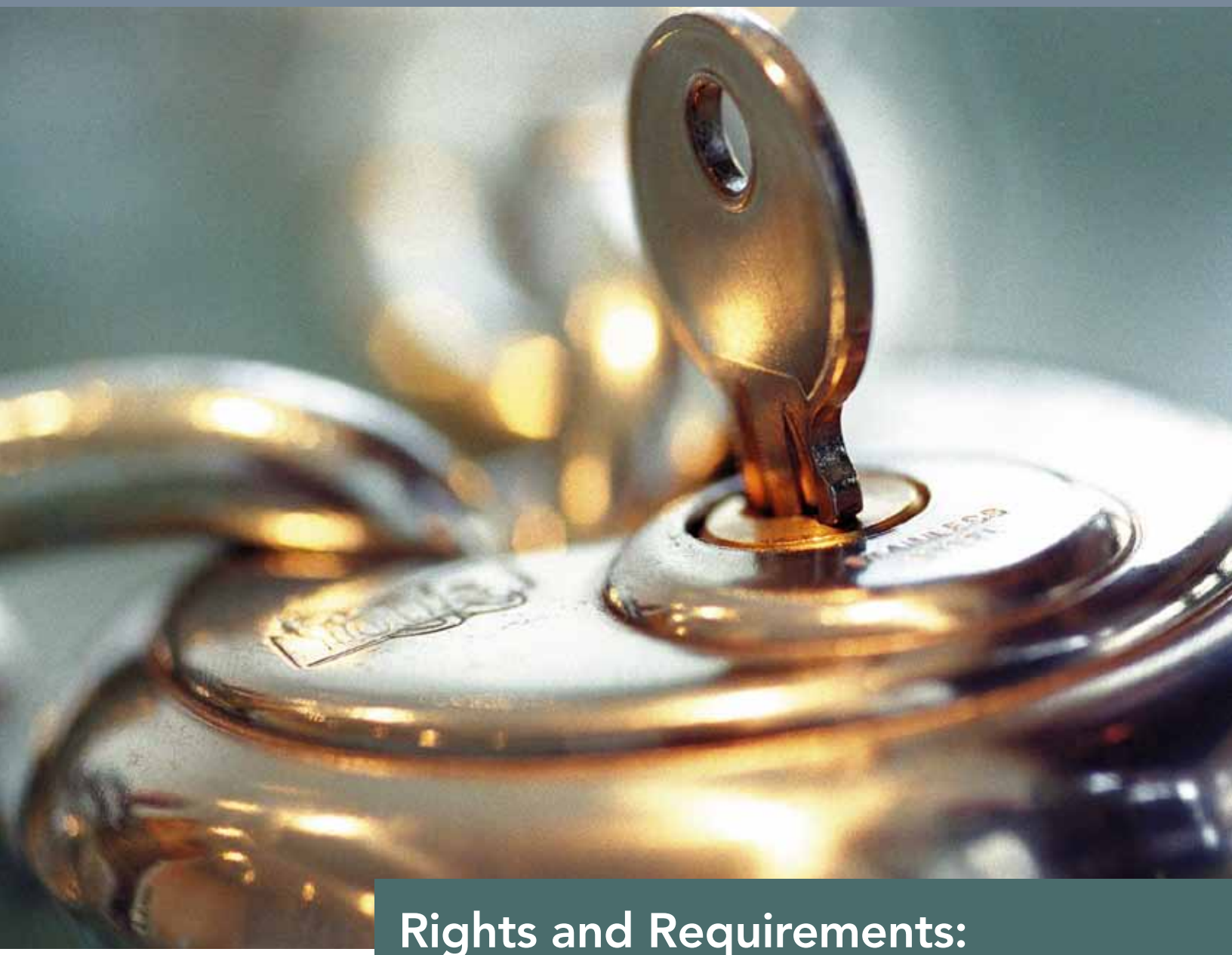
CALIFORNIA HEALTHCARE FOUNDATION



Rights and Requirements:
A Guide to Privacy and Security of Health Information in California

OCTOBER 2013

About the Authors

The **Center for Democracy & Technology** (CDT) is a nonprofit organization that promotes public policies to preserve privacy and enhance civil liberties in the digital age. Through its Health Privacy Project, CDT champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through development of industry best practices and technology standards.

Deven McGraw, JD, LLM, MPH, is director of the Health Privacy Project at CDT. Ms. McGraw's work focuses on the adoption and implementation of health information technology and electronic health information exchange to improve health care. She also chairs the privacy and security working group of the Health Information Technology Policy Committee, a federal advisory committee established by the American Recovery and Reinvestment Act of 2009.

Alice Leiter, JD, serves as policy counsel for CDT's Health Privacy Project. Her work focuses on developing policies for the advancement, adoption, and implementation of health information technology and electronic health information exchange to improve health care. She was formerly the director of health information technology policy for the National Partnership for Women & Families.

Christopher Rasmussen, MPP, is a policy analyst for CDT's Health Privacy Project. He focuses on developing workable privacy and security policies to govern personal health information in California. He formerly worked on health data privacy and security policies for the federal Veterans Health Administration.

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 www.chcf.org.

Contents

Introduction

Protecting the privacy and security of their personal health information is extremely important to patients. Indeed, fear that medical information might not be kept private and protected from unauthorized uses may even keep some patients from seeking care at all. In response, states and the federal government have enacted laws and rules to protect the privacy and security of health information.

This report analyzes the current health privacy landscape in California, including both federal and California state law, with particular attention to changes made by passage of the federal Health Information Technology for Economic and Clinical Health Act (HITECH) and the Patient Protection and Affordable Care Act (ACA). Specifically, the report covers:

- Sources of legal protection for health information privacy
- Who is covered by which privacy laws, and what types of health information are afforded protection
- Patients' rights to access, and to amend, health information
- Audit "trails" for health information disclosures
- How entities are permitted to use and disclose health information, and restrictions on such use
- Patient notification in the event of a breach
- Enforcement of health information privacy laws
- Specific protections for information collected by health insurers and health insurance exchanges.

The report also identifies gaps in privacy protection that remain unaddressed by state and federal law and that merit further attention from policymakers.

Sources of Legal Protection for Health Information

In California, legal protection for health information comes from a combination of federal and state law. The main source of federal protection is regulations enacted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which set the baseline for health information privacy and security in all states.[1] However, in enacting HIPAA, Congress expressly provided that stronger state health privacy laws could also be enforced, and under this authority specific California laws provide enhanced protection.

Federal Preemption of State Laws

The legal doctrine of preemption — that is, the overriding of state law by federal law on the same subject — is relatively simple in the area of health information privacy. Congress made explicit in HIPAA that the act's federal protections do not preempt state laws on the subject, and that state regulations more protective of patient rights than HIPAA's are enforceable. (Social Security Act §1178.) For California, this means two things: (1) to the extent that HIPAA and CMIA provide different but not conflicting protections, both apply; and (2) when the provisions of either law are more protective than the other's on the same matter, the more stringent rules set the legal standard. The advent of HITECH has not altered this dynamic — its health privacy provisions strengthen those in HIPAA but do not preempt even stronger provisions in California law.

The 2009 American Recovery and Reinvestment Act (ARRA) economic stimulus legislation added to HIPAA's federal protections.[2] HITECH, which is a section of ARRA, strengthened HIPAA protections in a number of substantial ways, in some cases providing stronger protections than previously existed for patients in California.[3] (For a discussion of the ways HITECH changed health information protection in California, see The Impact of Federal Stimulus Efforts on the Privacy and Security of Health Information in California.) In January 2013, federal regulations, commonly referred to as the HIPAA Omnibus

Rule, were issued to clarify and finalize implementation of the HITECH privacy and security provisions.[4]

The March 2010 enactment of the ACA also changed the health information landscape. The ACA mandates the establishment of health insurance exchanges to facilitate the enrollment of individuals into public or private health care coverage. States can establish their own exchanges — which California has chosen to do — or help their residents use a federal exchange offered by the United States Department of Health and Human Services (HHS).[5] Federal regulations implementing the ACA require information collected or accessed by these insurance exchanges to be protected by privacy and security policies that are consistent with the framework of fair information practices adopted by the HHS Office of the National Coordinator.[6]

California state law, especially the California Confidentiality of Medical Information Act (CMIA), has long provided health information privacy protection apart from federal requirements.[7] And since the 2009 passage of the federal HITECH protections, California has made important updates to its state privacy laws, amending the CMIA throughout the years to comply with changes in federal law and to strengthen privacy and security protections in significant ways.

Who and What Are Covered by Health Privacy Laws

Coverage Under Federal Law

HIPAA, the principal federal law regulating health information privacy, applies to what it refers to as "covered entities," which broadly consist of health care providers, health insurers, and health care clearinghouses (entities that process or facilitate the processing of health care information).[8] The HIPAA Privacy Rule — the regulations implementing HIPAA's privacy protections — establishes the circumstances under which "protected health information" (PHI) (information that does or can identify an individual) held by covered entities can be accessed, used, or disclosed. The Privacy Rule sets out when PHI can and cannot be used or disclosed without patient authorization, and grants individuals certain rights to their own health information.[9] The HIPAA Security Rule mandates appropriate safeguards — administrative, physical, and technical — to ensure the confidentiality, integrity, and security of PHI stored electronically.

HITECH extended HIPAA's coverage to include "business associates" that, on behalf of a HIPAA-covered entity, perform functions or services that include handling of PHI.[10] Pursuant to this HITECH expansion, HIPAA coverage now extends to any entity that "creates, receives, maintains, or transmits" PHI on behalf of a covered entity or on behalf of a business associate (i.e., subcontractor of a business associate).[11] HITECH also explicitly included entities such as regional health information organizations and health information exchanges (HIEs) in its expanded definition of what constitutes a business associate, meaning both are now directly accountable for complying with HIPAA.[12] This is important to California, as the state currently is working on implementing a network of HIEs, enabled by California Health eQuality.[13]

In implementing the HITECH changes to HIPAA, federal regulators have tried to clarify what types of activities trigger HIPAA obligations, whether by covered entities, business associates, or subcontractors. For example, the HIPAA status of intermediaries, which might store a provider's health data or facilitate the exchange of health data among providers or between providers and patients, has been a topic of much discussion. HHS recently made clear that a company that stores or maintains PHI on behalf of a covered entity is considered to be a business associate. However, "mere conduits" for the transmission of PHI are not considered to be business associates. With respect to what constitutes a mere conduit, HHS explained that any entity that transmits PHI and has regular or "more than random" access to it, or who stores it beyond the length of time reasonably needed to facilitate a transmission, is not a mere conduit but a business associate and so covered by HIPAA rules.[14] This interpretation is of great consequence for many health data service providers in California and elsewhere.

Coverage Under California Law

CMIA, the principal California state law addressing the privacy and security of medical information, lists permitted uses and disclosures of medical information for entities covered by the law, as HIPAA does. These covered entities include health care providers, health

services plans, and individuals and businesses that contract with these entities for work that involves access to medical information.[15] Further, CMIA covers "[a]ny business organized for the primary purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care," making its scope broader than HIPAA's.[16]

Though CMIA's coverage has been expanded in recent years, its application to one set of entities in particular has been somewhat unclear: vendors of personal health records (PHRs). PHRs are separate records of health information that are managed, controlled, and shared by individuals rather than by their health care providers. These tools tend to be offered by large companies with multiple business lines and, as a result, it is currently uncertain whether these vendors can be categorized as "organized for the primary purpose of" maintaining medical information.[17] Importantly, new legislation has addressed this issue, and as of September 2013, any business that offers a PHR or other digital tool for managing health information is now subject to CMIA.[18] (Of note, only PHRs offered through a HIPAA-covered entity, such as a physician or health plan, are covered by federal privacy laws.)[19] As with HIPAA, CMIA extends privacy protections only to identifiable health information, meaning that health information that cannot be connected to an individual patient is not subject to privacy regulation.

Patient Rights to View and Amend Health Information

Patient Access to Records

Both state and federal laws give residents of California the right to have access to their medical records, but on this issue California law is more stringent in favor of the patient. California law grants individuals broad general access to their medical records: inspection of records within five business days of making a request, and copies of records within 15 business days of request.[20] HIPAA, on the other hand, only requires covered entities to act on an individual's request for access to his or her PHI, paper or electronic, within 30 days of the request.[21]

In the near future, some patients may have much quicker access to their electronic medical records than currently required by federal law. An important component of HITECH was an incentive program that encourages the adoption and use by doctors and hospitals of electronic health record (EHR) technology. Beginning in 2014, one of the criteria to qualify for these incentives is for participating doctors and hospitals to make digital health information available to patients — for either viewing, transmission, or download — within four business days of the data being available to the entity.

Though California already has a similar timeframe for viewing records, this HITECH timeframe will be significantly faster than the 15 days for actual production of records provided by California law.[22] Although this rule will not apply to all records for all patients in California, the expectation is that the timely availability to patients of their digital health data will increase exponentially in the coming years.

HIPAA requires covered entities to provide individuals with copies of their medical records in the format they request (with limited exceptions) for a "reasonable" charge.[23] In California, state law sets these permissible costs at up to 25 cents per page for print records and 50 cents per page for microfilm, plus reasonable clerical fees.[24] Under HIPAA, patients have the right to an electronic copy of medical record information that is maintained electronically, as well as the right to send an electronic copy of their health data elsewhere, such as to another doctor, caregiver, or mobile health application. The fee for getting health information in digital form may not include page charges or any fees associated with new technology, systems maintenance, data access, or storage infrastructure, or a retrieval fee for electronic copies.[25] As a result, patients likely will pay less for copies of electronic records than the historic California maximum amounts, which apply to paper-based records.

Patient Amendment of Health Information

Under both federal and California law, if a patient finds an error in his or her medical record, the patient has a right to request an amendment to the record. Under HIPAA, a covered entity has up to 90 days (60 days, with one 30-day extension) to act on an individual's request for an amendment.[26] Under federal law, if a covered entity denies the request to amend, the patient may then ask that the request for amendment and the denial of that request be included with any subsequent disclosure of

the disputed portion of the medical record, and the covered entity must comply.[27] In California, any request to amend a portion of the health record must be included with subsequent disclosures to any third party of the allegedly incomplete or incorrect portion of the patient's record.[28]

Through the Personal Data Information Practices Act, Californians can also request to amend medical information held by state agencies. After receiving such a request, a state agency has 30 days (with one 30-day extension for good cause) to either make the correction or deny the request and inform the individual of the right to a review by the agency of that decision.[29]

Audit Trails of Patient Records

It is not only health care providers that come into contact with an individual's identifiable health information. Health data can be and often is shared among insurers, medical management services, prescription processors, and others. And this sharing of information is expanding exponentially with the rapidly spreading adoption of EHRs. As a result, an increasingly important aspect of the right to privacy is patients' ability to follow what is referred to as the "audit trail" of their medical records — that is, to learn who has obtained information from those records and for what purpose.

Under HIPAA, patients may ask covered entities for an "accounting of disclosures," an annual report of certain types of disclosures from their medical records, going back six years prior to the request.[32] However, routine disclosures from records — such as disclosures to other providers for treatment purposes, or to insurers for payment, or for "health care operations" (a HIPAA-defined category of routine business operations) — are not required to be included in the accounting. HITECH expanded this accounting rule by requiring entities using EHRs to provide an accounting or audit trail specifically including disclosures for routine purposes such as treatment, payment, and health care operations, going back three years.[33] (There is no comparable requirement for paper records.) Although this expansion increases transparency of disclosures for patients, it also would require covered entities or business associates that use or maintain EHRs to keep track of disclosures made for the most common and frequent health care transactions. Having recognized this potential burden on providers, HHS has yet to issue regulations regarding how to implement these HITECH provisions in a way that balances that burden against greater transparency for patients.[34] California law does not address an individual's right to request information about who has asked for and received copies of an identifiable medical record.

Another HIPAA provision enhancing transparency for patients requires all covered entities to notify individuals of the entity's privacy practices. This notice, which patients typically receive annually from their health insurer or from a new medical provider, must include a description of all the types of uses and disclosures that require patient authorization.[35] California does not have a similar requirement.

California Law to Preserve Electronic Record Changes

California law requires that EHR systems must have audit capabilities to record and preserve changes to or deletions of records, including the identity of the person who accessed and changed the information, in addition to the actual changes made.[30] Although the CMIA does not require entities holding records to make these audit trails available to patients, it is more stringent than HIPAA in that audit logs must record and preserve the actual content changes to a record.[31] This is meaningful for patients in that it decreases the potential for health information to get lost or omitted from records while increasing the potential for accountability in the event of an inquiry into the use or disclosure of medical information.

Permitted and Restricted Uses and Disclosures

State and Federal General Standards

It is not uncommon for PHI privacy laws to expressly permit uses and disclosures of information that are considered routine (and therefore to be reasonably expected by patients) or in circumstances where other public policy needs require that information be shared. Accordingly, both HIPAA and CMIA generally permit the disclosure of PHI for purposes of treatment, payment, and "health care operations" (which include certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment) without the need to first obtain express patient consent.[36] Both laws also include a variety of other permitted and/or required specific purposes. For example, CMIA permits disclosure of medical information related to child or elder abuse to a coroner conducting an investigation, and information from a psychotherapist under certain circumstances, such as disclosure to the FDA concerning potential safety issues of a drug or medical device.[37]

But for more sensitive types of information or non-routine uses, privacy laws frequently give individuals greater control over information sharing. California law requires prior written authorization for certain types of sensitive information disclosures, including psychotherapy notes, drug and alcohol treatment records, and HIV status and test results.[38]

On the federal front, HIPAA limits access to and use and disclosure of health information to the "minimum necessary" needed to accomplish a particular purpose. This requirement does not apply in the case of treatment (regulators did not want health care providers second-guessing how much information to provide in a treatment situation), disclosures to individuals of their own PHI, uses and disclosures pursuant to a written patient authorization (on the presumption that the authorization will specify the parameters of the data to be used and disclosed), disclosures required by law, and several other circumstances.[39] HITECH directed HHS to issue guidance to help entities covered by HIPAA in determining what is the "minimum necessary" in different contexts, but this guidance has yet to be released.[40] Also, there is a HIPAA requirement that researchers obtain written authorization from an individual prior to accessing PHI (except for public health research), although that requirement can be waived by an Institutional Review Board.[41]

Recent Changes Regarding Specific Uses and Disclosures

The following categories of PHI uses and disclosures have been affected by recent changes to federal law. These changes are pursuant to HITECH and were finalized in the HIPAA Omnibus Rule; they went into effect on March 26, 2013, and HHS officials began enforcing them on September 23, 2013. Some of the changes expand patient privacy protection while others broaden the use or disclosure of PHI.

Marketing

HIPAA requires covered entities to obtain consent from patients before using their PHI for marketing purposes. However, communications sent by providers and insurers to patients encouraging them to consider certain health care products or services historically were treated as patient education materials rather than marketing. California's rules regarding when patient information can be used for marketing purposes are similar to these historic HIPAA rules.[42] For example, patient authorization for marketing uses of information is required, but the law includes a number of exceptions, including when the communication is about plan benefits or services or the availability of more cost-effective prescription drugs, and when the communication is specifically tailored to advise or educate an individual about treatment options.[43]

Under HITECH, the standards under HIPAA were made more restrictive. Regulations now in effect, declare that if such communications are paid for (directly or indirectly) by the manufacturer of the product or service being promoted, they are considered marketing.[44] As a result, the use of a patient's PHI to send such sponsored communications requires the prior written authorization of the patient.

However, HITECH established an important exception to this authorization requirement for sponsored communications: prescription refill reminders.[45] Thus, covered entities can send patients subsidized communications about medications they are currently taking without first obtaining their authorization, so long as the subsidy is

both "reasonable in amount" and "reasonably related" to the entity's costs of making the communication.[46] In response to some concerns raised by consumer advocates regarding the sustainability of patient refill reminder programs in the wake of these stronger protections, HHS intends to release additional guidance regarding what constitutes "reasonable in amount" and "reasonably related."[47]

These recent changes to HIPAA's marketing rules now provide stronger protections than California law does, which means that, under the federal preemption doctrine, HIPAA rules govern any entity covered by both HIPAA and California law.

Fundraising

Historically, HIPAA has allowed basic PHI to be used for a covered entity's own fundraising purposes. This included some demographic information, such as an individual's health insurance status and dates of health care provided.[48] The entity's right to use this information was subject to the patient's right to opt out of having it used for this purpose. Entities were required to make "best efforts" to honor a patient's opt-out decision.

Recent changes to HIPAA allow more patient information to be used for fundraising purposes, including information about department of service, treating physician, and outcome. Usable demographic information now explicitly includes name, address, date of birth, and gender. However, the patient's right to opt out also has been strengthened; HHS clarified that individuals must have a right to easily and successfully elect not to have their information used for fundraising, and this right must be stated in a covered entity's notice of privacy practices.[49]

Sale of PHI

California law prohibits intentional, unauthorized (by the patient) sale of medical information for purposes that are not necessary to provide "health care services" to a patient.[50] Unfortunately, there is little guidance on what "necessary" and "health care services" mean; consequently, entities covered by the law are left to their own interpretations. Understandably, this has resulted in some confusion.[51]

Under recent changes to HIPAA, however, a covered entity or business associate is prohibited from receiving direct or indirect payment (including nonfinancial benefits) in exchange for any PHI of an individual, unless the covered entity obtains a valid authorization from that individual. There are, however, exceptions to this ban, including public health activities, some research purposes, treatment and payment purposes, health care operations, and others.[52] Many of the exceptions were intended to acknowledge the reality of the health care system: PHI is frequently shared, and money exchanged, as part of a routine health care transaction (such as payment for an insurance claim or payment to an academic medical center for conducting research), and such transactions should not be labeled as "sales" requiring prior patient authorization. Other exceptions (such as for research) were intended to ensure the availability of data for important purposes. (See Table 1 for a full list of these exceptions.)

Table 1. Exceptions to Authorization Requirement for Sale of PHI

The following are categories of exceptions to the HIPAA ban on payment in exchange for an individual's PHI:

- Public health
- Research — remuneration must be reasonably related to the cost of preparing and transmitting information (can include indirect costs but cannot result in a profit)
- Treatment and payment — disclosure of PHI to receive payment is not a "sale" of PHI
- Corporate transactions (i.e., sale, transfer, merger, consolidation of all or part of a covered entity and related due diligence)
- Disclosures to business associates
- Disclosures to the individual
- Disclosures required by law
- Other disclosures permitted by the rules, provided remuneration is limited to reasonable cost of making the disclosure.

Source: 78 Fed. Reg. 5603–5609.

Genetic Information

HIPAA now contains provisions required by the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits discrimination, in both health coverage and employment, based on an individual's genetic information.[53] Pursuant to GINA's requirements, the HIPAA Privacy Rule now explicitly prohibits the use or disclosure of genetic information for insurance underwriting purposes, except for long term care insurance.[54]

Patient Notification in the Event of a Breach

California was the first state to enact a breach notification law that applied to computerized personal information, pioneering the way for other states and eventually to federal breach notification laws.[55] California's breach law was amended in 2008 to extend the notification requirements specifically to electronic medical and health insurance information. In 2009, Congress enacted comprehensive breach notification requirements for entities covered by HIPAA and for PHRs, though in some respects California's law is more stringent, as discussed below.

Federal Law on Breach Notification

HITECH requires HIPAA-covered entities to notify individuals in the event of either unauthorized disclosure of health information to third parties or unauthorized insider access to information. HITECH defines "breach" as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information.[56] Business associates (contractors) of a covered entity must notify that entity, which in turn must notify the individual within 60 days after the breach is discovered.[57]

The HITECH notification requirement is not triggered if a breach involves information that cannot be read or accessed because it is protected by a secure technology or methodology, such as encryption, approved by the secretary of HHS. Federal law specifies how breach notices must be sent and what information they must contain, including how the breach occurred, what actions have been taken in mitigation, and contact information. All breaches must be reported to federal authorities, and an entity that incurs a breach that affects 500 or more people must notify prominent media outlets serving the state or area where the breach occurred.[58]

Shortly after the enactment of HITECH, HHS put forth an interim breach notification standard, which further defined a breach as one that posed a significant risk of financial, reputational, or other harm to the affected individual.[59] More recent regulations changed this standard, in response to concerns by consumer advocates that it was too subjective and provided too much discretion to the covered entities.[60] Under the new regulations, entities covered by HIPAA must treat a breach as requiring notification to individuals unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised in the breach.[61] HHS eliminated the subjective harm standard in favor of a four-factor risk analysis, which covered entities must conduct to determine whether PHI has been compromised. This analysis must consider:

- The nature and extent of PHI involved, including the types of identifiers and likelihood that an individual can be identified
- Who impermissibly used the PHI or to whom the PHI was impermissibly disclosed
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated.[62]

HITECH also includes its own separate breach notification provisions applicable to vendors of PHRs and to applications that interact with such PHRs or that are offered to individuals with PHR accounts. These entities must notify individuals directly in the event of a breach. For these tools, which often are patient-controlled, the notification requirement is triggered if unsecured information is acquired from their PHR without authorization.[63]

California Law on Breach Notification

California's breach law requires that individuals be notified when there has been a breach involving health information that is not secured through encryption if the information is "reasonably believed to have been acquired by an unauthorized person."[64] The state law requires certain entities (clinics, health facilities, home health agencies, and hospices) to notify affected individuals of a breach, as well as to notify the California Department of Health.[65] California entities to which the breach notification requirements apply have only five business days after discovering a breach of medical information to report it, and only law enforcement may request a delay in such notice.[66]

The breach notification must include: a general description of the incident, the type of information breached, the date and time of the breach, a toll-free telephone number to call for further information, and the toll-free telephone numbers and addresses of the three major

California credit bureaus if the breach exposed a Social Security, driver license, or California identification card number.[67]

California law also requires any agency, person, or business that sends a security breach notice to more than 500 California residents to electronically submit a single sample copy of that security breach notification to the state attorney general, excluding any personally identifiable information. The state Department of Health, after investigation, may assess an administrative penalty for a violation of this section of up to $25,000 per patient whose medical information was accessed, used, or disclosed unlawfully or without authorization, and up to $17,500 per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of that patient's medical information.[68] The law also deems a HIPAA-covered entity in California to have met the content notification requirements if it has complied with the similar HITECH requirements in section 13402(f) of that law, though this compliance does not exempt it from the other aspects of California's notification requirements.

Interaction Between State and Federal Breach Laws

Despite their similarities, California breach law differs from federal law in important ways, with its breach notification requirements more stringent in two respects: the standard for determining whether notification is required, and the timeframe for notification.

In California, if information is reasonably believed to have been acquired by an unauthorized person, notification is required. Under HIPAA, by contrast, information acquired by an unauthorized person does not require notification if the covered entity can demonstrate a low probability that the PHI has been compromised. With respect to notification timeframes, in California affected individuals must be notified within five days, as opposed to up to 60 days under federal law. (See Table 2 for a comparison of state and federal breach notification requirements.)

Table 2. Federal and California Breach Notification Compared

FEDERAL	CALIFORNIA
Notification required: Unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised. Four-factor test to determine compromise: 1. Nature and extent of PHI involved, including types of identifiers and likelihood that an individual can be identified 2. Who impermissibly used the PHI or to whom the PHI was impermissibly disclosed 3. Whether the PHI was actually acquired or viewed 4. Extent to which the risk to the PHI has been mitigated **Notification not required:** If a breach involves information that cannot be read or accessed because it is protected by a secure technology or methodology, such as encryption, approved by the Secretary of HHS.	**Notification required:** If information is reasonably believed to have been acquired by an unauthorized person. **Notification not required:** If information is secured through encryption.
Timing of notification: Within 60 days after breach is discovered.	**Timing of notification:** Within five days after breach is discovered.
Who must report: Covered entities, business associates, and PHR vendors.	**Who must report:** Clinics, health facilities, home health agencies, and hospices.
To whom reported: Covered entities to individuals, business associates to covered entities, PHR vendors to affected individuals; all breaches reported to federal authorities, and to prominent state/local media outlets if more than 500 people affected.	**To whom reported:** Covered entities to all affected patients and to the California Department of Health; any agency, person, or business that sends a security breach notice to more than 500 California residents must notify the state's attorney general.

Table 2. Federal and California Breach Notification Compared, *continued*

FEDERAL	CALIFORNIA
Content: Brief description of what happened, including date of breach and date of discovery of breach; description of types of PHI involved in breach; steps individuals should take to protect themselves from potential harm resulting from breach; brief description of what covered entity involved is doing to investigate breach, to mitigate losses, and to protect against further breaches; and contact procedures for individuals to learn more/ask questions, including a toll-free phone number and an e-mail address, website, or postal address.	**Content:** General description of the incident, type of information breached, date and time of breach, toll-free phone number to call for further information; also, the toll-free telephone numbers and addresses of the three major California credit bureaus if breach exposed a Social Security, driver license, or California identification card number. **Note:** With passage of California Senate Bill 24 in 2011, HIPAA-covered entities in California that comply with the breach notice requirements of HITECH will be deemed in compliance with the California content requirements, but such entities still have to comply with the attorney general notice provision.

Source: HIPAA, HITECH, California Civil Code §§ 1798.80–84.

Enforcement of Health Information Privacy Laws

With regard to federal law, HIPAA as significantly strengthened by HITECH provides for civil monetary penalties in case of a violation. (See Table 3.) These penalties go directly to HHS's Office for Civil Rights and are used to fund enforcement activities. HITECH also extends HIPAA civil and criminal liability to business associates of covered entities and requires HHS to periodically conduct audits for compliance with HIPAA rules. Importantly, HITECH also grants HIPAA enforcement authority to state attorneys general, meaning that state authorities may pursue remedies for a HIPAA violation if HHS or other federal department does not.[69]

In determining the amount of any civil monetary penalty under HIPAA, HHS considers the following factors:

- Nature and extent of the violation
- Nature and extent of the harm resulting from the violation
- History of prior HIPAA compliance, including violations, by the covered entity or business associate
- Financial condition of the covered entity or business associate
- "Such other matters as justice may require."[70]

Table 3. Categories of HIPAA Violations and Respective Penalty Amounts

VIOLATION CATEGORY	PENALTY AMOUNT Per Violation	PENALTY AMOUNT Maximum Combined*
Did not know of breach and by exercising reasonable diligence would not have known	$100 to $50,000	$1,500,000
Reasonable cause†	$1,000 to $50,000	$1,500,000
Willful neglect resulting in breach, but breach timely corrected	$10,000 to $50,000	$1,500,000
Willful neglect resulting in breach and breach not timely corrected	$50,000+	$1,500,000

*Maximum combined fine for violations of an identical provision in a calendar year.

†Reasonable cause means "[A]n act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." 45 CFR 160.401.

Source: 45 CFR 164.404(b).

HHS must look into any complaint that comes to it, and when a complaint comes directly to a state attorney general, federal officials must be notified. Federal officials have priority to investigate all complaints, whether they were initiated at the federal or state level. When a preliminary review of the facts indicates that a possible violation was due to willful neglect (as opposed to, for example, simple negligence), HHS will conduct a formal investigation, which may include a compliance review of the entity's HIPAA policies and procedures.[71]

Under California law, the state attorney general, a county counsel, district attorney, or city attorney may bring a civil action to enforce CMIA, and individuals may sue for damages arising from any negligent release of confidential information.[72] CMIA provides entities with some affirmative defenses to avoid paying damages, including that the entity was compliant with all security requirements and took the appropriate corrective steps after the breach was discovered.[73]

Protections for Information Collected by Health Insurers and Health Insurance Exchanges

The 2010 Patient Protection and Affordable Care Act (ACA) mandates the establishment of health insurance exchanges to facilitate the enrollment of individuals into public or private health care coverage. A state may establish its own exchange or instead may facilitate its residents' use of a federal exchange created by HHS. California is in the process of establishing its own state exchange, for which open enrollment began October 1, 2013. Federal regulations require that information collected or used by these insurance exchanges be protected by privacy and security policies.

ACA places strong limits both on the data that may be collected about a person seeking coverage through an exchange and on the use of this data. Data collection is limited to information strictly necessary to authenticate a person's identity, determine his or her eligibility, and determine the amount of an enrollee's federal credit or discount. Furthermore, an exchange may use such information only for the purpose of ensuring the efficient operation of the exchange (as opposed to, for example, using the information to market a product to its customers). ACA also specifically limits the collection, use, and disclosure of Social Security numbers, which can only be required once an applicant actually seeks to enroll in a health insurance plan, not from individuals who are simply exploring the exchange or comparing plans.[74]

In planning for Covered California, as its exchange is called, the state has enacted a number of provisions that address patient privacy. For example, the state's Health Care Eligibility, Enrollment, and Retention Act includes a mandate that Covered California take into account "protections for the confidentiality of personal information" in planning and developing the state's exchange, and abide by "all privacy and confidentiality rights under the [ACA] and other federal and state laws . . . including responses to security breaches."[75]

Gaps in Health Information Privacy Protection

In California, a combination of federal and state law provides a foundation of protections for health information, but gaps remain to be addressed. A number of these gaps were highlighted in the 2012 report Achieving the Right Balance: Privacy and Security Policies to Support Electronic Health Information Exchange. Since then, some of these gaps have been filled, some remain unaddressed, and other needs have surfaced. Based on the present report's assessment of the current landscape of PHI privacy protection in California, policymakers may want to give particular consideration to the following:

- All business entities that access, use, and disclose identifiable health information should be held legally accountable for complying with some baseline privacy and security obligations. Today, federal coverage under HIPAA is limited to traditional health care system entities (such as providers and insurers) and their contractors. As discussed above, California lawmakers have extended CMIA's scope, but it is unclear whether these expansions suffice to provide comprehensive protections for consumers and patients regardless of which type of entity is accessing their information. Specifically, the risks patients face in sharing their digital health data online (such as with a social networking site) or with offline commercial entities (such as a fitness company or a weight-loss organization) likely are not well addressed by laws like CMIA and HIPAA that were designed to accommodate the information collection and disclosure needs of doctors, hospitals, and health plans. Federal and state breach notification laws extend to a broader range of entities than those covered by HIPAA and CMIA, but establishing notification rights and penalties for

breach does little to regulate an entity's ability to collect, use, and disclose data.

- Enforcement of federal and state health privacy and security protections has significantly improved in recent years. At the same time, entities uncertain about their obligations under the law may err on the side of caution and decide not to share information, even in circumstances where they should — especially in the face of enhanced penalties for unauthorized disclosures. For example, some providers have refused to share information with other providers for treatment purposes or even with the patient, due to their lack of clarity about privacy laws. Increased guidance from regulators that sets clear expectations for compliant behavior can help obviate this problem.
- Security laws (such as the HIPAA Security Rule) should be regularly assessed to ensure that they are sufficient to meet new security challenges and to incorporate technological innovation. For example, reports of data breaches filed with HHS's Office for Civil Rights, which enforces breach notification requirements under HIPAA, strongly suggest that entities covered by these rules are not consistently using encryption to protect stored health information. Although encryption is standard in most other industries, the HIPAA Security Rule strongly encourages encryption but does not require it.
- Clear standards need to be established for de-identifying health data, and penalties need to be set for inappropriate or unauthorized re-identification.[76] Such standards and penalties ideally should be established at the federal level to avoid the confusion and resulting self-suppression of appropriate data sharing that might occur through adoption of potentially inconsistent state-level protections.
- Federal and state health information policy could provide incentives for the use of technical architectures for data sharing that enhance privacy. For example, decentralized data-sharing models avoid the need to create centralized, duplicative databases each time health information is needed for a particular purpose.

Conclusion

Recent legislative activity at both the federal and state levels has improved the health privacy landscape for patients in California. But work remains to be done to solidify the privacy and security of electronic health records and information exchange, and to build public trust in it. Policymakers can assist by filling gaps in the law, providing clear and comprehensive guidance on compliance with existing law, and supporting adequate enforcement of those protections.

Strong public policies are important — but there is a limit to what can be accomplished through government action. It is critical that all entities maintaining or transmitting health information implement responsible business practices that build on government-established baseline rules and are tailored to particular circumstances. A combination of public- and private-sector efforts can help realize the comprehensive framework of protections that will enable health information technology to power needed improvements in our nation's health care system.

Endnotes

1. Pub. L. 104–191, 110 Stat. 1936 (1996) (codified at Title XI of the Social Security Act).
2. Pub. L. 111–5, 123 Stat. 115 (Feb. 17, 2009).
3. *Id.* at Title XIII of Division A and Title IV of Division B.
4. 78 Fed. Reg. 5566–5702 (January 25, 2013).
5. 77 Fed. Reg. 18310 (March 27, 2012); see also Bernadette Fernandez and Annie L. Mach, *Health Insurance Exchanges Under the Patient Protection and Affordable Care Act (ACA)* (Washington, DC: Congressional Research Service, January 31, 2013), www.fas.org.
6. 77 Fed. Reg. 18339.
7. California Civil Code §§ 56–56.37.
8. 45 CFR 160.103.
9. 45 CFR 164.524.
10. 45 CFR 160.103.
11. 78 Fed. Reg. 5571–5574.
12. HITECH § 13408.
13. California Health eQuality (CHeQ) is a program of the Institute for Population Health Improvement at the University of California, Davis. Funded by the California Health and Human Services Agency, and under the auspices of the Office of the National Coordinator for Health IT (ONC) State HIE Cooperative Agreement, CHeQ promotes coordinated care through health information exchange. CHeQ programs include helping participants implement a trusted exchange environment, improving public health capacity for electronic reporting, identifying HIE acceleration funding opportunities, and monitoring HIE.
14. Joseph Lorenzo Hall, "HIPAA Final Rule Confirms That ISPs Transmitting PHI Are Not Business Associates," Center for Democracy & Technology, February 6, 2013, www.cdt.org/blogs/joseph-lorenzo-hall.
15. California Civil Code § 56.05–06.
16. *Id.*
17. "Personal Health Records and Privacy," Privacy Rights Clearinghouse, last modified October 2012, www.privacyrights.org.
18. California Assembly Bill 658, www.leginfo.ca.gov, signed into law September 9, 2013. The legislation subjects to the CMIA "any business that offers application software or hardware, including a mobile application or other related device that is designed to maintain medical information to allow an individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual."
19. See generally *Building a Strong Privacy and Security Policy Framework for Personal Health Records* (Washington, DC: Center for Democracy & Technology, July 21, 2010), www.cdt.org.
20. California Health and Safety Code § 123110.
21. Covered entities are permitted a one-time extension of up to 30 days for data that is maintained off-site. This notice must include the reason for the delay and the expected date of completion.
22. 77 CFR 170.314(e)(1).
23. 45 CFR 164.524(c)(4).
24. California Health and Safety Code § 123110.
25. 45 CFR 164.524 (2013).
26. 45 CFR 164.526.
27. *Id.*
28. California Health and Safety Code § 123111.
29. California Civil Code §§ 1798–1798.78.
30. Due to their very nature, there is no comparable requirement for paper records.
31. California Civil Code § 56.101.
32. 45 CFR 164.528.
33. HITECH Act § 13405(c).
34. Deven McGraw et al., *ARRA Accounting of Disclosure Requirements: Aligning Goals with Emerging Regulations* (Washington, DC: eHealth Initiative, February 2010), www.cdt.org.
35. 45 CFR 164.520.
36. 45 CFR 164.501.
37. California Civil Code § 56.10(b)(8) and § 56.104(e)(3).
38. California Health and Safety Code §§ 11845.5, 123105(b), and §§ 120975–121125; California Civil Code § 56.104.
39. 45 CFR 164.514(d).
40. The Omnibus Rule states that HHS still intends to issue future guidance on the minimum necessary standard but gives no timeframe.
41. 45 CFR 164.508, 164.512(i).
42. California Civil Code § 56.05(f).
43. California Civil Code § 1798.91 and §§ 56.05 and 56.10.
44. HITECH § 13406; see also 78 Fed. Reg. 5595–5597.
45. *Id.*
46. 78 Fed. Reg. 5597.
47. See, for example, Alice Leiter, "CDT Requests Clarification to HIPAA Marketing Guidance," Center for Democracy & Technology, June 10, 2013, www.cdt.org/blogs/alice-leiter.
48. 78 Fed. Reg. 5622.
49. 78 Fed. Reg. 5618–5622.
50. California Civil Code § 56.10(d).

51. See, for example, "Your Medical Information and Your Rights," Privacy Rights Clearinghouse, last modified July 2012, www.privacyrights.org.
52. 78 Fed. Reg. 5603–5609.1.
53. The Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233 (2008).
54. See 78 Fed. Reg. 5658–5669.
55. California Civil Code §§ 1798.82 and 1798.29.
56. HITECH § 13400(1).
57. HITECH § 13402.
58. *Id.*
59. 74 Fed. Reg. 42740, 42744.
60. "CDT and Markle Comments Requesting a Revised Harm Standard," Center for Democracy & Technology, October 23, 2009, www.cdt.org.
61. 78 Fed. Reg. 5641–5646.
62. *Id.*
63. HITECH § 13407.
64. California Civil Code § 1798.82(a).
65. California Health and Safety Code § 1280.15.
66. *Id.*
67. California Civil Code. § 1798.80–84; California Health and Safety Code § 1280.15.
68. California Health and Safety Code § 1280.15.
69. HITECH §§ 13410, 13411.
70. 45 CFR 160.408.
71. 78 Fed. Reg. 5578.
72. California Civil Code §§ 56.35–36.
73. California Civil Code § 56.36.
74. See 77 Fed. Reg. 42658–42672 (July 20, 2012); see also *Privacy and Security Protections for Personal Information in California's Health Benefit Exchange* (Washington, DC: Center for Democracy & Technology, March 28, 2012), www.cdt.org.
75. California Welfare and Institutions Code §§ 15925(b)(3)(G) and 15926(m).
76. Deven McGraw, "Building Public Trust in Uses of Health Insurance Portability and Accountability Act De-Identified Data," *Journal of the American Medical Informatics Association* 20, no. 1 (January 1, 2013): 29–34, jamia.bmj.com.