# Achieving the Right Balance:

## Privacy and Security Policies to Support Electronic Health Information Exchange

California HealthCare Foundation

ISSUE BRIEF

### Introduction

Electronic health records (EHRs) and the electronic exchange of health information have the potential to improve individual and population health while increasing cost efficiency. In the past three years major initiatives have been launched at the federal and state levels to encourage and support the adoption and use of health information technology (IT).

Although patients and consumers overwhelmingly support health IT, they have concerns about the privacy and security of their personal health information.[1] More than 80% of both doctors and the public believe that requiring protections and safeguards for patient privacy is important.[2] At the same time, two-thirds of consumers believe that privacy concerns should not stop the progress of health IT initiatives.[3]

Policy initiatives, therefore, must balance the sometimes competing aims of sharing data and protecting privacy. Consumer advocates hold that building enhanced privacy and security into electronic health systems will bolster trust while supporting the increased use and appropriate sharing of health data.

This issue brief discusses the importance of building a statewide (and nationwide) system of electronic health information exchange (HIE) and the role that sound privacy and security policies should play in building and sustaining the public's trust. It offers patient- and consumer-based policy solutions to privacy and security concerns that balance individual and societal issues. Finally, it identifies gaps in the legal framework that help assure a trusted, secure digital health ecosystem, and suggests areas that merit further attention from federal and state policymakers.

### The Importance of Efficient Health Information Flows

In today's electronic world, where information can be located and shared at the click of a mouse, much of America's health care remains mired in paper-based systems. Some 83% of doctors predominantly transmit their patients' information to other medical professionals by paper or fax — not electronically — according to a recent nationwide survey by the Markle Foundation.[4]

This lack of efficiency comes at tremendous cost to health care providers, the nation's economy, and Americans' health. For example, the Institute of Medicine's seminal 1999 study estimated that medical errors in hospitals cause 44,000 to 98,000 deaths every year.[5] More than a decade later, the system continues to generate unacceptable statistics. In 2006, the Institute of Medicine estimated that each hospital patient suffered at least one medication error per day, and more than 1.5 million adverse and preventable drug errors occurred annually.[6] A 2011 study found that adverse events occurred in 33% of hospital admissions, most commonly in medications, surgery, procedures, and hospital-associated infections.[7]

Evidence is mounting that electronic health records and information exchange are critical to reversing these trends. Studies have demonstrated

June 2012

that HIE and EHR technology can improve the quality, safety, and efficiency of care, as well as decisionmaking and care coordination among patients, doctors, and other caregivers.[8] HIE can also improve the public's health by better predicting and managing chronic diseases, epidemics, and health disparities; promoting patient safety and preventing medical errors; and reducing the cost of health care.[9] In 2005, the RAND Corporation estimated that implementing health IT could save $81 billion or more per year in efficiency and safety savings alone, and improvements to prevention and management of chronic disease could double this amount.[10]

The federal government recently launched an ambitious program to build a nationwide system of EHRs and HIE for providers and patients. In the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), Congress dedicated $22.6 billion to support the purchase and use of EHRs by providers and to establish an infrastructure for HIE.[11] States (including California) are also dedicating funds to support this movement.

Patients and consumers overwhelmingly support these efforts. Survey data indicate that a large majority of the public wants electronic access to health information for themselves and for their care providers to improve individual and population health. Two-thirds of patients (70%) and doctors (65%) believe that patients should be able to view and download their personal health information online.[12] About 74% of doctors prefer to share a patient's information electronically with other providers when needed.[13] Both the public and doctors strongly support the following priorities for health IT: requiring doctors and hospitals to share information to reduce medical errors (80% of public, 85% of doctors); cutting avoidable costs like duplicate tests (79% of public, 85% of doctors); better coordinating patient care (77% of public, 84% of doctors); measuring progress on health care quality and safety improvement (75% of public, 73% of doctors); and improving the nation's health in areas such as heart disease, obesity, diabetes, and asthma (69% of public and doctors).[14]

The shift from paper to electronic health records presents new challenges to protecting the privacy and security of a patient's health information; a breach that formerly affected a single paper record now can expose an entire database of patient records. However, HIE presents powerful new ways to improve the privacy and security of patients' data, including encryption, authentication and authorization controls, and electronic audit trails.

## Framework for Achieving the Right Balance

Patients and consumers want the benefits of information exchange, but they also want to be assured of the privacy and security of their electronic health information. In 2010, a cross-section of California consumer, patient, and civil rights organizations came together to frame a set of principles for health information exchange consistent with these ends. The resulting document, titled "Consumer and Patient Principles for Electronic Health Information Exchange in California," is key to ensuring the public's trust in HIE. (See the Appendix.)

An overarching message of these nine HIE principles is that there is no inherent tension between protecting privacy and sharing personal health information for clinical treatment and other appropriate health-related purposes. It is not a choice between privacy or better health care; HIE initiatives should aim to achieve both.

These principles balance patients' various and sometimes competing needs within the overall context of health and health care — for example, health care is coordinated among patients and diverse providers, and safety and quality data about providers and treatments are made accessible for the public good, all while the privacy and security of personal health information is assured.

The principles are based on fair information practices, which obligate data stewards to use personal data responsibly and with respect for its sensitivity. Fair information practices are the starting point for state, federal, and international policies for the collection, storage, use, and disclosure of personal information and the foundation for most US and international data protection laws.[15] For example, recent guidance issued by the US Department of Health and Human Services (HHS) requires states receiving federal health IT funding to develop policies that address all of the fair information practices.[16]

Building and preserving trust in HIE requires entities to implement the entire complement of fair information practices. Overreliance on one or some of the principles significantly weakens their overall efficacy. For example, some advocates and policymakers emphasize patient

### Fair Information Practices*

1. **Openness and transparency.** All data stewards should make their policies and practices regarding health information open and transparent to patients and to the public generally. Data stewards should inform individuals about what personal health information exists about them, for what purpose or purposes it may be used, who can access and use it, and who retains it. Data stewards should also maintain and provide individuals with corresponding audit trails.
2. **Collection limitation.** Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means, and, where possible, with the knowledge and consent of the data subject.
3. **Purpose specification and minimization.** The purposes for which personal health data are collected should be specified at the time of collection, and only the information reasonably necessary for those purposes should be collected.
4. **Data integrity and quality.** All personal health data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current. Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of health information exchange. There must also be transparent mechanisms to help patients and organizations correct or "clean" their data in the event that errors or omissions are discovered.
5. **Use and disclosure limitation.** Personal health information should be used, exchanged, or disclosed only for the purposes specified, and only the information needed to accomplish the purpose should be used, exchanged, or disclosed. Data stewards should immediately notify patients of breaches of privacy, security, or these limitations regarding their personal health information, and comply with all laws regarding such breaches.
6. **Individual participation and control.** Each entity that controls, accesses, or uses personal health data should inform an individual upon request whether it has personal health information relating to the individual. Each individual has the right to obtain from the entity a copy of the individual's personal health data within a reasonable time (at no or minimal charge), and in a form and language that the person can readily understand; if there are legal reasons why a copy cannot be provided, the individual has a right to know why the request was denied and to appeal the denial. Each individual has the right to challenge the collection, content, retention, use, or disclosure of personal health information relating to them, including the right to have the particular information corrected, completed, amended, omitted, or expunged.
7. **Local control.** Personal health information should remain in the control of the patient and the physicians and institutions that are directly involved with his or her health care. Local control also builds upon existing infrastructures (augmented as necessary to adhere to these principles, to ensure interconnection and interoperability, and to incorporate innovations), so that we may realize the benefits of health information exchange more quickly.

*Based on Markle Foundation/Connecting for Health's Common Framework of Policy Principles and Technology Principles (2006). See Appendix.

consent in developing recommendations for protecting the privacy of health information. Indeed, providing patients with some choice regarding how entities may use and share their health data is a core fair information practice. But consent alone cannot substitute for a comprehensive approach to privacy protection; overreliance on patient consent can undermine privacy and security in practice. Unfortunately, most patients do not focus on the details of consent forms, and those who do often do not understand the terms.[17] Many wrongly assume that the existence of a privacy policy means their personal information will not be shared, even when the policy states the opposite.[18] Consent forms are typically drafted by entities seeking the individual's consent to use information, so they are typically phrased in ways to secure that consent.[19]

Developing effective consent policy in California will require careful consideration of consumer and patient values, balanced with the need for information sharing. Policies must emphasize consent when information uses and disclosures do not meet consumers' reasonable expectations, and must promote a "layered" approach to consent that consumers easily understand, with priority given to the most critical aspects of data sharing.[20]

## Existing Law and Gaps to Address

The personal health information of California residents is protected under federal and state health privacy laws. Both federal law (regulations under the Health Insurance Portability and Accountability Act, or HIPAA) and California state law (mainly the Confidentiality of Medical Information Act, or CMIA) are based on fair information practices and provide a foundation for comprehensive privacy and security protections.[21,22]

The laws set baseline rules for how health care entities may collect, use, and share health information whether in paper or electronic form. In general, these laws permit health care providers to share information for treatment, payment, and certain administrative activities without first requiring specific authorization from patients, but they do require specific authorization for "unexpected uses," such as research and sale of identifiable health information. These laws also require entities to implement reasonable security safeguards for electronic health data.

However, there are gaps in the existing protections; they do not address all of the fair information practices outlined by the HIE principles. Many issues require further attention from policymakers:

- All business entities that access, use, and disclose personal health information should be held accountable for complying with comprehensive legal obligations to protect health data. Today, federal coverage under HIPAA is limited to traditional health care system entities (e.g., providers and insurers) and their contractors (business associates). California lawmakers recently extended the CMIA's scope, but it is unclear whether these expansions suffice to provide comprehensive protections for consumers and patients regardless of which entity is accessing their information.[23]

- Accountability for compliance with federal and state health privacy and security protections should be strengthened. Lack of effective enforcement of existing law undermines the public's trust in holders and users of personal health information. At the same time, enforcement policy at both federal and state levels must be robust without making health care entities so overly cautious that they fail to share information in ways that facilitate the provision of good health care, both at an individual and population level.

- Laws that protect electronic health data, such as the HIPAA Security Rule, should be reassessed to ensure that they are sufficient to meet new security challenges and to incorporate technological innovation. For example, reports of data breaches filed with the HHS Office for Civil Rights, which

enforces the breach notification requirements under HIPAA, strongly suggest that entities covered by these rules are not consistently using encryption to protect stored health information. Encryption is one of the core protections that electronic health records and information exchange make available.

- Rules on the use of personal health information for marketing purposes should be strengthened. Survey data demonstrate that this remains a persistent concern of consumers.[24] Congress enacted provisions in the HITECH Act to strengthen federal rules on the use of personal health information for marketing purposes, but two years later, regulations to implement those provisions have not been finalized and could instead weaken them.
- Policymakers should provide more clarity on how entities are expected to comply with existing and new health privacy laws. Entities that are uncertain about whether they can use and share information lawfully may err on the side of caution and decide not to share. In circumstances where sharing should be encouraged, such uncertainty could be an obstacle to progress in leveraging data to improve individual and population health.
- Policymakers should ensure that standards for de-identifying health data remain robust and should establish penalties for inappropriate or unauthorized re-identification.
- Where possible, data-sharing models that favor decentralization and local control should be prioritized in lieu of duplicate databases created each time health information is needed for a particular purpose. Duplication and centralization of data amplify the risk of security and privacy violations. Local control also builds upon existing infrastructures (augmented as necessary to adhere to privacy and security standards, to ensure interconnection and interoperability, and to incorporate innovations), so that the benefits of HIE are realized more quickly.

## Conclusion

Building trust in California's system of electronic HIE among providers and patients will require sound privacy and security policies based on the full complement of fair information practices. Such policies should build on current law, and most importantly, be designed and implemented to protect consumers and support the information flows that are critical to improving individual and population health.


### About the Authors

Mark Savage, senior attorney, Consumers Union

Consumers Union is a nonprofit organization that publishes Consumer Reports, works for a fair and safe marketplace for all consumers, and empowers consumers to protect themselves. Learn more at www.consumersunion.org.

Kate Black, staff counsel, and Deven McGraw, director of the Health Privacy Project, Center for Democracy & Technology

The Center for Democracy & Technology is a nonprofit public policy organization; its Health Privacy Project develops and promotes policies that enable the trusted use of information technology to improve health. Learn more at www.cdt.org.



### About the Foundation

The California HealthCare Foundation works as a catalyst to fulfill the promise of better health care for all Californians. We support ideas and innovations that improve quality, increase efficiency, and lower the costs of care. For more information, visit us online at www.chcf.org.

## **Appendix:** Consumer and Patient Principles for Electronic Health Information Exchange in California
June 21, 2010

Electronic health information exchange and technology can improve health outcomes, empower patients to participate actively in their care, generate research data to improve population health, and improve the effectiveness of our health system. California's patients and consumers need the benefits to individual and population health that electronic health information exchange and technology can achieve. We need the better health care outcomes for individual patients; the better decisionmaking and care coordination among doctors and patients; the greater engagement of patients and families in their care. We need the better public health outcomes; the improved quality, safety, and efficiency of health care; the reduction of unnecessary care and costs. We need the deeper, more comprehensive understanding of individual and population health that electronic health information exchange can provide.

California's patients and consumers also want the better privacy and security of health information that health information technology can provide. Comprehensive privacy and security protections and fair information practices, in turn, engender the public trust necessary to adopt health information technology widely and achieve the benefits of electronic health information exchange across California.

The nine principles below are core expectations and minimum criteria that should govern the design and implementation of health information exchange and technology in California. California's patients and consumers will use these principles to benchmark and evaluate efforts to implement electronic health information exchange and technology in California. We will also use these principles to evaluate whether policymakers and providers ensure the requisite public transparency and trust necessary to succeed. We urge California's policymakers, providers and other stakeholders to adopt and use these nine principles as well.

These principles are interdependent, and the benefits, effectiveness, protections, and balance of any one may depend in significant part upon one or more other principles.

### Principles

1. **Important benefits for individual health.** Electronic health information exchange and technology should be designed and used to improve individual health care and its quality, safety, and efficiency. Patients should have ready and complete electronic access to their health data as well as relevant tools and educational resources, in their primary or preferred languages, to make meaningful use of that information. The technology should facilitate active engagement of patients in their health care, and engagement of family members and others as the patient chooses or law provides. It should enable full coordination of the patient's care among diverse providers and systems. It should enhance the privacy and security of the patient's health information, and reduce costs.

2. **Important benefits for population health.** Electronic health information exchange and technology should also be designed and used to improve health for the public and communities at large, such as promoting healthy environments and preventing unhealthy environments; reducing and preventing chronic diseases, epidemics, and health disparities; promoting patient safety and preventing medical errors; measuring and reporting the quality and performance of providers and facilities, and the comparative effectiveness of treatments; and reducing the cost of health care.

3. **Inclusivity and equality.** All Californians should have full and equal use of electronic health information exchange and technology and their benefits, including California's underserved low-income communities, communities of color, people speaking primary languages other than English, people with disabilities, seniors and youth, immigrant residents, and rural and inner-city communities.

4. **Universal design, accessibility, and interoperability.** Electronic health information exchange and technology should be designed and built to meet the diverse needs of all Californians from the outset, without barriers or diminished function or quality for some. Universal design anticipates

and accommodates, for example, the differing needs of older people and younger people; of people from diverse cultures and communities and the need for cultural competency; of people who use diverse languages at home and the need for linguistic competency and translation; of people with diverse abilities and disabilities; of people across the range of income levels; of people across the range of literacy in reading, health care, and electronic technology. Different systems and different patients and providers should interconnect easily.

5. **Privacy and security.** Health information exchange and technology must promote trust and protect the privacy, security, confidentiality, and integrity of health data. Strong privacy and security policies should be established to accomplish these ends, which are then supported by the technology necessary to implement and enforce them. To this end, health information exchange and technology should be further governed by the data stewardship rules and fair information practices specified in Appendix A, and sufficient security safeguards should protect all health data against such risks as loss or unauthorized access, destruction, use, modification, or disclosure. Both policy and technology should incorporate innovations that can enhance individual privacy and security and address new risks.

6. **Preventing misuse of health data.** Electronic health information exchange and technology should protect against misuses of health data, including the use of health data to deny or restrict health care or insurance coverage; restrict or deny credit or other financial benefits; engage in unsolicited marketing to patients and consumers; restrict or deny employment or housing; and deny or restrict a patient's rights under the law, including a patient's rights in matters of law enforcement, national security, and immigration enforcement.

7. **Partnership and HIT literacy.** Electronic health information exchange and technology should connect patients, providers, public health officials, and consumers as partners in personal and public health care. Such partnership requires that patients and consumers be informed in their primary languages about how to use health information exchange and technology well, and about patients' rights, remedies, and responsibilities.

8. **Accountability.** Entities that collect, access, or use health data, and the governmental agencies that oversee them, must be held accountable for realizing the benefits of health information exchange for California's patients and communities.

9. **Enforcement.** Entities that collect, access, or use health data, and the governmental agencies that oversee them, must be held accountable for enforcing the protections of health information exchange for California's patients and communities. Sufficient resources and adequate legal and financial remedies must exist to address breaches or violations. The benefits and protections of health information exchange are public goods, and enforcement proceedings should be transparent and public.

## **Appendix A:** Specific Principles for Privacy and Security of Health Information*

Under principle 5 above, Privacy and Security, health information exchange and technology should be further governed by the following data stewardship rules and fair information practices.

**5a. Openness and transparency.** All data stewards should make their policies and practices regarding health information open and transparent to patients and to the public generally. Data stewards should inform individuals about what personal health information exists about them, for what purpose or purposes it may be used, who can access and use it, and who retains it. Data stewards should also maintain and provide individuals with corresponding audit trails.

**5b. Collection limitation.** Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means, and, where possible, with the knowledge and consent of the data subject.

**5c. Purpose specification and minimization.** The purposes for which personal health data are collected should be specified at the time of collection, and only the information reasonably necessary for those purposes should be collected.

*Appendix A is based upon Markle Foundation/Connecting for Health's Common Framework of Policy Principles and Technology Principles (2006).

**5d. Data integrity and quality.** All personal health data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current. Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of health information exchange. There must also be transparent mechanisms to help patients and organizations to correct or "clean" their data in the event that errors or omissions are discovered.

**5e. Use and disclosure limitation.** Personal health information should be used, exchanged, or disclosed only for the purposes specified, and only the information needed to accomplish the purpose should be used, exchanged, or disclosed. Data stewards should immediately notify patients of breaches of privacy, security, or these limitations regarding their personal health information, and comply with all laws regarding such breaches.

**5f. Individual participation and control.** Each entity that controls, accesses or uses personal health data should inform an individual upon request whether it has personal health information relating to the individual. Each individual has the right to obtain from the entity a copy of the individual's personal health data within a reasonable time (at no or minimal charge), and in a form and language that the person can readily understand; if there are legal reasons why a copy cannot be provided, the individual has a right to know why the request was denied and to appeal the denial. Each individual has the right to challenge the collection, content, retention, use or disclosure of personal health information relating to them, including the right to have the particular information corrected, completed, amended, omitted, or expunged.

**5g. Local control.** Personal health information should remain in the control of the patient and the physicians and institutions that are directly involved with his or her health care. Local control also builds upon existing infrastructures (augmented as necessary to adhere to these principles, to ensure interconnection and interoperability, and to incorporate innovations), so that we may realize the benefits of health information exchange more quickly.

## Organizations Endorsing the Consumer and Patient Principles for Electronic Health Information Exchange in California

as of September 7, 2011

Many organizations are working to ensure that electronic health information exchange in California fully incorporates consumers' and patients' needs and perspectives. These Consumer and Patient Principles are currently endorsed by the following organizations:

AARP

American Civil Liberties Union of Southern California

Asian & Pacific Islander American Health Forum

Association of Asian Pacific Community Health Organizations

California Pan-Ethnic Health Network

California Rural Indian Health Board

Center for Democracy & Technology

Congress of California Seniors

Consumer Action

Consumers Union of United States

Family Bridges, Inc.

Health Access

Latino Coalition for a Healthy California

National Council of La Raza

National Partnership for Women & Families

Pacific Business Group on Health

Planned Parenthood Affiliates of California

Prevention Institute

Privacy Activism

Southern Christian Leadership Conference of Greater Los Angeles

Summit Health Institute for Research and Education, Inc.

The Children's Partnership

ZeroDivide

## Endnotes

1. *Markle Survey on Health in a Networked Life 2010* (January 2011): 6, www.markle.org; California HealthCare Foundation, *Consumers and Health Information Technology: A National Survey* (April 2010): 20, www.chcf.org.
2. Markle Survey, 2011, p. 6.
3. Markle Survey, 2011, p. 26.
4. Markle Survey, 2011, p. 6.
5. Institute of Medicine, *To Err Is Human: Building a Safer Health System* (Washington, DC: National Academies Press, 2000): 26, www.nap.edu.
6. Institute of Medicine, *Preventing Medication Errors* (Washington, DC: National Academies Press, 2007): 4, www.nap.edu.
7. David C. Classen et al., "'Global Trigger Tool' Shows That Adverse Events in Hospitals May Be Ten Times Greater Than Previously Measured," *Health Affairs* 30, no. 4 (April 2011), www.healthaffairs.org.
8. See, e.g., Congressional Budget Office, *Evidence on the Costs and Benefits of Health Information Technology* (May 2008): 1, 3–17, www.cbo.gov.
9. Randall D. Cebul et al., "Electronic Health Records and Quality of Diabetes Care," *New Engl. J. Med.* 365 (September 1, 2011): 825, www.nejm.org.
10. RAND Corporation, *Health Information Technology: Can HIT Lower Costs and Improve Quality?* (2005), www.rand.org.
11. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L, No. 111-5 (February 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. U.S. Department of Health and Human Services, *Recovery Act Funding: Health Information Technology,* rev. January 2011, www.hhs.gov.
12. Markle Survey, 2011, p. 3.
13. Markle Survey, 2011, p. 4.
14. Markle Survey, 2011, p. 5.
15. The notion of "fair information practices" comes from a 1973 report, "Records, Computers and the Rights of Citizens," commissioned by the US Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems.
16. Program Information Notice, "Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program," March 22, 2012, www.healthit.hhs.gov.
17. Nathaniel Good et al., "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (July 8, 2005), www.cmu.edu.
18. Joseph Turow, Deirdre K. Mulligan, and Chris J. Hoofnagle, "Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace" (October 2007), www.berkeley.edu.
19. Janlori Goldman, Zoe Hudson, and Richard M. Smith, "Privacy: Report on Privacy Policies and Practices of Health Web Sites" (January 2000), www.chcf.org.
20. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" (March 2012), www.ftc.gov.
21. Health Insurance Portability and Accountability Act of 1996, Pub. L., No. 104–191, 110 Stat. 1936 (1996); 45 C.F.R. §§ 164.500–534.
22. California Civil Code §§ 56–56.37.
23. California Civil Code §§ 56.06(a).
24. Markle Survey, 2011, p. 7.