacy:

Envisioning Collaboration Between Payers, Providers & Patients With The Patient At The Core

Tyrone W A Grandison, *Senior Member, IEEE*

***Abstract* — Protection of personal healthcare information (PHI) has been as a significant hindrance to the acceptance, adoption and continued use of healthcare information technology (HIT). As nations and corporations encourage innovation in the healthcare sector for better outcomes for all its stakeholders, they are proceeding under a latent assumption – the equation of data stewardship with data ownership. This notion relegates the patient to the role of information provider and empowers infrastructure owners with data ownership rights. In this paper, we introduce *Patient-Centric Privacy*, which refers to 1) the recognition that patients are a fundamental and integral part of the disclosure, access and use processes, and 2) to the ability of the patient to control the release of their healthcare information.**

***Index Terms*—Health care, Privacy, Protection**

I. Introduction

IN order to best serve the community of patients, who entrust their information to medical practitioners and who have expectations on the protection of their information [1], we have to clearly describe the current healthcare landscape, which is built on a set of (often forgotten) core assumptions (or assertions).

The first assertion is that *businesses are in control of healthcare industry* [2]. This implies that there are market forces that necessitate that there are compelling economic motivations for the core processes, technologies and services offered by healthcare companies.

The second assertion is that *healthcare payers and providers view patient data they receive as their own assets* [3]. In the words of a retired practitioner "When I was practicing as a physician, I considered those records to be my property" [3]. Whether a conscious market decision or execution of established best practice, a common domain assumption is that data from patients or the information that is generated from processing patient data is a part of the healthcare entity's portfolio.

When combined, these two assertions engender a business model in which a trusted steward[1], i.e. hospital, laboratory, insurance company, etc., claims ownership[2] over the data it collects. Additionally, these businesses provide access to this data to a client base for profit. The data users in this client base include patients, who normally pay for these services to be performed, or agents that cover the cost of the services. These users may also be third party affiliates or business associates that are willing to pay for data in order to deliver their own products and services. This set may even include researchers who are investigating an area that is of interest to the healthcare entity.

Unfortunately, this business model is not optimized to deliver either maximum benefit to the patient (who is the entity with the most at risk in this system) or to attain an equilibrium point where risk and reward is spread equally amongst all involved. In this paper, we purport that this is the case because the system was not (and is not) built on the premise of *patient-centricity*.

Patient-Centricity refers to the notion that patients are *fundamental* and *integral* to the healthcare ecosystem. *Fundamental* refers to the fact that patients are the basic, foundational and essential building blocks of the system. *Integral* refers to the fact that patients (and their input) are necessary to the completeness and usefulness of the system. Both facets imply patients are critical to the system's success and that their input should be included in all the processes and decisions that affect them.

As previously stated, the business model for the healthcare sector assumes that the entities that operate the infrastructure adopt a mindset where they believe that they are data owners. In this environment, the patient is not always consulted before their data is to be used in dubious or potentially risky ways; nor are they automatically included when benefits and profits are reaped. Typically, the best interest of the steward is normally the dominant (and often the only) one considered.

In a patient-centric privacy model, it is presumed that the patient has ultimate control of their data and that they are always consulted when decisions are to be made regarding disclosure, use or access of their information.

As healthcare systems through the ages have followed the approach of equating stewardship and ownership, a transition to patient-centric systems will no doubt involve a concerted collaboration between providers, payers and patients. However, this is only possible with a clear, articulated vision of what this should look like. This paper seeks to provide the initial steps towards this goal.

To avoid confusion and ensure that the language and

Tyrone W A Grandison is with IBM Services Research, Hawthorne, NY 10532, USA (Phone: 408-927-1951; Fax: 408-927-3215; E-mail: tyroneg@us.ibm.com)

[1] A data steward ("steward") is an entity who receives a client's data, in the operation and execution of their (business) function, with the expectation that they will be a trustworthy agent or proxy on behalf of the client.

[2] A data owner ("owner") is an entity that provides data or has information generated about them in the process of using a service.

COLLABORATECOM 2010, October 9-12, Chicago, USA

DOI 10.4108/icst.collaboratecom.2010.24

associated semantics used in this paper are understood, section II will provide the required background information. Then a description of current model for the healthcare system will be provided and finally the patient-centric model presented.

II. Background

There is a confluence of factors that have led to the current state of HIT.

A. The Evolution

Centuries ago, the practice of medicine was characterized by the one-to-one relationship between the patient and the physician [4], where the physician was a general practitioner with a wide knowledge base. Over time, the field adopted the philosophy that greater efficiency and innovation could be achieved if professionals focused on specific areas of study i.e. if they became specialists [5]. Today, the treatment experience normally has multiple providers with multiple specialties, e.g. pharmacologists, endocrinologists, nurses, therapists, radiologists, etc., who function in a complex web and in a semi-coordinated fashion. For example, [6] documents that the record of a typical patient (at a teaching hospital) was viewed by at least 75 healthcare personnel during an in-patient stay.

With this move towards a multi-tier, multiple-interaction, specialist-oriented model of care delivery, a financial structure (including health insurance companies, health maintenance organizations, etc.) evolved in order to facilitate healthcare payments [7]. These financial institutions quickly realized that there was a lucrative market for the data that they held – and thus began the merging of the notions of data stewardship and data ownership in healthcare. As the industry became digitized, information technology (IT) companies courted parties in the industry that could afford the costs of computerization, i.e. the healthcare financial institutions that are now commonly referred to as *healthcare payers*. As service providers, these IT firms delivered on the requirements specified by healthcare payers, which included systems with the *non-patient-centric* assumption.

As this digitization has progressed, patients have expressed high expectations on the measures being employed to protect their information and to keep them informed of its use and disclosure [1]. This belief is often supported by the media and "sound-bite" explanations of the legal rights afforded to them [8-10]. Unfortunately, these expectations have been shown to be misrepresentations of current practice [1]. This disconnect between patient privacy expectation and its associated technology support has sparked interesting initial work.

B. The Related Work

David & Prosch [11] apply the seven foundational principles of *Privacy By Design*[3] [12] to the *"next generation"* notion to corporate citizenship proposed in [13], which states that for effective corporate citizenship, firms must minimize harm and maximize benefits through all their actions, factoring in and being responsive to all stakeholders. The authors of [11] describe an approach that embeds structures, systems, processes and policies into and across a company's inter-organizational supply chain. Unfortunately, this work does not address how to create patient-centric privacy-enabled healthcare systems.

In April of 2010, the Office of the National Coordinator for Health Information Technology (ONCHIT) in the US Department of Health and Human Services (HHS) awarded $60 million in grants under the Strategic Health IT Advanced Research Projects (SHARP) Program in four topic areas [14]. Two of the areas are 1) Security and Health Information Technology & 2) Health care Application and Network Design. Both areas seek to develop new technologies while ensuring and improving privacy and security. However, both efforts are in their infancy with few deliverables to date.

On August 19th, 2010, the Privacy and Security Tiger team, which advises the HHS' HIT Policy Committee on patient data privacy and security, recommended the adoption of guidelines set out in the Fair Information Practices (FIP). They state that "this overarching set of principles, when taken together, constitute good data stewardship and form a foundation of public trust in the collection, access, use, and disclosure of personal information" [15, 16]. At the highest level, they assume that control is in the hands of the provider and they articulate initial proposals for facilitating patient consent.

C. The Other Core Definitions

In this context, the definition of privacy is "the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others" [17]. This is congruent with the prior discussion on patient-centric privacy model (in section I) and assumes that the person that provides data still owns the data even after it is stored on or in someone else's system.

It is recognized that there are recent initiatives that assert other definitions of patient-centric privacy [18]. However, these initiatives are grounded in the data stewardship – data ownership equality assumption. For example, definitions have been circulated that hint to patient-centric privacy (and patient-centric security) controls being those controls that are able to manipulate artifacts at the patient-level, i.e. record-level or tuple-level controls.

III. The Current Model

Fig. 1 provides a simplified illustration of the key salient points of the current operational model in the (American) healthcare industry.

In the process of receiving care, patients give a healthcare entity (normally a mainstream healthcare provider or service organization) all the information required by the medical practitioners to perform their job. Implicit in the figure is the fact that not only do patients provide a valuable asset, i.e. data,

[3] The 7 Foundational Principles of *Privacy By Design* [12] are: 1) Proactive not Reactive, 2) Privacy as the Default, 3) Privacy Embedded into the Design, 4) Full-functionality - Positive Sum, not Zero-Sum, 5) End-to-End Lifecycle Protection, 6) Visibility and Transparency, and 7) Respect for User Privacy.

to healthcare entities, but that they also pay for the service that they are accessing.

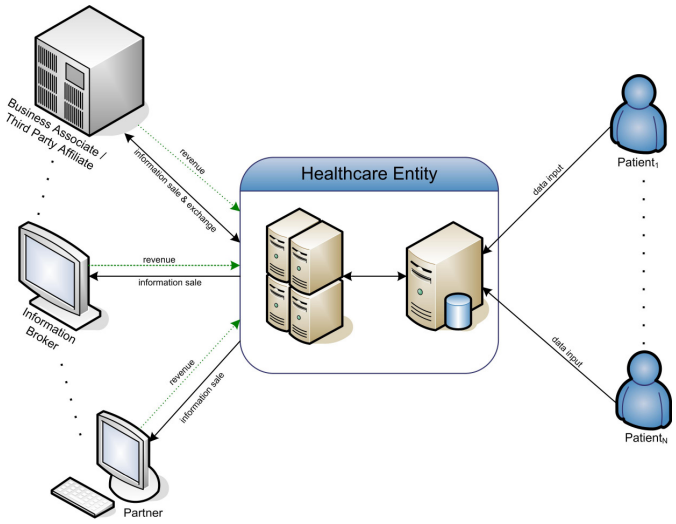

Fig. 1. Current Operational Model.

Healthcare entities maximize their profit by 1) entering into revenue sharing agreements, based on patient data, with associates and third parties, 2) selling patient data to information brokers, who may re-package, collate and aggregate data to offer value-added services to optimize other businesses, and 3) utilizing the services of partners to make patient data more valuable. In all these activities, the entity assumes control of the ingested data and the patient is assumed to have no control over the use of her data. Additionally, she receives none of the revenue generated from the use of her data.

Though, it can be argued that some of the profit-boosting activities of the healthcare entities subsidize the cost of care to the patient, this behavior may only translate into a cost reduction for the patient and never a (personal) revenue increase; as is the case for the business.

The true detriment of this model is that the patient assumes a significantly higher proportion of the (privacy, security, financial, and even health) risk [19-21] without gaining the (considerable) revenue upside that the healthcare entity enjoys. In such a scenario, the provider (or payer) is often incentivized to take significant risk; so long as the reward to the organization exceeds the expenditure needed to stem or repair any reputational damage and or trust erosion that may be incurred.

To redress this risk-reward imbalance faced by patients and to move towards a situation where conditions are more favorable for the patient and her privacy, we must start by creating and communicating new models.

IV. A Patient-Centric Model

In order to realistically transition to a healthcare system with a patient-centric privacy model at the core, there must be two critical factors in place that facilitate the collaboration between all the parties involved, namely a financial incentive and collective willpower.

The financial incentive requires that the Return On Investment (ROI), Expected Loss Valuation and the probability of loss be calculated. Fortunately, mathematical models can be created for each of these variables based on private revenue data and publicly-available data from national (and international) organizations that have archived fraud and breach data, e.g. the National Health Care Anti-Fraud Association (NHCAA) and the HHS' Office of Civil Rights (OCR). This incentive model would help payers (and providers) see the case for porting their systems; as increased patient participation in schemes that offer them a meaningful reward should translate into (rationalized) orders of magnitude more benefit to the payer. Unfortunately, the creation of this mathematical model is beyond the scope of this paper.

There is a low percentage of patients who are 1) aware of their rights with respect to their healthcare data and 2) know what healthcare payers and providers do with their data [22-23]. Education on these activities will either reassure patients [24] or spur them into action to effect change.

With these factors in place, a new healthcare model may be fashioned where control of every facet of a patient's data remains under her control during the entire information lifecycle. Technically, access control mechanisms with native support for (advanced) consent (and delegation) management will be the bedrock. Additionally, all systems should be set to enable the maximum level of privacy by default and patients must opt-in for their data to be used; given that the patient finds the associated remuneration to be at an acceptable level.

In order to be immediately applicable, our model leverages the Nationwide Health Information Network (NHIN)[4] effort, which is currently supported by the Office of the National Coordinator for Health Information Technology (ONC). This work defines a collection of standards, protocols, legal agreements, specifications, and services that enable secure Health Information Exchange (HIE).

Fig. 2 shows the basic elements of a patient-centric privacy-enabled healthcare system that can be leveraged by today's infrastructure. There is an assumption of a Healthcare (Service) Bus, which securely transports healthcare messages throughout the network. For simplicity, the Translation service, the Patient Identity Cross Referencing Service and Conversion services of a typical HIE are not shown in Fig. 2. For this paper, they are assumed services that co-exist with the Patient Registry.

Our paper introduces a Consent Server that, at minimum, contains a table with the following schema:

PERMISSIONS (*patient_ref_no* **char**(18),
consent_decision **Boolean**, *data_segment* **char**(18),

[4] The NHIN standards, services and policies are being developed by the NHIN Cooperative - a group of federal agencies, local, regional and state-level Health Information Exchange Organizations (HIOs) and integrated delivery networks. Initial recommendations have recently spurred work on a new initiative NHIN Direct. More information is available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nationwide_health_information_network/1142

for_purpose **char**(18), *granted_person* **char**(32), *delegated_person* **char**(32), *negotiated_remuneration* **int,** *further_constraints* **char**(32))

The use case semantics of the PERMISSIONS table is that patient with *patient_ref_no* has decided to grant consent *(consent_decision = 1)* or not *(consent_decision = 0)* for her data of type *data_segment* to be used for purpose *for_purpose* by professional *granted_person* with the understanding that *negotiated_remuneration* will be paid and further conditions *further_constraints* are met. Note that either *granted_person* or *delegated_person* must be blank. If *delegated_person* is specified, then this becomes a statement of the delegation of this consent to *delegated_person*.

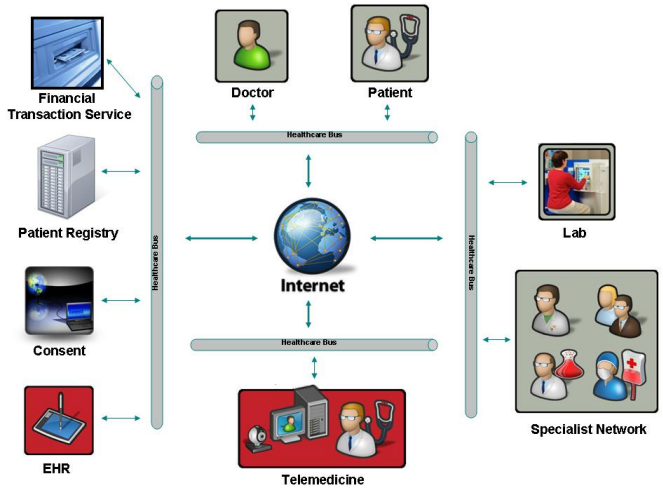

Fig. 2. Patient-centric Privacy-enabled Healthcare Model for Current Systems

We also introduce the Financial Transaction Service, which is triggered whenever an incoming request triggers a positive consent decision, and supervises the transfer of funds from utilized data and issues payments to the involved parties.

Incoming requests from HIE consumers operate as normal, with the slight modification that they are enhanced with consent filter predicates that are evaluated prior to EHR retrieval.

This approach was taken because it is a currently technically feasible way to ensure that patient input is always included and that the risk-reward disparity is addressed. Through its simplicity, the scheme offers a powerful way to enforce fine-grained consent management with delegation. It is envisioned that further investigation into this space will uncover more sophisticated and robust techniques and schemes that can be built around or on top of this base.

V. The Hard Questions

There are a series of difficult questions that all stakeholders must negotiate to get to patient-centric privacy. Here, an initial (and non-exhaustive) list of some of these questions (as well as initial thoughts on answers) is provided:

A. *What is the motivation to include the patient in the loop?*

Currently, the prevailing business model will persist as long as the public remains unaware of their lack of control and the inherent risk they face. As previously hinted at, increased patient awareness, more transparency into healthcare business practices and an increasing number of healthcare data breaches will facilitate a need for change. As previously stated, this phenomenon would be accelerated by work on new fair ROI models for EHRs.

B. *Do we have all the components to make this a reality?*

The components needed fall into four categories: business, technology, legislative and societal (BLTS). In this paper we introduced the business and technical components required. The legislative and societal components involve 1) policy advocacy to strengthen laws and regulations with regards to patients' interests and 2) consumer education on their rights, current healthcare best practices and their role in the ecosystem.

C. *Will the transition & maintenance costs be prohibitive?*

Federal funding from the American Recovery Act of 2009 will provide fuel for the initial stages of HIT development (if core patient-centric privacy principles were included at design time). The transition and maintenance costs for initiatives can hopefully be negligibly factored into the overall system cost.

D. *How is this going to happen? Who should lead it?*

As this is an initiative for the greater good of the people and the people collectively have a considerable voice when properly targeted, the likely agents of change should be the Federal government – who are the representatives of the people and the group who can effectively interface with all the stakeholders. This effort requires a concerted collaboration between all the stakeholders in the healthcare system to be effective.

E. *Is the current approach ideal?*

In an ideal world, Fig. 3 would represent the starting point for a solution. The inherent assumptions of Fig. 3 are that healthcare entities focus on delivering better service and that this is the only driver for their continued revenue success and that patients maintain ownership of and have contractual rights over their data. Unfortunately, this represents a radical change from the current system.

In this new world, after the patient pays for a service and provides her data to a healthcare entity, the entity publishes an anonymized synopsis of the patient data with a reference to the patient (or the patient's account information). Anonymization offers an added layer of security for identity protection. This entire process may be viewed as being similar to that of HIE registration.

Interested parties may query the Information Publication/Discovery resource and request to use the specific patient data that is relevant to them. Use of this data requires consent from the data owner (i.e. the patient) and payment for using this data (i.e. sent to the patient's account), which would be handled through a trusted Financial Transaction service.

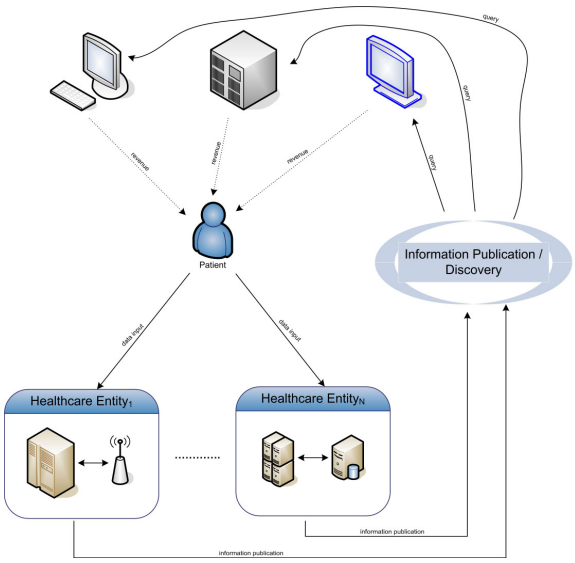

Fig. 3. Another Proposed Architecture.

It should be noted that securing patient account information must be addressed before this model is deployed. In lieu of having links back to the patient information, one could use previously stored consent management information, along with more creative reimbursement schemes, to achieve the same goal. Further research is required on the optimal variant of the system in Fig. 3. As developing countries are starting to create their healthcare infrastructure, exploration on such models may be possible in these environments.

VI. Conclusion

As we embark on a process to transform the healthcare sector, it is an appropriate time to evaluate and implement models that ensure the long-term success of the industry going forward. The intention of this paper is to spur discussion and debate on this issue.

The equating of data stewardship rights with data ownership rights by healthcare payers and providers have left the patient out of the loop. Correcting this issue requires a coordinated collaboration of healthcare stakeholders. In this paper, we present a starting point.

References

[1] Tyrone Grandison, Rafae Bhatti. “HIPAA Compliance and Patient Privacy Protection”. The proceedings of the 13th World Congress on Medical and Health Informatics (MEDINFO). September 12-15, 2010. Cape Town, South Africa.

[2] James Gubb, Oliver Meller-Herbert. “Markets in Health care - The theory behind the policy”. CIVITAS: Institute for the Study of Civil Society Report. Dec 2009. http://www.civitas.org.uk/nhs/download/Civitas_Markets_in_healthcare_Dec09.pdf

[3] Tim O'Reilly. “A Manifesto on Health Data Rights”. O'Reilly Radar. June 22, 2009. http://radar.oreilly.com/2009/06/manifesto-health-data-rights.html

[4] Gerald Higgins. “The History of Confidentiality in Medicine: The Physician-Patient Relationship”. Canadian Family Physician 35 (April 1989): 921-926.

[5] Rafae Bhatti, Tyrone Grandison. “Improving Security Policy Coverage in Healthcare”. In "Certification and Security in Health-Related web applications: Concepts and Solutions". Editors: Anargyros Chryssanthou, Iraklis Varlamis, Ioannis Apostolakis. IGI Global. 2010.

[6] Mark Siegler. “Confidentiality in Medicine – A Decrepit Concept”. New England Journal of Medicine 307, no. 24 (1982): 1518-1521.

[7] Terree P Wasley. “Health care in the twentieth century: a history of government interference and protection”. Moneywatch.com, April 1993. http://findarticles.com/p/articles/mi_m1094/is_n2_v28/ai_13834930/

[8] ScienceDaily. “Misleading Media Coverage of Medicine”. Nov 6, 2008. Retrieved from http://www.sciencedaily.com/releases/2008/11/081126075613.htm

[9] Eve Bender. “Federal Privacy Rule: Contradiction in Terms?”. Psychiatric News, Vol 37, No 23, Pg 10. Dec 6, 2002. Retrieved from http://pn.psychiatryonline.org/content/37/23/10.full

[10] Patient Privacy Rights. “Who can snoop in your PHR - Personal Health Record Report Card” Retrieved from http://www.patientprivacyrights.org/site/PageServer?pagename=phr_report_card.

[11] Julie S David, Marilyn Prosch. “Extending the value chain to incorporate privacy by design principles”. Identity in the Information Society. Vol 3, No 2, 295-318. August 2010.

[12] Ann Cavoukian. “Privacy by Design: Take the Challenge”. Office of the Information and Privacy Commissioner of Ontario. Retrieved From http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf

[13] Guy Morgan, Kwang Ryu, Philip Mirvis. “Leading corporate citizenship: governance, structure, systems”. Corporate Governance, 9(1), 39-49.

[14] Anthony Guerra. “ONC Awards $60 Million in SHARP Grants”. HealthSystemCIO. April 2, 2010. Retrieved from http://healthsystemcio.com/2010/04/02/onc-awards-60-million-in-sharp-grants/

[15] Nicole Lewis. “Health Data Privacy Recommendations Balance Security, Accessibility”. InformationWeek. August 20, 2010. Retrieved from http://www.informationweek.com/news/healthcare/policy/showArticle.jhtml?articleID=226800438&subSection=All+Stories

[16] Privacy & Security Tiger Team, HIT Policy Committee. http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19421

[17] Allan F Westin. “Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I - The Current Impact of Surveillance on Privacy”. Columbia Law Review 1003, Vol. 66, No 6. June 1966.

[18] R.W. Donnell. “What does "patient-centered" mean?” Aug 5, 2008. Retrieved from http://doctorrw.blogspot.com/2008/08/what-does-patient-centered-mean.html

[19] George Hulme. “Healthcare Breach Costs May Reach $800 Million”. InformationWeek. Aug 15, 2010. Retrieved From http://www.informationweek.com/blog/main/archives/2010/08/analysis_health.html;jsessionid=2MGZMX2KGORDTQE1GHPSKH4ATMY32JVN

[20] Saul William Seidman. “Trillion Dollar Scam: Exploding Health Care Fraud”. Universal-Publishers, 2008. ISBN-13: 978-1599429564

[21] David A Hyman. "HIPAA and Healthy Care Fraud: An Empirical Perspective". The Cato Journal. March 22, 2002. http://www.cato.org/pubs/journal/cj22n1/cj22n1-10.pdf

[22] N. Kuzu, A. Ergin, M. Zencir. "Patients' awareness of their rights in a developing country". Public Health, Vol. 120, Issue 4, Pages 290-296, April 2006. DOI: 10.1016/j.puhe.2005.10.014)

[23] Margaret A. Stone, Sarah A. Redsell, Jennifer T. Ling, and Alastair D. Hay. “Sharing Patient Data: Competing Demands of Privacy, Trust and Research in Primary Care” British Journal of General Practice 55, no. 519 (October 2005): 783–789.

[24] Arthur Williams, DC Herman, JP Moriarty, TJ Beebe, SK Bruggeman, EW Klavetter, PH Steger, JK Bartz. “HIPAA Costs and Patient Perceptions of Privacy Safeguards at Mayo Clinic.” Joint Commission Journal on Quality and Patient Safety 34, no. 1 (Jan. 2008): 27–35.